# 5. Polynome

## Vorbemerkungen

Für einen $K$-Vektorraum $V$ der Dimension $n < \infty$ bilden die Endomorphismen $\tau\colon V \longrightarrow V$ einen Ring $\mathrm{End}_K(V)$, der gemäß 3.3/2 als $K$-Vektorraum von der Dimension $n^2$ ist. Betrachtet man daher zu einem Endomorphismus $\tau$ von $V$ dessen Potenzen $\tau^{n^2}, \ldots, \tau^0 = \mathrm{id}$, so sind diese linear abhängig. Folglich existiert in $\mathrm{End}_K(V)$ eine Gleichung der Form

$$(*) \qquad \tau^r + c_1\tau^{r-1} + \ldots + c_r = 0$$

mit Konstanten $c_i \in K$ und einer natürlichen Zahl $r \leq n^2$, wobei man stets $r \leq n$ wählen kann, wie genauere Überlegungen später zeigen werden. Es handelt sich also um eine Gleichung $r$-ten Grades mit Koeffizienten aus $K$, eine so genannte *algebraische Gleichung* von $\tau$ über $K$. Diese kann genau dann linear gewählt werden (d. h. mit $r = 1$), wenn $\tau$ ein skalares Vielfaches der Identität ist, so dass im Allgemeinen $r > 1$ gelten wird. Nun ist die Theorie algebraischer Gleichungen allerdings nicht mehr der *Linearen* Algebra zuzurechnen, sie gehört thematisch eher zu dem Bereich, den man heute meist als "Algebra" bezeichnet.

Dennoch sind Gleichungen des Typs $(*)$ für unsere Zwecke sehr wichtig, da man aus ihnen bereits wertvolle Informationen über die Struktur des zugehörigen Endomorphismus $\tau$ ablesen kann. All dies werden wir im Kapitel 6 über die Normalformentheorie von Endomorphismen genauestens studieren. Dabei sind jedoch gewisse Grundkenntnisse über solche Gleichungen und insbesondere über die zugehörigen *Polynome*

$$(**) \qquad t^r + c_1t^{r-1} + \ldots + c_r$$

erforderlich, wobei das zu $(*)$ gehörige Polynom $(**)$ einen Ausdruck darstellt, in dem man $\tau$ durch eine so genannte *Variable* $t$ ersetzt hat, die bei Bedarf unterschiedliche Werte annehmen kann.

Wir werden in diesem Kapitel insbesondere den Ring aller Polynome mit Koeffizienten aus einem gegebenen Körper $K$ betrachten und zeigen, dass dieser in Bezug auf Teilbarkeitseigenschaften sehr große Ähnlichkeiten mit dem Ring $\mathbb{Z}$ der ganzen Zahlen aufweist. Beispielsweise werden wir für Polynomringe den Satz von der eindeutigen Primfaktorzerlegung herleiten.

## 5.1 Ringe

Bereits in Abschnitt 3.3 hatten wir Ringe betrachtet, und zwar zu einer natürlichen Zahl $n \geq 1$ den Matrizenring $K^{n\times n}$ über einem Körper $K$, sowie zu einem $K$-Vektorraum $V$ den Endomorphismenring $\mathrm{End}_K(V)$. Um bestimmte Eigenschaften von Elementen in $K^{n\times n}$ oder $\mathrm{End}_K(V)$ genauer zu beschreiben, ist es zweckmäßig, so genannte *Polynomringe* zu benutzen. Wir wollen daher zunächst einige allgemeine Dinge über Ringe zusammenstellen, wobei wir uns grundsätzlich auf Ringe *mit Eins* beschränken werden. Zunächst sei nochmals an die in 3.3/1 gegebene Definition eines Ringes erinnert.

**Definition 1.** *Eine Menge $R$ mit zwei Verknüpfungen " + " (Addition) und " · " (Multiplikation) heißt ein* Ring (mit Eins), *wenn folgende Bedingungen erfüllt sind*:

(i) *$R$ ist eine abelsche Gruppe bezüglich der Addition.*

(ii) *Die Multiplikation ist assoziativ, d. h. es gilt*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \textit{für} \quad a, b, c \in R.$$

(iii) *Es existiert ein Einselement in $R$, also ein Element $1 \in R$, so dass $1 \cdot a = a = a \cdot 1$ für alle $a \in R$ gilt.*

(iv) *Addition und Multiplikation verhalten sich distributiv, d. h. für $a, b, c \in R$ gilt*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

