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

Elliptische Kurven

Arbeitsblatt 13

Aufgaben

Die folgenden Aufgaben nehmen Bezug auf den Chinesischen Restsatz für den Polynomring $K[X]$.

Aufgabe 13.1.*

Schreibe den Restklassenring $\mathbb{Q}[X]/(X^4-1)$ als ein Produkt von Körpern, wobei lediglich die Körper $\mathbb{Q}$ und $\mathbb{Q}[\mathrm{i}]$ vorkommen. Schreibe die Restklasse von X^3+X als ein Tupel in dieser Produktzerlegung.

Aufgabe 13.2. Realisiere den Produktring

$$\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}$$

als einen Restklassenring von $\mathbb{R}[X]$.

Aufgabe 13.3. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es seien $a_1,\ldots,a_n\in K$ verschiedene Elemente und

$$F = (X-a_1)\cdots(X-a_n)$$

das Produkt der zugehörigen linearen Polynome. Zeige, dass der Restklassenring $K[X]/(F)$ isomorph zum Produktring K^n ist.

Aufgabe 13.4. Sei K ein algebraisch abgeschlossener Körper und $K[X]$ der Polynomring über K. Zeige, dass der Restklassenring zu einem Polynom $F\neq 0$ die Struktur

$$K[X]/(F) \cong K[T]/(T^{n_1})\times\cdots\times K[T]/(T^{n_r})$$

besitzt. Zeige, dass dabei

$$\operatorname{grad}(F) = n_1+\cdots+n_r$$

ist.

Aufgabe 13.5.*

Das Polynom $X^3 - 7X^2 + 3X - 21$ besitzt in $\mathbb{R}[X]$ die Zerlegung

$$X^3 - 7X^2 + 3X - 21 = (X-7)(X^2+3)$$

in irreduzible Faktoren und daher gilt die Isomorphie

$$\mathbb{R}[X]/(X^3 - 7X^2 + 3X - 21) \cong \mathbb{R}[X]/(X-7) \times \mathbb{R}[X]/(X^2+3).$$

a) Bestimme das Polynom kleinsten Grades, das rechts dem Element $(1,0)$ entspricht.

a) Bestimme das Polynom kleinsten Grades, das rechts dem Element $(0,1)$ entspricht.

Aufgabe 13.6. Zeige, dass die folgenden Daten bzw. Konstruktionen den gleichen Morphismus

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

von der projektiven Geraden in sich festlegen (dabei seien $(a,b),(c,d) \in K^2$ linear unabhängig).

(1) Der induzierte Morphismus im Sinne von Satz 12.11 (Bündel, Garben und Kohomologie (Osnabrück 2019-2020)) zum homogenen Ringhomomorphismus $K[X,Y] \to K[S,T]$ mit $X \mapsto aS + bT$, $Y \mapsto cS + dT$.

(2) Der Morphismus zu den beiden Schnitten

$$as + bt, cs + dt \in \Gamma\left(\mathbb{P}^1_K, \mathcal{O}_{\mathbb{P}^1_K}(1)\right)$$

im Sinne von Lemma 28.1 (Bündel, Garben und Kohomologie (Osnabrück 2019-2020)).

(3) Der Morphismus im Sinne von Lemma 7.13 zur rationalen Funktion $\frac{as+bt}{cs+dt} \in K\left(\frac{s}{t}\right)$.

Aufgabe 13.7. Es sei C eine irreduzible glatte projektive Kurve mit Funktionenkörper $Q(C) =$ und $q \in Q(C)$ mit zugehörigem Morphismus

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

Sei $a \in K$. Zeige, dass es einen Automorphismus

$$\theta\colon \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$$

derart gibt, dass das Diagramm

$$\begin{array}{ccc} C & \xrightarrow{q} & \mathbb{P}^1_K \\ & q-a \searrow & \downarrow \theta \\ & & \mathbb{P}^1_K \end{array}$$

kommutiert.

Zu einem Ringhomomorphismus $\varphi\colon R \to S$ zwischen kommutativen Ringen und einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ nennt man $(S/\mathfrak{q}S)_{\varphi(R\setminus\mathfrak{q})}$ den *Faserring* über $\mathfrak{q}$.

AUFGABE 13.8. Es sei K ein Körper und

$$K[Y] \longrightarrow K[X] \cong K[Y][X]/(Y - X^n),\ Y \longmapsto X^n,$$

die n-te Potenzabbildung. Bestimme zu $b \in K$ den Faserring über $(Y - b)$. Wann sind alle Primfaktoren von $X^n - b$ einfach?

AUFGABE 13.9.*

Bestimme die Faser zum Morphismus

$$V(Y^2 - X^3 + 3X + 2) \longrightarrow \mathbb{A}^1_{\mathbb{C}},\ (x, y) \longmapsto x,$$

für die Punkte

(1)
$$P = 0,$$
(2)
$$Q = 2,$$
(3)
$$R = 3.$$

AUFGABE 13.10.*

Zeige, dass durch

$$\varphi\colon V(Z^2+W^2-1) \longrightarrow V(X^2+Y^2-1),\ (Z, W) \longmapsto (Z^2-W^2, 2ZW) = (X, Y).$$

ein Morphismus des Einheitskreises in sich gegeben ist. Zeige, dass das Urbild zu jedem Punkt $P \in V(X^2 + Y^2 - 1)$ aus zwei Punkten besteht.

