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

Algebraische Zahlentheorie

Arbeitsblatt 2

Übungsaufgaben

Zwei Elemente a und b eines kommutativen Ringes R heißen *assoziiert*, wenn es eine Einheit $u \in R$ derart gibt, dass $a = ub$ ist.

Aufgabe 2.1. Zeige, dass die Assoziiertheit in einem kommutativen Ring eine Äquivalenzrelation ist.

Aufgabe 2.2. Beweise die folgenden Eigenschaften zur Teilbarkeit in einem kommutativen Ring R

(1) Für jedes Element a gilt $1|a$ und $a|a$.
(2) Für jedes Element a gilt $a|0$.
(3) Gilt $a|b$ und $b|c$, so gilt auch $a|c$.
(4) Gilt $a|b$ und $c|d$, so gilt auch $ac|bd$.
(5) Gilt $a|b$, so gilt auch $ac|bc$ für jedes $c \in R$.
(6) Gilt $a|b$ und $a|c$, so gilt auch $a|rb+sc$ für beliebige Elemente $r, s \in R$.

Aufgabe 2.3. Zeige, dass in einem kommutativen Ring R folgende Teilbarkeitsbeziehungen gelten.

(1) Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.
(2) Ist R ein Integritätsbereich, so gilt hiervon auch die Umkehrung.

Aufgabe 2.4. Zeige, dass in einem kommutativen Ring R folgende Teilbarkeitsbeziehungen gelten.

(1) -1 ist eine Einheit, die zu sich selbst invers ist.
(2) Jede Einheit teilt jedes Element.
(3) Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.
(4) Teilt a eine Einheit, so ist a selbst eine Einheit.

Aufgabe 2.5. Zeige, dass ein Unterring eines Körpers ein Integritätsbereich ist.

Aufgabe 2.6. Es sei R ein kommutativer Ring und seien f, g Nichtnullteiler in R. Zeige, dass das Produkt fg ebenfalls ein Nichtnullteiler ist.

Aufgabe 2.7. Was bedeutet die Eigenschaft, dass man in einem Integritätsbereich „kürzen“ kann? Beweise diese Eigenschaft.

Aufgabe 2.8.*

Es sei R ein kommutativer Ring. Zu jedem $f \in R$ sei

$$\mu_f \colon R \longrightarrow R, \, g \longmapsto fg,$$

die Multiplikation mit f. Zeige, dass μ_f genau dann bijektiv ist, wenn es surjektiv ist.

Man zeige durch ein Beispiel, dass in dieser Situation aus der Injektivität nicht die Bijektivität folgt.

Aufgabe 2.9.*

Es sei R ein kommutativer Ring und $f \in R$. Charakterisiere mit Hilfe der Multiplikationsabbildung

$$\mu_f \colon R \longrightarrow R, \, g \longmapsto fg,$$

wann f ein Nichtnullteiler und wann f eine Einheit ist.

Aufgabe 2.10. Zeige, dass $\mathbb{Z} \subseteq \mathbb{Q}$ eine Untergruppe, aber kein Ideal ist.

Aufgabe 2.11.*

Zeige, dass ein kommutativer Ring genau dann ein Körper ist, wenn er genau zwei Ideale enthält.

Aufgabe 2.12. Sei R ein kommutativer Ring und sei f_j, $j \in J$, eine Familie von Elementen in R. Es sei angenommen, dass die f_j zusammen das Einheitsideal erzeugen. Zeige, dass es eine endliche Teilfamilie f_j, $j \in J_0 \subseteq J$ gibt, die ebenfalls das Einheitsideal erzeugt.

Aufgabe 2.13. Sei R ein kommutativer Ring und sei

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

eine aufsteigende Kette von Idealen. Zeige, dass die Vereinigung $\bigcup_{n \in \mathbb{N}} \mathfrak{a}_n$ ebenfalls ein Ideal ist. Zeige durch ein einfaches Beispiel, dass die Vereinigung von Idealen im Allgemeinen kein Ideal sein muss.

Aufgabe 2.14. Sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Zeige, dass p genau dann irreduzibel ist, wenn es genau zwei Hauptideale oberhalb von (p) gibt, nämlich (p) selbst und $(1) = R$.

Aufgabe 2.15. Zeige, dass im Polynomring $K[X]$ über einem Körper K die Variable X irreduzibel und prim ist.

Aufgabe 2.16. Bestimme im Polynomring $K[X]$, wobei K ein Körper sei, die Einheiten und die Assoziiertheit. Gibt es in den Assoziiertheitsklassen besonders schöne Vertreter?

Aufgabe 2.17. Beweise die Formel

$$X^u + 1 = (X+1)\big(X^{u-1} - X^{u-2} + X^{u-3} - \cdots + X^2 - X + 1\big)$$

für u ungerade.

Aufgabe 2.18.*

Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass ein Polynom vom Grad zwei oder drei genau dann irreduzibel ist, wenn es keine Nullstelle in K besitzt.

Aufgabe 2.19.*

Bestimme die Primfaktorzerlegung des Polynoms $X^6 - 1$ über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(7)$ und $\mathbb{Z}/(5)$.

Aufgabe 2.20. Man wende eine Form des Eisensteinkriteriums an, um die Irreduzibilität der folgenden Polynome aus $\mathbb{Q}[X]$ nachzuweisen.