*Der Ring $R$ heißt* kommutativ, *wenn die Multiplikation kommutativ ist.*

Es ist klar, dass das Einselement 1 eines Ringes durch seine definierende Eigenschaft eindeutig bestimmt ist. Als nahe liegendes Beispiel eines kommutativen Rings kann man den Ring $\mathbb{Z}$ der ganzen Zahlen betrachten. Im Übrigen ist jeder Körper, also insbesondere $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, ein kommutativer Ring. Wie schon in Abschnitt 3.3 definiert, heißt ein Element $a$ eines Ringes $R$ eine *Einheit*, wenn es ein Element $b \in R$ mit $ab = ba = 1$ gibt. Die Menge $R^*$ aller Einheiten von $R$ bildet eine Gruppe bezüglich der Multiplikation. Für $1 \neq 0$ gilt $R^* \subset R - \{0\}$, wobei dies im Allgemeinen eine echte Inklusion ist. Genauer ist die Gleichung $R^* = R - \{0\}$ äquivalent zu der Bedingung, dass $R$ ein Körper ist. Als triviales Beispiel eines Rings hat man den so genannten *Nullring* 0. Dieser besteht nur aus einem Element 0 mit den Verknüpfungen $0 + 0 = 0$ und $0 \cdot 0 = 0$. Hier ist das Element 0 ein Null- und Einselement zugleich, so dass wir $1 = 0$ schreiben können. Der Nullring ist der einzige Ring, in dem diese Gleichung gilt.

Bei dem Matrizenring $K^{n\times n}$ über einem Körper $K$ bzw. dem Endomorphismenring $\mathrm{End}_K(V)$ eines $K$-Vektorraums $V$ handelt es sich für $n \geq 2$ bzw. $\dim_K(V) \geq 2$ um nicht-kommutative Ringe; vgl. Abschnitt 3.3. Als weiteres Beispiel kann man für einen Ring $R$ dessen $n$-faches kartesisches Produkt $R^n$ als Ring betrachten, indem man Addition und Multiplikation komponentenweise erklärt:

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$$
$$(\alpha_1, \ldots, \alpha_n) \cdot (\beta_1, \ldots, \beta_n) = (\alpha_1 \cdot \beta_1, \ldots, \alpha_n \cdot \beta_n)$$

Es ist dann $0 = (0, \ldots, 0)$ das Nullelement und $1 = (1, \ldots, 1)$ das Einselement. Im Falle $R \neq 0$ und $n \geq 2$ zeigt die Gleichung

$$(1, 0, \ldots, 0) \cdot (0, \ldots, 0, 1) = (0, \ldots, 0),$$

dass dieser Ring nicht-triviale Nullteiler besitzt. Dabei heißt ein Element $a$ eines Rings ein *Nullteiler*, wenn es ein Element $b \neq 0$ dieses Rings mit $a \cdot b = 0$ oder $b \cdot a = 0$ gibt. Man nennt einen kommutativen Ring $R$ mit $1 \neq 0$ einen *Integritätsring*, wenn $R$ keine nicht-trivialen Nullteiler besitzt, wenn also für $a, b \in R - \{0\}$ stets $a \cdot b \neq 0$ gilt.

Als wichtiges Beispiel wollen wir nunmehr den *Polynomring* $R[T]$ über einem *kommutativen* Ring $R$ in einer Variablen $T$ konstruieren. Um unsere Intentionen klarzulegen, gehen wir dabei zunächst in naiver Weise vor und erklären $R[T]$ als Menge aller formal gebildeten Summen des Typs $\sum_{i=0}^{m} a_i T^i$, mit Koeffizienten $a_i \in R$ und variabler oberer Grenze $m \in \mathbb{N}$. Addiert und multipliziert man solche Ausdrücke "wie gewöhnlich", so erkennt man $R[T]$ als kommutativen Ring. Dabei stelle man sich $T$ als eine "variable" bzw. "allgemeine" Größe vor, für die man nach Bedarf Elemente z. B. aus $R$ einsetzen darf. Wichtig ist, dass Addition und Multiplikation in $R[T]$ bei einem solchen Ersetzungsprozess in die entsprechenden Verknüpfungen von $R$ übergehen. Man rechnet daher mit $T$ in gleicher Weise wie mit einer "konkreten" Größe, etwa aus $R$.

Der Polynomring $R[T]$ soll nun aber auch noch auf präzisere Weise konstruiert werden. Wir setzen $R[T] = R^{(\mathbb{N})}$ und verstehen hierunter die Menge aller Folgen $(a_i)_{i\in\mathbb{N}}$ von Elementen $a_i \in R$, für die $a_i = 0$ für fast alle $i \in \mathbb{N}$ gilt, also für alle $i \in \mathbb{N}$, bis auf endlich viele Ausnahmen. Addition und Multiplikation solcher Folgen seien erklärt durch die Formeln

$$(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} := (a_i + b_i)_{i\in\mathbb{N}},$$
$$(a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}} := (c_i)_{i\in\mathbb{N}},$$

mit

$$c_i := \sum_{i=\mu+\nu} a_\mu b_\nu = \sum_{\mu=0}^{i} a_\mu b_{i-\mu}.$$

Indem man die Ringeigenschaften von $R$ benutzt, kann man leicht nachrechnen, dass $R^{(\mathbb{N})}$ mit diesen Verknüpfungen einen kommutativen Ring (mit Eins) bildet. Das Nullelement wird gegeben durch die Folge $0 = (0, 0, \ldots)$, das Einselement durch die Folge $1 = (1, 0, 0, \ldots)$.

