Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Arbeitsblatt 7

Aufgaben

Aufgabe 7.1. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und es sei $R \subseteq L$ ein Unterring mit den folgenden Eigenschaften:

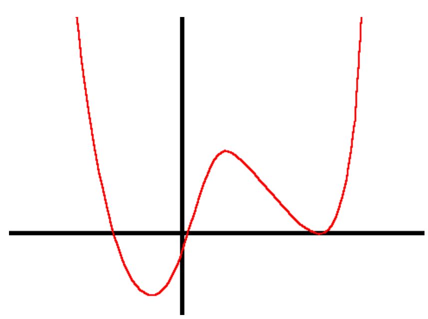
1. R ist ganz über $\mathbb{Z}$.
2. Es ist $Q(R) = L$.
3. R ist normal.

Dann ist R der Ring der ganzen Zahlen von L.

Aufgabe 7.2. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Man gebe Beispiele für Unterringe $R \subseteq L$, die je zwei der folgenden Eigenschaften erfüllen, aber nicht die dritte.

1. R ist ganz über $\mathbb{Z}$.
2. Es ist $Q(R) = L$.
3. R ist normal.

Aufgabe 7.3. Der abgebildete Graph gehört zu einem normierten ganzzahligen Polynom F. Kann $R = \mathbb{Z}[X]/(F)$ ein Zahlbereich sein?



Aufgabe 7.4. Es sei R ein Zahlbereich und es sei $R \subseteq S$ eine endliche Erweiterung von kommutativen Ringen. Es sei S ein normaler Integritätsbereich. Zeige, dass S ebenfalls ein Zahlbereich ist.

Aufgabe 7.5. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und R der zugehörige Zahlbereich. Zeige, dass es eine natürliche Bijektion zwischen Zahlbereichen $\mathbb{Z} \subseteq S \subseteq R$ und Zwischenkörpern $\mathbb{Q} \subseteq K \subseteq L$.

Aufgabe 7.6. Es seien R und S Zahlbereiche. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) R und S sind isomorph.
(2) Es gibt ein $f \in R$ und ein $g \in S$, beide nicht 0, derart, dass die Nenneraufnahmen R_f und S_g zueinander isomorph sind.
(3) Es gibt ein Primideal $\mathfrak{p}$ von R und ein Primideal $\mathfrak{q}$ von S derart, dass die Lokalisierungen $R_{\mathfrak{p}}$ und $S_{\mathfrak{q}}$ zueinander isomorph sind.
(4) Die Quotientenkörper $Q(R)$ und $Q(S)$ sind isomorph.

In den drei folgenden Aufgaben wird der Begriff des primitiven Polynoms verwendet:

Ein Polynom $F \in \mathbb{Z}[X]$ heißt *primitiv*, wenn die Koeffizienten von F teilerfremd sind.

Aufgabe 7.7. Es sei $F \in \mathbb{Z}[X]$ ein Polynom. Zeige, dass man F als $F = n\tilde{F}$ mit $n \in \mathbb{N}$ und primitivem $\tilde{F}$ schreiben kann.

Aufgabe 7.8. Es sei $F \in \mathbb{Z}[X]$ ein irreduzibles Polynom. Dann ist F, aufgefasst als Polynom in $\mathbb{Q}[X]$, ebenfalls irreduzibel.

Aufgabe 7.9. Seien $F, G \in \mathbb{Z}[X]$ primitive Polynome. Zeige, dass dann auch das Produkt FG primitiv ist.

