Prof. Dr. H. Brenner Osnabrück WS 2016/2017

# Zahlentheorie

## Arbeitsblatt 16

### Übungsaufgaben

Aufgabe 16.1. Berechne die Diskriminante zur Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}]$$

zur Basis 1 und i und zur Basis $2 - 5\mathrm{i}$ und $4 + 7\mathrm{i}$.

Aufgabe 16.2.*

Berechne explizit die Diskriminante des quadratischen Zahlbereichs $A_{-7}$. Stelle die Multiplikationsmatrix bezüglich einer geeigneten Basis für das Element

$$f = \frac{3}{2} + \frac{5}{2}\sqrt{-7}$$

auf und berechne damit die Spur und die Norm von $f$.

Aufgabe 16.3. Beweise Lemma 16.6 unter der zusätzlichen Voraussetzung, dass $L$ von $z$ erzeugt wird.

Aufgabe 16.4. Sei $G$ eine kommutative Gruppe. Zeige, dass $G$ auf genau eine Weise die Struktur eines $\mathbb{Z}$-Moduls trägt. Kommutative Gruppen und $\mathbb{Z}$-Moduln sind also äquivalente Objekte.

Aufgabe 16.5. Seien $R$ und $A$ kommutative Ringe. Zeige, dass $A$ eine $R$-Algebra ist genau dann, wenn $A$ ein $R$-Modul ist, für den zusätzlich gilt

$$r(ab) = (ra)b \text{ für alle } r \in R,\ a, b \in A\,.$$

Aufgabe 16.6. Sei $\mathfrak{a}$ ein Ideal in einem kommutativen Ring $R$. Zeige, dass $\mathfrak{a}$ genau dann ein Primideal ist, wenn $\mathfrak{a}$ der Kern eines Ringhomomorphismus $\varphi\colon R \rightarrow K$ in einen Körper $K$ ist.

Aufgabe 16.7. Zeige, dass jeder Restklassenring eines Hauptidealringes wieder ein Hauptidealring ist. Man gebe ein Beispiel, dass ein Restklassenring eines Hauptidealbereiches kein Hauptidealbereich sein muss.

Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring $R$ heißt *Radikal* (oder *Radikalideal*), wenn folgendes gilt: Falls $f^n \in \mathfrak{a}$ ist für ein $n \in \mathbb{N}$, so ist bereits $f \in \mathfrak{a}$.

Aufgabe 16.8. Zeige, dass ein Primideal ein Radikal ist.

Aufgabe 16.9. Zeige, dass ein Ideal $\mathfrak{a}$ in einem kommutativen Ring $R$ genau dann ein Radikal ist, wenn der Restklassenring $R/\mathfrak{a}$ reduziert ist.

Sei $R$ ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann nennt man die Menge

$$\{f \in R | \text{ es gibt ein } r \text{ mit } f^r \in \mathfrak{a}\}$$

das *Radikal* zu $\mathfrak{a}$. Es wird mit $\operatorname{rad}(\mathfrak{a})$ bezeichnet.

Aufgabe 16.10. Bestimme in $\mathbb{Z}$ das Radikal zum Ideal $\mathbb{Z}27$.

Aufgabe 16.11. Es sei $R$ ein kommutativer Ring und $S \subseteq R$ ein Unterring. Bestätige oder widerlege die folgenden Aussagen.

(1) Zu einem Ideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Ideal (in $S$).
(2) Zu einem Radikal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Radikal.
(3) Zu einem Primideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Primideal.
(4) Zu einem maximalen Ideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein maximales Ideal.

## Aufgaben zum Abgeben

Aufgabe 16.12. (3 Punkte)

Sei $(G, +, 0)$ eine kommutative Gruppe. Sei

$$E := \operatorname{End}(G) = \operatorname{Hom}(G, G)$$

die Menge der Gruppenhomomorphismen von $G$ nach $G$ (also die Gruppenendomorphismen auf $G$). Definiere auf $E$ eine Addition und eine Multiplikation, so dass $E$ zu einem (in der Regel nicht kommutativen) Ring wird.

Aufgabe 16.13. (3 Punkte)

Sei $(M, +, 0)$ eine kommutative Gruppe und sei $E = \operatorname{End}_{\mathbb{Z}}(M)$ der zugehörige Endomorphismenring. Sei $R$ ein kommutativer Ring. Zeige, dass eine $R$-Modulstruktur auf $M$ äquivalent ist zu einem Ringhomomorphismus $R \to \operatorname{End}_{\mathbb{Z}}(M)$.

Aufgabe 16.14. (4 Punkte)

Seien $R$ und $S$ kommutative Ringe und sei $\varphi : R \to S$ ein Ringhomomorphismus. Sei $\mathfrak{p}$ ein Primideal in $S$. Zeige, dass das Urbild $\varphi^{-1}(\mathfrak{p})$ ein Primideal in $R$ ist.

Zeige durch ein Beispiel, dass das Urbild eines maximalen Ideales kein maximales Ideal sein muss.

Aufgabe 16.15. (3 Punkte)

Sei $R$ ein kommutativer Ring und sei $\mathfrak{a} \neq R$ ein Ideal in $R$. Zeige: $\mathfrak{a}$ ist genau dann ein maximales Ideal, wenn es zu jedem $g \in R$, $g \notin \mathfrak{a}$, ein $f \in \mathfrak{a}$ und ein $r \in R$ gibt mit $rg + f = 1$.