

Elemente der Algebra**Arbeitsblatt 15****Übungsaufgaben**

AUFGABE 15.1. Bestätige den kleinen Fermat direkt für die Primzahlen $p = 2, 3, 5, 7, 11$.

AUFGABE 15.2. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(7)$.

AUFGABE 15.3.*

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

AUFGABE 15.4. Finde einen Restklassenring $\mathbb{Z}/(n)$ derart, dass die Einheitengruppe davon nicht zyklisch ist.

AUFGABE 15.5. Konstruiere endliche Körper mit 4, 8, 9, 16, 25, 27, 32 und 49 Elementen.

AUFGABE 15.6.*

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 15.7. Sei $f(x) = x^7 + 2x^3 + 3x + 4 \in (\mathbb{Z}/(5))[x]$. Finde ein Polynom $g(x) \in (\mathbb{Z}/(5))[x]$ vom Grad < 5 , das für alle Elemente aus $\mathbb{Z}/(5)$ mit $f(x)$ übereinstimmt.

2

AUFGABE 15.8.*

a) Zeige, dass durch

$$K = \mathbb{Z}/(7)[T]/(T^3 - 2)$$

ein Körper mit 343 Elementen gegeben ist.

b) Berechne in K das Produkt $(T^2 + 2T + 4)(2T^2 + 5)$.

c) Berechne das (multiplikativ) Inverse zu $T + 1$.

AUFGABE 15.9. Zeige, dass $\mathbb{Q}[X]/(X^3 - 2)$ ein Körper ist und bestimme das Inverse von $4x^2 - 2x + 5$, wobei x die Restklasse von X bezeichne.

AUFGABE 15.10. Man gebe einen Restklassenring $\mathbb{Z}/(d)$ an, in dem es nicht-triviale idempotente Elemente gibt.

AUFGABE 15.11. Finde in $\mathbb{Q}[X]/(X^2 - 1)$ nichttriviale idempotente Elemente.

AUFGABE 15.12. Sei R ein kommutativer Ring und sei $f \in R$. Es sei f sowohl nilpotent als auch idempotent. Zeige, dass $f = 0$ ist.

AUFGABE 15.13. Seien R und S kommutative Ringe und sei $R \times S$ der Produktring $R \times S$. Zeige, dass die Teilmenge $R \times 0$ ein Hauptideal ist.

AUFGABE 15.14. Sei R ein faktorieller Bereich und $p \in R$ ein Primelement. Zeige, dass der Restklassenring $R/(p^n)$ nur die beiden trivialen idempotenten Elemente 0 und 1 besitzt.

AUFGABE 15.15. Seien R ein kommutativer Ring und I, J Ideale in R . Sei weiter

$$\varphi: R \longrightarrow R/I \times R/J, r \longmapsto (r + I, r + J).$$

Zeige, dass φ genau dann surjektiv ist, wenn $I + J = R$ gilt. Wie sieht $\ker \varphi$ aus? Benutze jetzt den Homomorphiesatz um einzusehen, was das im Falle $R = \mathbb{Z}$ mit dem chinesischen Restsatz zu tun hat.

AUFGABE 15.16. Sei R ein kommutativer Ring und seien $I, J \subseteq R$ Ideale. Wir betrachten die Gruppenhomomorphismen

$$\varphi: R/I \cap J \longrightarrow R/I \times R/J, r \longmapsto (r, r),$$

und

$$\psi: R/I \times R/J \longrightarrow R/I + J, (s, t) \longmapsto s - t.$$

Zeige, dass φ injektiv ist, dass ψ surjektiv ist und dass

$$\text{bild } \varphi = \text{kern } \psi$$

ist. Sind φ und ψ Ringhomomorphismen?

AUFGABE 15.17. Sei K ein Körper und sei $K[X]$ der Polynomring über K . Es seien $a_1, \dots, a_n \in K$ 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 15.18.*

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 15.19.*

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

AUFGABE 15.20. Zeige, dass jeder echte Restklassenring von $\mathbb{C}[X]$ isomorph zu einem Produktring der Form

$$\begin{aligned} \mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{C}[X]/(X^2) \times \cdots \times \mathbb{C}[X]/(X^2) \times \mathbb{C}[X]/(X^3) \times \cdots \\ \times \mathbb{C}[X]/(X^3) \times \cdots \times \mathbb{C}[X]/(X^m) \times \cdots \times \mathbb{C}[X]/(X^m) \end{aligned}$$

ist.

AUFGABE 15.21. Realisiere den Produktring

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

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

AUFGABE 15.22.*

Es seien R_1, R_2, \dots, R_n kommutative Ringe und sei

$$R = R_1 \times R_2 \times \cdots \times R_n$$

der Produktring.

(1) Es seien

$$I_1 \subseteq R_1, I_2 \subseteq R_2, \dots, I_n \subseteq R_n$$

Ideale. Zeige, dass die Produktmenge

$$I_1 \times I_2 \times \cdots \times I_n$$

ein Ideal in R ist.

(2) Zeige, dass jedes Ideal $I \subseteq R$ die Form

$$I = I_1 \times I_2 \times \cdots \times I_n$$

mit Idealen $I_j \subseteq R_j$ besitzt.

(3) Sei

$$I = I_1 \times I_2 \times \cdots \times I_n$$

ein Ideal in R . Zeige, dass I genau dann ein Hauptideal ist, wenn sämtliche I_j Hauptideale sind.

(4) Zeige, dass R genau dann ein Hauptidealring ist, wenn alle R_j Hauptidealringe sind.

Aufgaben zum Abgeben

AUFGABE 15.23. (3 Punkte)

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

AUFGABE 15.24. (3 Punkte)

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 15.25. (4 Punkte)

Zeige, dass $\mathbb{Q}[X]/(X^3 - 5)$ ein Körper ist und bestimme das Inverse von $5x^2 - x + 7$, wobei x die Restklasse von X bezeichne.

AUFGABE 15.26. (4 Punkte)

Sei R ein kommutativer Ring und sei $e \in R$ ein idempotentes Element. Zeige, dass auch $1 - e$ idempotent ist und dass die „zusammengesetzte“ Restklassenabbildung

$$R \longrightarrow R/(e) \times R/(1 - e)$$

eine Bijektion ist.

Der folgende Satz heißt *Satz von Wilson*.

Sei p eine Primzahl. Dann ist

$$(p - 1)! = -1 \pmod{p}.$$

AUFGABE 15.27. (4 Punkte)

Bestimme die Zerlegung von $X^{p-1} - 1$ in irreduzible Polynome im Polynomring $\mathbb{Z}/(p)[X]$. Beweise aus dieser Zerlegung den Satz von Wilson.