Aufgabe 7.10. Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit dem zugehörigen Primideal

$$\mathfrak{p} = (F) \in \operatorname{Spek}(\mathbb{Q}[X]) \subseteq \operatorname{Spek}(\mathbb{Z}[X]),$$

wobei die letzte Inklusion zur Nenneraufnahme $\mathbb{Z}[X] \to \mathbb{Q}[X]$ im Sinne von Proposition 5.4 (3) gehört. Zeige, dass der Abschluss von $\mathfrak{p}$ in $\operatorname{Spek}(\mathbb{Z}[X])$ gleich $V(\mathfrak{a})$ mit

$$\mathfrak{a} = \{qF \mid q \in \mathbb{Q},\, qF \in \mathbb{Z}[X]\}$$

ist. Zeige ferner, dass zu isomorphen Restekörpern $\kappa(\mathfrak{p}_1)$ und $\kappa(\mathfrak{p}_2)$ die Restklassenringe $R/\mathfrak{a}_1$ und $R/\mathfrak{a}_2$ nicht isomorph sein müssen.

Aufgabe 7.11. Erstelle die Multiplikationsmatrix zum Element $7x^2-4x+5$ in der kubischen Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\big(X^3-6X^2+5X-8\big).$$

Aufgabe 7.12. Erstelle die Multiplikationsmatrix zum Element $7x^2+3x-8$ in der kubischen Körpererweiterung

$$\mathbb{Q} \,=\, \mathbb{Q}[X]/\big(X^3+9X^2-2X+5\big).$$

Aufgabe 7.13.*

Es seien p,q verschiedene Primzahlen und

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p},\sqrt{q}] \,=:\, L$$

die zugehörige Körpererweiterung. Erstelle die Multiplikationsmatrix zu einem Element $a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq} \in L$ bezüglich der Basis $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$.

Aufgabe 7.14. Wir betrachten die quadratische Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] \,=\, L$. Erstelle die Matrix der Multiplikationsabbildung zu $-4+9\sqrt{3}$ bezüglich der $\mathbb{Q}$-Basis $1, \sqrt{3}$ von L.

Aufgabe 7.15. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass die Abbildung

$$L \longrightarrow \operatorname{End}_K(L),\; f \longmapsto \mu_f,$$

ein injektiver Ringhomomorphismus ist.

Aufgabe 7.16. Es sei $K \subseteq M \subseteq L$ eine Körpererweiterung. Es sei $f \in M$ und B die beschreibende Matrix der Multiplikationsabbildung $\mu_f\colon\, M \to M$ bezüglich einer K-Basis von M. Zeige, dass bezüglich einer geeigneten K-Basis von L die Multiplikationsabbildung $\mu_f\colon\, L \to L$ durch eine Blockmatrix der Form

$$\begin{pmatrix} B & 0 & \ldots & 0 \\ 0 & B & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & B \end{pmatrix}$$

beschrieben wird.

Aufgabe 7.17. Zeige, dass die Definition Anhang 6.2 der Spur eines Modulhomomorphismus unabhängig von der gewählten Basis des freien Moduls ist.

Aufgabe 7.18. Es sei K ein Körper und es sei A eine $m \times n$-Matrix und B eine $n \times m$-Matrix über K. Zeige

$$\operatorname{Spur}(A \circ B) \,=\, \operatorname{Spur}(B \circ A).$$

Aufgabe 7.19. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K. Wie findet man die Spur (M) im charakteristischen Polynom χ_M wieder?

Aufgabe 7.20. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K. Wie findet man die Determinante von M im charakteristischen Polynom χ_M wieder?

Aufgabe 7.21. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K mit der Eigenschaft, dass das charakteristische Polynom in Linearfaktoren zerfällt, also

$$\chi_M = (X - \lambda_1)^{\mu_1} \cdot (X - \lambda_2)^{\mu_2} \cdots (X - \lambda_k)^{\mu_k}.$$

Zeige, dass

$$\operatorname{Spur}(M) = \sum_{i=1}^{k} \mu_i \lambda_i$$

ist.

Aufgabe 7.22. Es sei

$$M \in \operatorname{Mat}_n(K)$$

eine Matrix mit n (paarweise) verschiedenen Eigenwerten. Zeige, dass die Spur von M die Summe der Eigenwerte ist.