Wir wollen exemplarisch nur das Assoziativgesetz der Multiplikation nachrechnen. Für $(a_i)_i, (b_i)_i, (c_i)_i \in R^{(\mathbb{N})}$ gilt

$$\begin{aligned}\big[(a_i)_i \cdot (b_i)_i\big] \cdot (c_i)_i &= \Big(\sum_{\lambda+\mu=i} a_\lambda b_\mu\Big)_i \cdot (c_i)_i \\ &= \Big(\sum_{\kappa+\nu=i} \Big(\sum_{\lambda+\mu=\kappa} a_\lambda b_\mu\Big) \cdot c_\nu\Big)_i = \Big(\sum_{\lambda+\mu+\nu=i} a_\lambda b_\mu c_\nu\Big)_i,\end{aligned}$$

sowie in entsprechender Weise

$$(a_i)_i \cdot [(b_i)_i \cdot (c_i)_i] = (a_i)_i \cdot (\sum_{\mu+\nu=i} b_\mu c_\nu)_i$$
$$= (\sum_{\lambda+\kappa=i} a_\lambda \cdot (\sum_{\mu+\nu=\kappa} b_\mu c_\nu))_i = (\sum_{\lambda+\mu+\nu=i} a_\lambda b_\mu c_\nu)_i.$$

Um schließlich die Elemente von $R^{(\mathbb{N})}$ wie gewohnt als Polynome, also Ausdrücke der Form $\sum_{i=0}^{<\infty} a_i T^i$, zu schreiben, betrachte man das Element

$$T = (0, 1, 0, \ldots) \in R^{(\mathbb{N})}.$$

Für $n \in \mathbb{N}$ gilt $T^n = (\delta_{in})_{i\in\mathbb{N}}$, wobei dies insbesondere für $n = 0$ aufgrund unserer Konvention über das leere Produkt richtig ist. Identifizieren wir nun die Elemente $a \in R$ mit den entsprechenden Elementen $(a, 0, 0, \ldots) \in R^{(\mathbb{N})}$, so ist diese Identifizierung mit den Verknüpfungen in $R$ und $R^{(\mathbb{N})}$ verträglich. Wir können also $R$ sozusagen als "Unterring" von $R^{(\mathbb{N})}$ auffassen. Elemente $f = (a_i)_{i\in\mathbb{N}} \in R^{(\mathbb{N})}$ lassen sich dann als Polynome in $T$ mit Koeffizienten aus $R$ schreiben, nämlich in der Form

$$f = (a_i)_{i\in\mathbb{N}} = \sum_{i\in\mathbb{N}} (a_i \delta_{ij})_{j\in\mathbb{N}} = \sum_{i\in\mathbb{N}} a_i (\delta_{ij})_{j\in\mathbb{N}} = \sum_{i\in\mathbb{N}} a_i T^i,$$

wobei die Koeffizienten $a_i \in R$ in der Darstellung $f = \sum_{i\in\mathbb{N}} a_i T^i$ jeweils eindeutig bestimmt sind; man nennt $a_i$ den *Koeffizienten von $f$ zum Grad $i$*.

Wir werden von nun an für den gerade konstruierten Polynomring stets die Notation $R[T]$ verwenden und dessen Elemente als Polynome der Form $\sum_{i\in\mathbb{N}} a_i T^i$ mit Koeffizienten $a_i \in R$ schreiben (wobei anstelle von $T$ natürlich auch ein anderer Buchstabe zur Bezeichnung der Variablen zugelassen ist). Dabei sei immer stillschweigend vorausgesetzt, dass die Koeffizienten $a_i$ für fast alle Indizes $i \in \mathbb{N}$ verschwinden, die vorstehende Summe also jeweils als *endliche* Summe Sinn macht. Addition und Multiplikation in $R[T]$ beschreiben sich dann durch die bekannten Formeln

$$\Big(\sum_{i\in\mathbb{N}} a_i T^i\Big) + \Big(\sum_{i\in\mathbb{N}} b_i T^i\Big) = \sum_{i\in\mathbb{N}} (a_i + b_i) T^i,$$
$$\Big(\sum_{i\in\mathbb{N}} a_i T^i\Big) \cdot \Big(\sum_{i\in\mathbb{N}} b_i T^i\Big) = \sum_{i\in\mathbb{N}} (\sum_{\mu+\nu=i} a_\mu b_\nu) \cdot T^i.$$

Ist für ein Polynom $f = \sum_{i\in\mathbb{N}} a_i T^i \in R[T]$ ein $n \in \mathbb{N}$ bekannt mit $a_i = 0$ für $i > n$, so können wir auch $f = \sum_{i=0}^{n} a_i T^i$ schreiben. Gilt zudem $a_n \neq 0$, so nennt man $a_n$ den *höchsten Koeffizienten* von $f$, und es wird $n$ als *Grad* von $f$ bezeichnet, $n = \operatorname{grad} f$. Jedes nicht-triviale Polynom $f \in R[T]$ besitzt einen wohlbestimmten Grad. Darüber hinaus trifft man die Konvention, dem Nullpolynom 0 den Grad $-\infty$ zuzuordnen.

