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

Zahlentheorie

Arbeitsblatt 18

Übungsaufgaben

Aufgabe 18.1. 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 18.2. Es sei R ein kommutativer Ring und

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

eine (als Algebra) endlich erzeugte R-Algebra, die ganz über R sei. Zeige, dass S ein endlich erzeugter R-Modul ist.

Aufgabe 18.3. 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 18.4. Sei R ein Zahlbereich und sei $f \in R$. Zeige, dass $N(f) \in (f)$ ist, dass also die Norm zum von f erzeugten Hauptideal gehört. Zeige durch ein Beispiel, dass dies für die Spur nicht gelten muss.

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

Aufgabe 18.6. Sei $F \in \mathbb{Z}[X]$ ein irreduzibles Polynom. Dann ist F, aufgefasst als Polynom in $\mathbb{Q}[X]$, ebenfalls irreduzibel.

Aufgabe 18.7. Seien $F, G \in \mathbb{Z}[X]$ primitive Polynome. Zeige, dass dann auch das Produkt FG primitiv ist.

Aufgabe 18.8. Es sei R ein faktorieller Zahlbereich und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung. Zu einer Primzahl p sei

$$p = q_1^{r_1} \cdots q_k^{r_k}$$

die Primfaktorzerlegung von p in R (die q_i seien also paarweise nicht assoziiert). Zeige, dass die Primideale $\mathfrak{p}$ von R mit der Eigenschaft $\mathfrak{p} \cap \mathbb{Z} = (p)$ genau die Primideale der Form $\mathfrak{p} = (q_i)$ sind.

Aufgabe 18.9. Sei R ein Zahlbereich und sei $f_1, \ldots, f_n \in R$ eine $\mathbb{Z}$-Basis von R. Zeige, dass dann der Betrag der Diskriminante

$$|\triangle(f_1, \ldots, f_n)|$$

minimal ist unter allen Diskriminanten von linear unabhängigen n-Tupeln aus R.

Aufgabe 18.10. Berechne die Diskriminante der Gaußschen Zahlen. Man gebe zwei wesentlich verschiedene $\mathbb{Z}$-Basen von $\mathbb{Z}[i]$ an und überprüfe, dass die Diskriminanten übereinstimmen.

Aufgabe 18.11. Man gebe ein Beispiel für einen Dedekindbereich, wo jeder Restklassenring $\neq 0$ unendlich ist, und für einen Dedekindbereich, der einen Körper enthält und wo alle echten Restklassenringe endlich sind.

Aufgabe 18.12. Sei R ein noetherscher, kommutativer Ring. Zeige, dass dann auch jeder Restklassenring $R/\mathfrak{a}$ noethersch ist.

Aufgabe 18.13. Sei K ein Körper und sei

$$K[X_n,\, n \in \mathbb{N}]$$

der Polynomring über K in unendlich vielen Variablen. Man beschreibe darin ein nicht endlich erzeugtes Ideal und eine unendliche, echt aufsteigende Idealkette.

Die folgenden Aufgaben benutzen das Produkt von Idealen.

Zu zwei Idealen $\mathfrak{a}$ und $\mathfrak{b}$ in einem kommutativen Ring wird das *Produkt* durch

$$\mathfrak{a}\mathfrak{b} = \{a_1 b_1 + a_2 b_2 + \cdots + a_k b_k\}$$

mit $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ definiert. Das ist das Ideal, das von allen Produkten ab (mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$) erzeugt wird.

Für das n-fache Produkt eines Ideals $\mathfrak{a}$ mit sich selbst schreibt man $\mathfrak{a}^n$.

Aufgabe 18.14. Zeige, dass das Produkt von Hauptidealen wieder ein Hauptideal ist.

Aufgabe 18.15. Es seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale in einem kommutativen Ring R. Zeige, dass die Beziehung

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$$

gilt.

Aufgabe 18.16. Es sei $\mathfrak{a} \subseteq R$ ein Ideal in einem kommutativen Ring R. Zeige, dass die Potenzen $\mathfrak{a}^n$, $n \in \mathbb{N}_+$, alle dasselbe Radikal besitzen.

Aufgabe 18.17.*

Es seien I und J Ideale in einem kommutativen Ring R und sei $n \in \mathbb{N}$. Zeige die Gleichheit

$$(I + J)^n = I^n + I^{n-1}J + I^{n-2}J^2 + \cdots + I^2 J^{n-2} + I J^{n-1} + J^n.$$

Aufgaben zum Abgeben

Aufgabe 18.18. (5 Punkte)

Sei $R = \mathbb{Z}[X]/(X^4 + X^3 + X^2 + X + 1)$. Bestimme die Primideale in R, die über den Primzahlen $p = 2, 3, 5, 7$ liegen.

Aufgabe 18.19. (3 Punkte)

Sei p eine Primzahl und betrachte die Körpererweiterung

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

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 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 18.20. (3 Punkte)

Sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ verschiedene Primideale $\neq 0$. Dann gibt es einen Ringisomorphismus

$$R/\mathfrak{p} \cap \mathfrak{q} \longrightarrow R/\mathfrak{p} \times R/\mathfrak{q}.$$

Aufgabe 18.21. (4 Punkte)

Sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ zwei verschiedene Primideale. Dann ist

$$\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p} \cdot \mathfrak{q}.$$

Aufgabe 18.22. (4 Punkte)

Zeige: Ein kommutativer Ring R ist noethersch genau dann, wenn es in R keine unendliche echt aufsteigende Idealkette

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \ldots$$

gibt.