Aufgabe 7.23. Es sei p eine Primzahl. Betrachte die endliche Körpererweiterung

$$\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(X^3 - p)$$

vom Grad 3. Sei $f = aX^2 + bX + c \in L$ ein Element davon mit $a, b, c \in \mathbb{Q}$. Berechne das Minimalpolynom von f und man gebe die Koeffizienten davon explizit an. Bestimme insbesondere die Norm und die Spur von f.

Welche Bedingungen an a, b, c ergeben sich aus der Voraussetzung, dass f ganz über $\mathbb{Z}$ ist?

Aufgabe 7.24. Bringe für die Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ die Konzepte Norm und Spur mit dem Betrag und dem Realteil einer komplexen Zahl in Verbindung.

Aufgabe 7.25. Berechne für das Element $2 + 4x + 5x^2$ in der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\big(X^3 - 3X + 1\big) =: L$$

die Norm und die Spur.

AUFGABE 7.26. Es sei $K \subseteq M \subseteq L$ eine Kette von quadratischen Körpererweiterungen. Zeige, dass für die Normen die Beziehung
$$N_K^L = N_K^M \circ N_M^L$$
gilt.

AUFGABE 7.27.*

Bestimme für sämtliche Elemente der Körpererweiterung
$$\mathbb{Z}/(2) \subseteq \mathbb{Z}/(2)[X]/\big(X^2 + X + 1\big)$$
die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

AUFGABE 7.28. Bestimme für sämtliche Elemente der Körpererweiterung
$$\mathbb{Z}/(3) \subseteq \mathbb{Z}/(3)[X]/\big(X^2 - 2\big)$$
die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

AUFGABE 7.29.*

Es sei $K \subseteq L$ eine endliche Körpererweiterung und $f \in L$. Zeige, dass es für die Eigenwerttheorie der K-linearen Multiplikationsabbildung
$$\mu_f \colon L \longrightarrow L$$
grundsätzlich nur zwei Möglichkeiten gibt.

AUFGABE 7.30. Sei K ein Körper und sei $P = X^n - c \in K[X]$ ein irreduzibles Polynom. Es sei
$$f = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$$
ein Element in der einfachen endlichen Körpererweiterung $K \subseteq L = K[X]/(P)$ vom Grad n. Zeige, dass die Spur von f gleich na_0 ist.

AUFGABE 7.31. Sei p eine Primzahl und sei
$$L = \mathbb{Q}[X]/\big(X^3 - p\big)$$
der durch das irreduzible Polynom $X^3 - p$ definierte Erweiterungskörper von $\mathbb{Q}$. Es sei
$$f = 2 + 3x - 4x^2 .$$

(1) Finde die Matrix bezüglich der $\mathbb{Q}$-Basis $1, x, x^2$ von L der durch die Multiplikation mit f definierten $\mathbb{Q}$-linearen Abbildung.
(2) Berechne die Norm und die Spur von f.

(3) Bestimme das Minimalpolynom von f.
(4) Finde das Inverse von f.
(5) Berechne die Diskriminante der Basis $1, f, f^2$.

Aufgabe 7.32. Es sei $K \subseteq L$ eine Körpererweiterung, $f \in L$ und $M = K[f]$. Zeige, dass das charakteristische Polynom der Multiplikationsabbildung

$$\mu_f \colon L \longrightarrow L$$

eine Potenz des Minimalpolynoms von f ist.

Aufgabe 7.33. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und sei

$$\rho \colon L \longrightarrow \mathbb{C}$$

ein Ringhomomorphismus. Zeige, dass für jeden Körperautomorphismus

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

auch $\rho \circ \varphi$ ein Ringhomomorphismus nach $\mathbb{C}$ ist, und dass daher die Galoisgruppe von L auf der Menge der komplexen Einbettungen von L operiert.

Aufgabe 7.34. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Zeige, dass genau dann eine Galoiserweiterung vorliegt, wenn die Bildkörper unter allen komplexen Einbettungen von L übereinstimmen.

Aufgabe 7.35. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a genau dann eine mehrfache Nullstelle von F ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

Abbildungsverzeichnis