**Satz 2.** *Es sei $R$ ein kommutativer Ring und $R[T]$ der Polynomring einer Variablen über $R$. Für $f, g \in R[T]$ gilt dann*

$$\operatorname{grad}(f+g) \le \max\{\operatorname{grad} f, \operatorname{grad} g\},$$
$$\operatorname{grad}(f\cdot g) \le \operatorname{grad} f + \operatorname{grad} g.$$

*Ist $R$ ein Integritätsring, so gilt sogar*

$$\operatorname{grad}(f\cdot g) = \operatorname{grad} f + \operatorname{grad} g.$$

*Beweis.* Die Behauptung ist problemlos zu verifizieren, falls $f$ oder $g$ das Nullpolynom ist. Wir dürfen daher $f$ und $g$ als nicht-trivial annehmen, also $m = \operatorname{grad} f \ge 0$ sowie $n = \operatorname{grad} g \ge 0$. Sei etwa $f = \sum a_i T^i$, $g = \sum b_i T^i$. Dann folgt $a_i = 0$ für $i > m$ und $b_i = 0$ für $i > n$ und damit $a_i + b_i = 0$ für $i > \max\{m,n\}$, also $\operatorname{grad}(f+g) \le \max\{m,n\}$. Auf ähnliche Weise sieht man $\sum_{\mu+\nu=i} a_\mu b_\nu = 0$ für $i > m+n$, und dies bedeutet $\operatorname{grad}(f\cdot g) \le m+n$. Insbesondere ist

$$a_m b_n = \sum_{\mu+\nu=m+n} a_\mu b_\nu$$

der Koeffizient in $f\cdot g$ vom Grad $m+n$ und damit der höchste Koeffizient, falls er nicht verschwindet. Ist nun $R$ ein Integritätsring, so gilt $a_m b_n \ne 0$ wegen $a_m \ne 0 \ne b_n$, und man erkennt $\operatorname{grad}(f\cdot g) = m+n$. □

**Korollar 3.** *Ist $R$ ein Integritätsring, so auch der Polynomring $R[T]$.*

*Beweis.* Seien $f, g \in R[T]$ zwei nicht-triviale Polynome. Dann folgt $\operatorname{grad} f \ge 0$, $\operatorname{grad} g \ge 0$ und somit gemäß Satz 2 $\operatorname{grad}(f\cdot g) = \operatorname{grad} f + \operatorname{grad} g \ge 0$. Dies zeigt $f\cdot g \ne 0$, d. h. $R[T]$ ist ein Integritätsring. □

Wir wollen im Weiteren spezielle Werte für die Variable $T$ eines Polynomrings $R[T]$ einsetzen. Hierzu ist es von Nutzen, neben Homomorphismen von Ringen auch so genannte Algebren und deren Homomorphismen zu betrachten.

**Definition 4.** *Eine Abbildung $\varphi\colon R \longrightarrow R'$ zwischen Ringen $R, R'$ heißt ein* Homomorphismus, *genauer ein* Ringhomomorphismus, *wenn gilt*:

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ *für* $a, b \in R$.
(ii) $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$ *für* $a, b \in R$.
(iii) $\varphi(1_R) = 1_{R'}$, *d. h. $\varphi$ bildet das Einselement $1_R \in R$ auf das Einselement $1_{R'} \in R'$ ab.*

Wie bei Vektorraumhomomorphismen spricht man von einem *Mono-*, *Epi-* bzw. *Isomorphismus*, wenn $\varphi$ injektiv, surjektiv bzw. bijektiv ist. Weiter wird ein Homomorphismus $\varphi\colon R \longrightarrow R$ auch als *Endomorphismus* von $R$ bezeichnet, bzw. als *Automorphismus*, wenn dieser ein Isomorphismus ist.

**Definition 5.** *Es sei $R$ ein kommutativer Ring. Eine* $R$-Algebra *besteht aus einem (nicht notwendig kommutativen) Ring $A$ und einem Ringhomomorphismus $\varphi\colon R \longrightarrow A$, derart dass alle Elemente aus $\varphi(R)$ mit den Elementen aus $A$ vertauschbar sind, also $\varphi(r)a = a\varphi(r)$ für alle $r \in R$, $a \in A$ gilt.*

Häufig spricht man einfach von $A$ als $R$-Algebra, ohne den Homomorphismus $\varphi\colon R \longrightarrow A$ explizit zu erwähnen. Entsprechend schreibt man $r \cdot a$ anstelle von $\varphi(r) \cdot a$ für Elemente $r \in R$, $a \in A$, wobei der definierende Homomorphismus $R \longrightarrow A$ dann durch $r \longmapsto r \cdot 1_A$ gegeben ist. Wenn dieser nicht injektiv ist, so darf man allerdings statt $r \cdot 1_A$ keinesfalls wieder $r$ schreiben, denn es ist dann nicht möglich, die Elemente $r \in R$ mit ihren Bildern $r \cdot 1_A \in A$ zu identifizieren. Beispielsweise sind $R$ und der Polynomring $R[T]$ auf kanonische Weisen $R$-Algebren, indem man die identische Abbildung $R \longrightarrow R$ bzw. die Inklusionsabbildung $R \hookrightarrow R[T]$ betrachtet. Weiter definiert für einen Vektorraum $V$ über einem Körper $K$ die Abbildung

