Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

Körper- und Galoistheorie

Arbeitsblatt 7

Aufwärmaufgaben

Aufgabe 7.1. Sei R ein kommutativer Ring und $p \in R$, $p \neq 0$. Zeige, dass p genau dann ein Primelement ist, wenn der Restklassenring $R/(p)$ ein Integritätsbereich ist.

Aufgabe 7.2. Sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zeige, dass ein Element $f \in R$ genau dann eine Einheit in S ist, wenn in R das Ideal $\mathfrak{a}$ zusammen mit f das Einheitsideal erzeugt.

Aufgabe 7.3. Sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zeige, dass die Ideale von S eindeutig denjenigen Idealen von R entsprechen, die $\mathfrak{a}$ umfassen.

Aufgabe 7.4. Sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zu einem Ideal $I \subseteq R$ welches $\mathfrak{a}$ enthält, sei $I' = IR/\mathfrak{a}$ das zugehörige Ideal in S. Zeige, dass es eine kanonische Ringisomorphie

$$R/I \cong S/I'$$

gibt.

Aufgabe 7.5. Wende Satz 7.5 auf den kanonischen Ringhomomorphismus $\mathbb{Z} \to R$ zu einem kommutativen Ring R an.

Aufgabe 7.6. Es sei K ein Körper, A eine K-Algebra mit einem Element $f \in A$. Wende Satz 7.5 auf den zugehörigen Einsetzungshomomorphismus $K[X] \to A$, $X \mapsto f$, an.

Aufgabe 7.7. Zeige, dass die komplexen Zahlen $\mathbb{C}$ die Restklassendarstellung

$$\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$$

besitzen.

Aufgabe 7.8. Sei X ein topologischer Raum und $R = \mathrm{C}^0(X, \mathbb{R})$ der Ring der stetigen Funktionen auf X. Es sei $T \subseteq X$ eine Teilmenge. Zeige, dass die Teilmenge

$$I = \{f \in R \mid f|_T = 0\}$$

ein Ideal in R ist. Definiere einen Ringhomomorphismus $R/I \to \mathrm{C}^0(T, \mathbb{R})$. Ist dieser immer injektiv? Surjektiv?

Aufgabe 7.9. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(7)$.

Aufgabe 7.10.*

Berechne 3^{1457} in $\mathbb{Z}/(13)$.

Aufgabe 7.11. Sei p eine Primzahl. Beweise durch Induktion den kleinen Fermat, also die Aussage, dass $a^p - a$ ein Vielfaches von p für jede ganze Zahl a ist.

Aufgabe 7.12. Bestimme im Polynomring $\mathbb{F}_5[X]$ alle irreduziblen Polynome vom Grad 3.

Aufgabe 7.13. Bestimme die fünf kleinsten Primzahlen p mit der Eigenschaft, dass das Polynom $X^6 - 1$ über $\mathbb{Z}/(p)$ in Linearfaktoren zerfällt.

Aufgabe 7.14.*

Betrachte den Körper $K = \mathbb{F}_4 = \mathbb{Z}/(2)[U]/(U^2 + U + 1)$. Führe im Polynomring $K[X]$ die Polynomdivision

$$X^4 + uX^3 + (u + 1)X + 1 \text{ durch } uX^2 + X + u + 1$$

aus, wobei u die Restklasse von U in K bezeichnet.

Aufgabe 7.15. a) Bestimme die Primfaktorzerlegung des Polynoms $F = X^3 + X + 2$ in $\mathbb{Z}/(5)[X]$.

b) Zeige, dass durch

$$K = \mathbb{Z}/(5)[T]/(T^2 - 2)$$

ein Körper mit 25 Elementen gegeben ist.

c) Bestimmen die Primfaktorzerlegung von $F = X^3 + X + 2$ über $K = \mathbb{Z}/(5)[T]/(T^2 - 2)$.

Aufgabe 7.16.*

Sei p eine Primzahl und sei $f(x)$ ein Polynom mit Koeffizienten in $\mathbb{Z}/(p)$ vom Grad $d \geq p$. Zeige, dass es ein Polynom $g(x)$ mit einem Grad $< p$ derart gibt, dass für alle Elemente $a \in \mathbb{Z}/(p)$ die Gleichheit

$$f(a) = g(a)$$

gilt.