AUFGABE 13.11. Es sei K ein Körper und A eine endlichdimensionale, reduzierte K-Algebra. Zeige, dass dann A ein endliches direktes Produkt von endlichen Körpererweiterungen von K ist.

AUFGABE 13.12.*

Bestimme den Faserring (einschließlich der Produktzerlegung) zum Morphismus

$$V(Y^2 - X^3 + 3X + 2) \longrightarrow \mathbb{A}^1_{\mathbb{C}},\ (x, y) \longmapsto x,$$

für die Punkte

(1)
$$P = 0,$$

(2)

$$Q = 2,$$

(3)

$$R = 3.$$

Aufgabe 13.13. Diskutiere die Ausnahmen für die Gradbedingung im Beweis zu Lemma 13.3 an den Beispielen

(1)

$$f(x) = \frac{x+1}{x}.$$

(2)

$$f(x) = \frac{3x^2+5x-3}{4x^2-x+1}.$$

(3)

$$f(x) = \frac{x}{x^2-5}.$$

Aufgabe 13.14. Es seien C und D irreduzible glatte Kurven über einem algebraisch abgeschlossenen Körper K und sei

$$\varphi\colon C \longrightarrow D$$

eine nichtkonstante Abbildung. Es sei $Q \in C$ und $\varphi(Q) = P$. Zeige

$$\operatorname{Verz}(Q|P) = \dim_K(\mathcal{O}_{C,Q}/\mathfrak{m}_P\mathcal{O}_{C,Q}).$$

Aufgabe 13.15.*

Es sei E eine elliptische Kurve über einem algebraisch abgeschlossenen Körper K der Charakteristik $\neq 2$, die affin durch eine Gleichung der Form

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

gegeben ist. Zeige, dass unter der durch X gegebenen Projektion auf die projektive Gerade genau in den Punkten $\mathfrak{O}$, $(\lambda_1, 0)$, $(\lambda_2, 0)$, $(\lambda_3, 0)$ Verzweigung vorliegt.

Aufgabe 13.16. Es seien $R \subseteq S$ und $S \subseteq T$ endliche Erweiterungen von Dedekindbereichen. Es sei $\mathfrak{p}$ ein Primideal von R, das in S verzweigt. Zeige, dass dann $\mathfrak{p}$ auch in T verzweigt.

Aufgabe 13.17. Es sei B ein diskreter Bewertungsring, sei $u \in B^\times$ eine Einheit und sei $X^n - u$ irreduzibel in $B[X]$. Zeige, dass

$$R = B[X]/(X^n - u)$$

normal ist, falls n eine Einheit in B ist.

Aufgabe 13.18. Es sei B ein diskreter Bewertungsring, in dem 2 eine Einheit sei, und sei p eine Ortsuniformisierende von B. Bestimme, für welche m der Ring

$$R = B[X]/\left(X^2 - p^m\right)$$

ein normaler Integritätsbereich ist.

Es sei K ein Körper. Ein Polynom $P \in K[X]$ heißt *separabel*, wenn es über keinem Erweiterungskörper $K \subseteq L$ mehrfache Nullstellen besitzt.

Aufgabe 13.19.*

Es sei K ein Körper und sei $P \in K[X]$ ein Polynom. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) P ist separabel.
(2) Es gibt eine Körpererweiterung $K \subseteq L$ derart, dass P über L in einfache Linearfaktoren zerfällt.
(3) P und die Ableitung P' sind teilerfremd.
(4) P und die Ableitung P' erzeugen das Einheitsideal.

Aufgabe 13.20. Es sei K ein Körper und $P \in K[X]$ ein separables Polynom. Zeige, dass ein Teiler $F \in K[X]$ von P ebenfalls separabel ist.

Die folgenden Aufgaben diskutieren, zunächst auf der Ringebene, wie sich Körperautomorphismen einer Körpererweiterung des Grundkörpers auf Varietäten auswirken.

Aufgabe 13.21. Es sei L ein Körper und sei

$$\varphi\colon L \longrightarrow L$$

ein Körperautomorphismus. Zeige, dass die Abbildung

$$L[X] \longrightarrow L[X],\ \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \varphi(a_i) X^i,$$

ein Ringautomorphismus des Polynomrings $L[X]$ ist.

Aufgabe 13.22. Es sei K ein Körper, $K \subseteq L$ eine Körpererweiterung und $\varphi\colon L \to L$ ein K-Körperautomorphismus. Zeige, dass der Ringautomorphismus $L[X] \to L[X]$ aus Aufgabe 13.21 ein K-Algebraautomorphismus, aber im Allgemeinen kein L-Algebraautomorphismus von $L[X]$ ist.