$$K \longrightarrow \mathrm{End}_K(V), \qquad \alpha \longmapsto \alpha \cdot \mathrm{id}_V,$$

den Endomorphismenring $\mathrm{End}_K(V)$ als $K$-Algebra. Entsprechend ist der Matrizenring $K^{n\times n}$ für $n \in \mathbb{N} - \{0\}$ unter der Abbildung

$$K \longrightarrow K^{n\times n}, \qquad \alpha \longmapsto \alpha \cdot E_n,$$

eine $K$-Algebra, wobei $E_n$ die Einheitsmatrix in $K^{n\times n}$ bezeichne.

Ist $A$ eine $R$-Algebra, so kann man neben der Addition und Multiplikation des Ringes $A$ auch noch die äußere Multiplikation

$$R \times A \longrightarrow A, \qquad (r, a) \longmapsto r \cdot a,$$

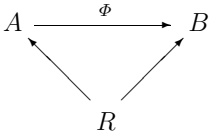
mit Elementen aus $R$ betrachten. Diese Multiplikation erfüllt Eigenschaften, wie sie etwa in 1.4/1 für die skalare Multiplikation eines Vektorraums gefordert werden. In der Tat wird $A$ im Falle eines Körpers $K = R$ unter der äußeren Multiplikation zu einem $K$-Vektorraum, wobei wir für $\mathrm{End}_K(V)$ und $K^{n\times n}$ jeweils die auch früher schon betrachteten $K$-Vektorraumstrukturen erhalten. Im Übrigen sei darauf hingewiesen, dass die äußere Multiplikation mit der inneren Multiplikation auf $A$ verträglich ist, d. h. es gilt

$$r \cdot (a \cdot b) = (r \cdot a) \cdot b = a \cdot (r \cdot b) \qquad \text{für } r \in R, a, b \in A.$$

Homomorphismen zwischen $R$-Algebren werden in natürlicher Weise als Ringhomomorphismen erklärt, die zusätzlich die äußere Multiplikation mit $R$ respektieren:

**Definition 6.** *Es seien $A, B$ Algebren über einem kommutativen Ring $R$. Ein* Homomorphismus von $R$-Algebren *$\Phi\colon A \longrightarrow B$ ist ein Ringhomomorphismus, so dass $\Phi(ra) = r\Phi(a)$ für alle $r \in R$, $a \in A$ gilt.*

Sind $R \longrightarrow A$ und $R \longrightarrow B$ die definierenden Homomorphismen der betrachteten $R$-Algebren, so ist ein Ringhomomorphismus $\Phi\colon A \longrightarrow B$ genau dann ein Homomorphismus von $R$-Algebren, wenn das Diagramm




kommutiert.

**Satz 7.** *Es sei $R$ ein kommutativer Ring, $R[T]$ der Polynomring einer Variablen über $R$, sowie $A$ eine beliebige $R$-Algebra. Zu jedem $t \in A$ gibt es dann einen eindeutig bestimmten $R$-Algebrahomomorphismus $\Phi\colon R[T] \longrightarrow A$ mit $\Phi(T) = t$. Dieser wird beschrieben durch*

$$\sum_{i\in\mathbb{N}} a_i T^i \longmapsto \sum_{i\in\mathbb{N}} a_i t^i$$

*oder, in suggestiver Schreibweise, durch*

$$f \longmapsto f(t),$$

*wobei dann insbesondere*

$$(f+g)(t) = f(t) + g(t), \qquad (f\cdot g)(t) = f(t)\cdot g(t)$$

*für $f, g \in R[T]$ gilt. Man nennt $\Phi$ auch den* Einsetzungshomomorphismus, *der $t$ anstelle von $T$ einsetzt.*

*Beweis.* Ist $\Phi$ ein $R$-Algebrahomomorphismus der geforderten Art, so gilt für $\sum_{i\in\mathbb{N}} a_i T^i \in R[T]$

$$\Phi(\sum_{i\in\mathbb{N}} a_i T^i) = \sum_{i\in\mathbb{N}} \Phi(a_i T^i) = \sum_{i\in\mathbb{N}} a_i \Phi(T)^i = \sum_{i\in\mathbb{N}} a_i t^i.$$