(1) $X^4 + 2X^2 + 2$,
(2) $20X^5 - 15X^4 + 125X^3 - 10X + 4$,
(3) $X^4 + 9$.

Aufgabe 2.21. Bestimme im Polynomring $\mathbb{Z}/(2)[X]$ alle irreduziblen Polynome vom Grad $2, 3, 4$.

Aufgabe 2.22. Bestimme im Polynomring $\mathbb{Z}/(3)[X]$ alle normierten irreduziblen Polynome vom Grad 3.

Aufgabe 2.23. Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3. Zeige, dass F entweder eine oder drei reelle Nullstellen besitzt.

Aufgabe 2.24. Zeige, dass ein reelles Polynom von ungeradem Grad nicht irreduzibel ist.

Aufgabe 2.25.*

Zeige, dass das Polynom

$$X^3 - 3X + 1$$

über $\mathbb{Q}$ irreduzibel ist.

Aufgabe 2.26.*

Zeige, dass das Polynom

$$X^3 - 3X - 1$$

über $\mathbb{Q}$ irreduzibel ist.

Aufgabe 2.27. Es sei K ein Körper und sei $F \in K[X]$ ein von 0 verschiedenes Polynom. Zeige, dass es eine (bis auf die Reihenfolge der Faktoren) eindeutige Produktdarstellung

$$F = aF_1 \cdots F_r$$

mit $a \in K^\times$ und irreduziblen normierten Polynomen F_i, $i = 1, \ldots, r$, gibt.

Aufgabe 2.28.*

Es sei K ein Körper und sei $K[X]$ der Polynomring über K und sei $P \in K[X]$ ein Polynom, das eine Zerlegung in Linearfaktoren besitze. Es sei T ein Teiler von P. Zeige, dass T ebenfalls eine Zerlegung in Linearfaktoren besitzt, wobei die Vielfachheit eines Linearfaktors $X - a$ in T durch seine Vielfachheit in P beschränkt ist.

Aufgabe 2.29.*

(1) Es sei F ein normiertes Polynom aus $\mathbb{Z}[X]$ und es gebe eine Primzahl q mit der Eigenschaft, dass F modulo q, also aufgefasst in $\mathbb{Z}/(q)[X]$, irreduzibel sei. Zeige, dass dann schon F irreduzibel ist.
(2) Zeige, dass die erste Aussage für ein nichtnormiertes Polynom nicht stimmen muss.
(3) Es sei p eine Primzahl und $G \in \mathbb{Z}/(p)[X]$ ein normiertes Polynom. Zeige, dass es ein normiertes Polynom $F \in \mathbb{Z}[X]$ gibt, das modulo p mit G übereinstimmt und das zusätzlich irreduzibel ist.

Aufgabe 2.30. Zeige, dass $\mathbb{Z}[X]$ und der Polynomring in zwei Variablen $K[X,Y]$ über einem Körper K keine Hauptidealbereiche sind.

Aufgabe 2.31. Zeige, dass in $\mathbb{Z}[X]$ die Ideale

$$\mathfrak{a} = \left(X^6 + X^3 + 1, 6X^5 + 3X^2\right)$$

und

$$\mathfrak{b} = \left(X^6 + X^3 + 1, 3X^3 - 3, 9\right)$$

übereinstimmen. Bestimme die Anzahl der Elemente im Restklassenring.

Aufgabe 2.32.*

Es sei R ein kommutativer Ring und sei $p \in R$ ein Primelement. Zeige, dass p auch im Polynomring $R[X]$ prim ist.

Aufgabe 2.33. Sei K ein algebraisch abgeschlossener Körper. Bestimme in $K[X]$ die irreduziblen Polynome.

Aufgabe 2.34. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass es unendlich viele normierte irreduzible Polynome in $K[X]$ gibt.

Aufgabe 2.35. Es sei $P \in \mathbb{R}[X]$ ein nichtkonstantes Polynom mit reellen Koeffizienten. Zeige, dass man P als ein Produkt von reellen Polynomen vom Grad 1 oder 2 schreiben kann.

Aufgabe 2.36. Es sei $K \subseteq L$ eine Körpererweiterung und es sei $a \in L$. Zeige, dass die Einsetzungsabbildung, also die Zuordnung

$$\psi\colon\ K[X] \longrightarrow L,\ P \longmapsto P(a),$$

folgende Eigenschaften erfüllt (dabei seien $P, Q \in K[X]$).

(1) $(P+Q)(a) = P(a) + Q(a)$,
(2) $(P \cdot Q)(a) = P(a) \cdot Q(a)$,
(3) $1(a) = 1$.

Aufgabe 2.37. Es sei K ein Körper, $\varphi\colon\ V \to V$ ein Endomorphismus auf einem endlichdimensionalen K-Vektorraum und

$$K[X] \longrightarrow \operatorname{End}(V),\ P \longmapsto P(\varphi),$$

der zugehörige Einsetzungshomomorphismus. Vergleiche diese Situation mit dem durch ein Element $a \in L$ zu einer Körpererweiterung $K \subseteq L$ gegebenen Einsetzungshomomorphismus $P \mapsto P(a)$.

Die folgenden Aufgaben benutzen das Produkt von Idealen.

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

$$\mathfrak{a}\mathfrak{b} = \{a_1b_1 + a_2b_2 + \cdots + a_kb_k\}$$

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

Aufgabe 2.39. 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 2.40. 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 2.41.*

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

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

Abbildungsverzeichnis