Aufgabe 13.23. Es sei K ein Körper, $K \subseteq L$ eine Körpererweiterung und $\varphi\colon L \to L$ ein K-Körperautomorphismus. Es sei

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

eine endlich erzeugte kommutative K-Algebra und

$$R_L = R \otimes_K L \cong L[X_1, \ldots, X_n]/\mathfrak{a}L[X_1, \ldots, X_n]$$

die entsprechende L-Algebra.

(1) Zeige, dass durch $\mathrm{Id}_R \otimes \varphi$ ein Ringautomorphismus auf R_L gegeben ist.
(2) Zeige, dass die Abbildung aus (1) ein K-Algebraautomorphismus ist, aber im Allgemeinen kein L-Algebraautomorphismus.
(3) Es sei nun $L = K[T]/(G)$ und $\varphi(T) = P \in K[T]$. Zeige

$$R_L \cong K[T, X_1, \ldots, X_n]/(G, \mathfrak{a})$$

und dass die Abbildung aus (1) der Einsetzungshomomorphismus zu $T \mapsto P, X_i \mapsto X_i$ ist.

Aufgabe 13.24. Es sei K ein Körper, $K \subseteq L$ eine Körpererweiterung und $\varphi\colon L \to L$ ein K-Körperautomorphismus. Es sei $R = K[X_1, \ldots, X_n]$ und $R_L = L[X_1, \ldots, X_n]$, wir bezeichnen

$$\mathrm{Id}_R \otimes \varphi\colon R_L \longrightarrow R_L$$

einfach mit φ. Zeige

$$\varphi^{-1}(X - a_1, \ldots, X - a_n) = (X - \varphi^{-1}(a_1), \ldots, X - \varphi^{-1}(a_n))$$

für $(a_1, \ldots, a_n) \in L^n$.

Die vorstehende Aufgabe bedeutet, dass unter φ L-Punktideale in natürlicher Weise auf Punktideale abgebildet werden. Die entsprechende Abbildung auf dem affinen Raum über L wird mit φ^* bezeichnet, also

$$\varphi^*(a_1, \ldots, a_n) = (\varphi^{-1}(a_1), \ldots, \varphi^{-1}(a_n)).$$

Aufgabe 13.25. Es sei K ein Körper und $K \subseteq L$ eine endliche Galoiserweiterung. Es sei $R = K[X_1, \ldots, X_n]$ und $R_L = L[X_1, \ldots, X_n]$. Zu jedem $\varphi \in \mathrm{Gal}\,(L|K)$ gehört der Ringautomorphismus $\varphi\colon R_L \to R_L$ und $\varphi^*\colon \mathbb{A}_L^n \to \mathbb{A}_L^n$, vergleiche Aufgabe 13.24. Zeige, dass ein Punkt $(a_1, \ldots, a_n) \in L^n$ genau dann zu K^n gehört, wenn er unter allen φ^* zu $\varphi \in \mathrm{Gal}\,(L|K)$ auf sich selbst abgebildet wird.

Aufgabe 13.26.*

Es sei L ein Körper und $\varphi\colon L \to L$ ein Körperautomorphismus. Es sei $\varphi\colon L[X_1, \ldots, X_n] \to L[X_1, \ldots, X_n]$ der zugehörige Ringautomorphismus und $\varphi^*\colon \mathbb{A}_L^n \to \mathbb{A}_L^n$, $(a_1, \ldots, a_n) \mapsto (\varphi^{-1}(a_1), \ldots, \varphi^{-1}(a_n))$, vergleiche Aufgabe 13.24. Es sei $F \in L[X_1, \ldots, X_n]$ ein Polynom. Es sei $P = (a_1, \ldots, a_n) \in L^n$. Zeige $P \in V(\varphi(F))$ genau dann, wenn $\varphi^*(P) \in V(F)$ gilt.

Aufgabe 13.27. Es sei K ein Körper, $K \subseteq L$ eine Körpererweiterung und $\varphi\colon L \to L$ ein K-Körperautomorphismus. Es sei

$$\varphi^*\colon \mathbb{A}_L^n \longrightarrow \mathbb{A}_L^n,\ (a_1, \ldots, a_n) \longmapsto (\varphi^{-1}(a_1), \ldots, \varphi^{-1}(a_n))$$

die zugehörige Abbildung. Es sei $F \in K[X_1, \ldots, X_n]$ ein über K definiertes Polynom. Zeige, dass mit $P = (a_1, \ldots, a_n) \in V(F)$ auch $\varphi^*(P) \in V(F)$ gilt.

Die vorstehende Aufgabe zeigt, dass ein K-Automorphismus auf L einen Automorphismus auf einer über K definierten Hyperfläche $V(F)$ induziert. Das gilt allgemeiner für über K definierte Varietäten und auch für über K definierte projektiven Varietäten.

Aufgabe 13.28. Es sei E eine elliptische Kurve über einem Körper K in kurzer Weierstraßform $Y^2 = X^3 + aX + b$. Es sei $K \subseteq L$ eine Körpererweiterung,

$$\varphi\colon L \longrightarrow L$$

ein K-Automorphismus und $\varphi^*\colon E(L) \to E(L)$ die zugehörige Abbildung auf den L-rationalen Punkten der Kurve. Zeige, dass φ^* ein Gruppenhomomorphismus ist.

Abbildungsverzeichnis