Dies zeigt die Eindeutigkeit von $\Phi$. Um auch die Existenz nachzuweisen, erkläre man $\Phi$ durch

$$\Phi(\sum_{i\in\mathbb{N}} a_i T^i) = \sum_{i\in\mathbb{N}} a_i t^i.$$

Man sieht dann unmittelbar, dass $\Phi$ ein $R$-Algebrahomomorphismus ist. Beispielsweise ergibt sich die Verträglichkeit von $\Phi$ mit der Multiplikation aufgrund folgender Rechnung:

$$\begin{aligned}\Phi(\sum_{i\in\mathbb{N}} a_i T^i \cdot \sum_{i\in\mathbb{N}} b_i T^i) &= \Phi(\sum_{i\in\mathbb{N}} (\sum_{\mu+\nu=i} a_\mu b_\nu)\cdot T^i) = \sum_{i\in\mathbb{N}} (\sum_{\mu+\nu=i} a_\mu b_\nu)\cdot t^i \\ &= \sum_{i\in\mathbb{N}} \sum_{\mu+\nu=i} (a_\mu t^\mu)\cdot(b_\nu t^\nu) = (\sum_{i\in\mathbb{N}} a_i t^i)\cdot(\sum_{i\in\mathbb{N}} b_i t^i) \\ &= \Phi(\sum_{i\in\mathbb{N}} a_i T^i)\cdot\Phi(\sum_{i\in\mathbb{N}} b_i T^i)\end{aligned}$$

Man beachte dabei, dass wir die Vertauschbarkeit von $t$ mit den (Bildern der) Koeffizienten $b_i$ in $A$ benutzt haben. □

Betrachten wir beispielsweise den Endomorphismenring $A = \mathrm{End}_K(V)$ eines $K$-Vektorraums $V$ als $K$-Algebra, so können wir zu jedem Endomorphismus $\tau\colon V \longrightarrow V$ den $K$-Algebrahomomorphismus

$$\Phi_\tau\colon K[T] \longrightarrow \mathrm{End}_K(V), \qquad \sum_{i\in\mathbb{N}} a_i T^i \longmapsto \sum_{i\in\mathbb{N}} a_i \tau^i,$$

betrachten, der den Endomorphismus $\tau$ anstelle von $T$ einsetzt. Dabei ist $\tau^i$ natürlich erklärt als $i$-fache Komposition $\tau \circ \ldots \circ \tau$ von $\tau$ mit sich selber, und das Bild eines Polynoms $\sum_{i\in\mathbb{N}} a_i T^i \in K[T]$ unter $\Phi_\tau$ ergibt sich als Endomorphismus

$$\sum_{i\in\mathbb{N}} a_i \tau^i\colon V \longrightarrow V, \qquad v \longmapsto \sum_{i\in\mathbb{N}} a_i \tau^i(v).$$

Wir werden den Homomorphismus $\Phi_\tau$ insbesondere zur Definition des so genannten *Minimalpolynoms* von $\tau$ verwenden; vgl. 6.2/9 und 6.2/10. Anstelle des Endomorphismenrings eines Vektorraums kann man natürlich auch den Matrizenring $K^{n\times n}$ betrachten. Zu jeder Matrix $C \in K^{n\times n}$ erhält man dann einen $K$-Algebrahomomorphismus

$$\Phi_C\colon K[T] \longrightarrow K^{n\times n}, \qquad \sum_{i\in\mathbb{N}} a_i T^i \longmapsto \sum_{i\in\mathbb{N}} a_i C^i,$$

der $C$ anstelle von $T$ einsetzt.

Wir wollen ein weiteres Beispiel betrachten. Es sei $K$ ein Körper und $\mathrm{Abb}(K, K)$ die Menge aller Abbildungen $K \longrightarrow K$ oder, mit anderen Worten, die Menge aller $K$-wertigen Funktionen auf $K$. Zu jedem Polynom $f \in K[T]$ lässt sich dann die zugehörige Polynomfunktion $t \longmapsto f(t)$ als Element von $\mathrm{Abb}(K, K)$ betrachten. Diese ordnet einem Element $t \in K$ den Wert $f(t) \in K$ zu, den man erhält, indem man $t$ anstelle von $T$ in $f$ einsetzt. Auf diese Weise ergibt sich eine Abbildung

$$\Psi\colon K[T] \longrightarrow \mathrm{Abb}(K, K), \qquad f \longmapsto (t \longmapsto f(t)),$$

die wir im Folgenden als Homomorphismus von $K$-Algebren deuten wollen. Um $A = \mathrm{Abb}(K, K)$ als $K$-Algebra zu erklären, betrachten wir die gewöhnliche Addition und Multiplikation $K$-wertiger Funktionen, gegeben durch

$$\begin{aligned} p + q\colon K &\longrightarrow K, \qquad t \longmapsto p(t) + q(t), \\ p \cdot q\colon K &\longrightarrow K, \qquad t \longmapsto p(t) \cdot q(t). \end{aligned}$$

Mit diesen Verknüpfungen ist $A$ ein kommutativer Ring, in dem die Nullfunktion 0 das Nullelement und die Funktion $1_A$, die identisch 1 ist, das Einselement bilden. Für $\alpha \in K$ kann man weiter das $\alpha$-fache eines Elementes $p \in A$ durch

$$\alpha \cdot p\colon K \longrightarrow K, \qquad t \longmapsto \alpha \cdot (p(t)),$$

erklären. In diesem Sinne ist dann

$$K \longrightarrow A, \qquad \alpha \longmapsto \alpha \cdot 1_A,$$

ein Ringhomomorphismus, der $A$ zu einer $K$-Algebra macht. Mit Satz 7 folgt leicht, dass die Abbildung $\Psi$, die einem Polynom $f \in K[T]$ die zugehörige Polynomfunktion $t \longmapsto f(t)$ zuordnet, tatsächlich ein Homomorphismus von $K$-Algebren ist. Gleiches gilt, wenn man allgemeiner anstelle von $K$ einen kommutativen Ring $R$ zugrunde legt. Die Homomorphie-Eigenschaft für $\Psi$ besagt insbesondere, dass man mit dem Element $T$ in gleicher Weise rechnet, wie man es mit konkreten Werten $t$ anstelle von $T$ tun würde. Dies rechtfertigt die Bezeichnung von $T$ als "Variable".