Aufgabe 7.17.*

Es sei R ein kommutativer Ring und $R[X]$ der Polynomring über R. Es sei $\mathfrak{a} \subseteq R[X]$ ein Ideal mit Erzeugern

$$\mathfrak{a} = (F_0, F_1, \ldots, F_n),$$

wobei $F_0 = X - r$ mit $r \in R$ sei. Für $i \geq 1$ seien G_i die Elemente aus R, die entstehen, wenn man in F_i die Variable X durch r ersetzt. Zeige, dass eine Ringisomorphie der Restklassenringe

$$R[X]/\mathfrak{a} \cong R/(G_1, \ldots, G_n)$$

vorliegt.

Aufgabe 7.18.*

Bestimme in $\mathbb{Q}[X]/(X^3 + 4X^2 - 7)$ das Inverse von $\frac{1}{3}x + 5$ (x bezeichnet die Restklasse von X).

Aufgabe 7.19.*

Bestimme in $\mathbb{Q}[X]/(X^3 - 7)$ das Inverse von $3x + 4$ (x bezeichnet die Restklasse von X).

Aufgabe 7.20. Bestimme das Inverse von

$$1 + \sqrt{2} + 3\sqrt{10}$$

im Körper $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$.

Aufgabe 7.21. Sei p eine Primzahl.

a) Zeige, dass das Polynom $X^4 - p$ irreduzibel über $\mathbb{Q}$ ist.

b) Schließe daraus, dass

$$\mathbb{Q}[\sqrt[4]{p}] \subseteq \mathbb{R}$$

über $\mathbb{Q}$ den Grad vier besitzt.

c) Finde einen echten Zwischenkörper

$$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}[\sqrt[4]{p}].$$

Aufgabe 7.22. Zeige, dass die Abbildung

$$\mathbb{Q}[\mathrm{i}]^\times \longrightarrow (\mathbb{Q}_+, 1, \cdot),\ z = x + \mathrm{i}y \longmapsto |z|^2 = x^2 + y^2,$$

ein Gruppenhomomorphismus ist.

Aufgabe 7.23. Zeige, dass die Menge

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

mit der Multiplikation in $\mathbb{Q}[\mathrm{i}]$ eine kommutative Gruppe ist.

Aufgabe 7.24. Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Berechne die ersten vier Potenzen von $\frac{3}{5} + \frac{4}{5}\mathrm{i} \in S^1_{\mathbb{Q}}$.

Aufgaben zum Abgeben

Aufgabe 7.25. (3 Punkte)

Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 7.26. (5 Punkte)

Bestimme im Polynomring $\mathbb{Z}/(3)[X]$ alle irreduziblen Polynome vom Grad 4.

Aufgabe 7.27. (4 Punkte)

Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Zeige, dass die Gruppen $S^1_{\mathbb{Q}}$ und $\mathbb{Q}/\mathbb{Z}$ nicht isomorph sind.

Aufgabe 7.28. (5 Punkte)

Zeige, dass der Gruppenhomomorphismus

$$\mathbb{Q}[\mathrm{i}]^\times \longrightarrow (\mathbb{Q}_+, 1, \cdot),\ x + \mathrm{i}y \longmapsto x^2 + y^2,$$

nicht surjektiv ist.

Aufgabe 7.29. (5 (1+1+2+1) Punkte)

Betrachte den Körper $\mathbb{Z}/(13) = \{0, 1, 2, ..., 12\}$ mit 13 Elementen.

(1) Zeige, dass 5 kein Quadrat in $\mathbb{Z}/(13)$ ist und folgere, dass

$$\mathbb{Z}/(13)[X]/(X^2 - 5) =: \mathbb{Z}/(13)[\sqrt{5}]$$

ein Körper ist.

(2) Betrachte die quadratische Körpererweiterung

$$\mathbb{Z}/(13) \subset \mathbb{Z}/(13)[\sqrt{5}]$$

und berechne

$$(2 + 3\sqrt{5})(1 + 11\sqrt{5})(10 + 7\sqrt{5})$$

(3) Finde das Inverse zu $7 + 3\sqrt{5}$ in $\mathbb{Z}/(13)[\sqrt{5}]$.

(4) Zeige, dass -5 kein Quadrat in $\mathbb{Z}/(13)$ ist, dafür aber in $\mathbb{Z}/(13)[\sqrt{5}]$.

Aufgabe 7.30. (4 Punkte)

Bestimme das Inverse von

$$2 + 3\sqrt{5} + \sqrt{7} + 3\sqrt{35}$$

im Körper $\mathbb{Q}[\sqrt{5}, \sqrt{7}]$.

Aufgabe 7.31. (4 Punkte)

Bestimme das Minimalpolynom von

$$\sqrt{3} + \sqrt{5}$$

über $\mathbb{Q}$.

Abbildungsverzeichnis