Enthält der Körper $K$ unendlich viele Elemente, so ist die Abbildung $\Psi$ injektiv, wie wir später aus 5.3/2 ablesen können. Man könnte dann Polynome aus $K[T]$ mit ihren zugehörigen Polynomfunktionen $K \longrightarrow K$ identifizieren. Für einen endlichen Körper $K = \{\alpha_1, \ldots, \alpha_q\}$ jedoch ist beispielsweise

$$f = (T - \alpha_1) \ldots (T - \alpha_q) \in K[T]$$

ein nicht-triviales Polynom, dessen zugehörige Polynomfunktion $K \longrightarrow K$ identisch verschwindet, so dass also $\Psi(f) = 0$ gilt. Die Abbildung $\Psi$ ist daher im Allgemeinen nicht injektiv, und dies ist einer der Gründe dafür, dass wir Polynome nicht als konkrete Funktionen, sondern als formale Ausdrücke unter Zuhilfenahme einer "Variablen" erklärt haben.

Wir wollen nun noch Ideale und Unterringe von Ringen einführen, Begriffe, die im Zusammenhang mit Ringhomomorphismen von Bedeutung sind.

**Definition 8.** *Es sei $R$ ein Ring (mit Eins). Ein* Unterring *von $R$ besteht aus einer Teilmenge $S \subset R$, derart dass gilt*:

(i) $a, b \in S \Longrightarrow a - b, a \cdot b \in S$.

(ii) $1 \in S$.

$S$ ist dann mit den von $R$ induzierten Verknüpfungen selbst wieder ein Ring, und die Inklusionsabbildung $S \hookrightarrow R$ ist ein Ringhomomorphismus. Man überlegt sich leicht, dass das Bild $\varphi(R)$ eines Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ stets ein Unterring von $R'$ ist.

**Definition 9.** *Es sei $R$ ein Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt* Ideal, *falls gilt*:

(i) $\mathfrak{a}$ *ist additive Untergruppe von $R$, d. h. man hat $\mathfrak{a} \neq \emptyset$, und aus $a, b \in \mathfrak{a}$ folgt $a - b \in \mathfrak{a}$.*

(ii) *Aus $a \in \mathfrak{a}$, $r \in R$ folgt $ra, ar \in \mathfrak{a}$.*

Man rechnet leicht nach, dass für jeden Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ der *Kern*

$$\ker \varphi = \{a \in R\,;\, \varphi(a) = 0\}$$

ein Ideal ist, wobei $\varphi$ genau dann injektiv ist, wenn $\ker \varphi$ das Nullideal ist, d. h. nur aus dem Nullelement besteht. Ist $R$ ein beliebiger Ring, so kann man zu

einem Element $a \in R$, welches mit allen übrigen Elementen von $R$ vertauschbar ist, das hiervon erzeugte *Hauptideal*

$$(a) = Ra = \{ra\,;\, r \in R\}$$

betrachten. Speziell besteht für $R = \mathbb{Z}$ das Ideal (2) aus allen geraden Zahlen, das Ideal (12) aus allen durch 12 teilbaren Zahlen. In jedem Ring gibt es die so genannten trivialen Ideale, nämlich das *Einheitsideal* $(1) = R$ sowie das *Nullideal* (0), welches man meist mit 0 bezeichnet. Ein Körper besitzt außer den trivialen keine weiteren Ideale. Umgekehrt kann man zeigen, dass ein kommutativer Ring, der genau zwei Ideale hat, ein Körper ist.

Ist $\mathfrak{a}$ ein Ideal eines Ringes $R$, so kann man ähnlich wie in Abschnitt 2.2 den *Quotienten-* oder *Restklassenring* $R/\mathfrak{a}$ konstruieren. Da man auf diese Weise interessante Ringe und sogar Körper erhalten kann, wollen wir die Konstruktion hier kurz besprechen. Man erklärt eine Relation " $\sim$ " auf $R$, indem man für $a, b \in R$ setzt:

$$a \sim b \Longleftrightarrow a - b \in \mathfrak{a}$$

Man sieht dann unschwer, dass " $\sim$ " eine Äquivalenzrelation ist. Für $a \in R$ hat man $a \sim a$ wegen $a - a = 0 \in \mathfrak{a}$. Die Relation ist daher reflexiv. Gilt weiter $a \sim b$, so folgt $a - b \in \mathfrak{a}$ und damit auch $b - a = -(a - b) \in \mathfrak{a}$. Letzteres bedeutet $b \sim a$, und es folgt die Symmetrie von " $\sim$ ". Zum Nachweis der Transitivität schließlich nehme man $a \sim b$ und $b \sim c$ für Elemente $a, b, c \in R$ an. Dann gilt $a - b, b - c \in \mathfrak{a}$, und man erhält

$$a - c = (a - b) + (b - c) \in \mathfrak{a},$$

d. h. $a \sim c$. Es ist " $\sim$ " also eine Äquivalenzrelation, und wir können zu einem Element $a \in R$ die zugehörige Äquivalenzklasse

$$[a] := \{b \in R\,;\, b \sim a\} = a + \mathfrak{a}$$

bilden, wobei $a + \mathfrak{a}$ als *Nebenklasse von $a$ bezüglich* $\mathfrak{a}$, also als Menge aller Summen des Typs $a + a'$ mit $a' \in \mathfrak{a}$ zu interpretieren ist. Gemäß 2.2/4 sind zwei Äquivalenzklassen $[a]$, $[b]$ entweder disjunkt oder aber identisch (im Falle $a \sim b$). Insbesondere ist $R$ die disjunkte Vereinigung aller Äquivalenzklassen.

Man bezeichne nun die Menge aller Nebenklassen bezüglich $\mathfrak{a}$ mit $R/\mathfrak{a}$. Um $R/\mathfrak{a}$ zu einem Ring zu machen, werden folgende Verknüpfungen erklärt:

$$[a] + [b] = [a + b], \qquad [a] \cdot [b] = [a \cdot b]$$

Dabei ist zu verifizieren, dass die Klasse $[a + b]$ bzw. $[a \cdot b]$ nicht von der Wahl der Repräsentanten $a$ und $b$ der betrachteten Klassen $[a], [b]$ abhängt. Gelte etwa $[a] = [a']$ und $[b] = [b']$. Dann folgt $a - a'$, $b - b' \in \mathfrak{a}$ und damit

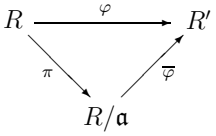
$$(a + b) - (a' + b') \in \mathfrak{a}, \qquad ab - a'b' = a(b - b') + (a - a')b' \in \mathfrak{a},$$

also $a + b \sim a' + b'$ und $ab \sim a'b'$. Addition und Multiplikation in $R/\mathfrak{a}$ sind daher wohldefiniert, und man sieht unmittelbar aufgrund der Ringeigenschaften von $R$, dass auch $R/\mathfrak{a}$ ein Ring ist, und zwar derart, dass die Abbildung

$$\pi\colon R \longrightarrow R/\mathfrak{a}, \qquad a \longmapsto [a],$$

ein surjektiver Ringhomomorphismus mit Kern $\mathfrak{a}$ ist. Man bezeichnet $R/\mathfrak{a}$ als *Restklassen-* oder *Quotientenring von $R$ modulo $\mathfrak{a}$*. Ähnlich wie in 2.2/8 gilt folgender Homomorphiesatz:

**Satz 10.** (Homomorphiesatz für Ringe). *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus, $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{a} \subset \ker\varphi$ und $\pi\colon R \longrightarrow R/\mathfrak{a}$ die natürliche Projektion. Dann existiert ein eindeutig bestimmter Ringhomomorphismus $\overline{\varphi}\colon R/\mathfrak{a} \longrightarrow R'$, so dass das Diagramm*




*kommutiert. Dabei ist $\overline{\varphi}$ genau dann injektiv, wenn $\mathfrak{a} = \ker\varphi$ gilt und genau dann surjektiv, wenn $\varphi$ surjektiv ist.*

*Beweis.* Da man die Argumentation aus 2.2/8 mutatis mutandis übernehmen kann, wollen wir uns hier kurz fassen und nur auf die Definition von $\overline{\varphi}$ eingehen. Um $\overline{\varphi}(\overline{a})$ für ein Element $\overline{a} \in R/\mathfrak{a}$ zu erklären, wähle man ein $\pi$-Urbild $a \in R$ und setze $\overline{\varphi}(\overline{a}) = \varphi(a)$. Dabei ist natürlich zu verifizieren, dass das Element $\varphi(a)$ unabhängig von der Wahl des $\pi$-Urbildes $a$ zu $\overline{a}$ ist. Letzteres folgt aus der Bedingung $\mathfrak{a} \subset \ker\varphi$. □

## Aufgaben

$R$ sei stets ein *kommutativer* Ring.

1. Für ein Element $t \in R$ betrachte man den Homomorphismus $\Phi\colon R[T] \longrightarrow R$, $f \longmapsto f(t)$, der $t$ anstelle der Variablen $T$ einsetzt. Man zeige:

$$\ker\Phi = R[T] \cdot (T - t)$$

(Hinweis: Man reduziere auf den Fall $t = 0$, indem man den Einsetzungshomomorphismus $R[T] \longrightarrow R[T]$ betrachtet, der $T$ durch $T + t$ ersetzt.)

2. Es sei $V$ ein nicht-trivialer Vektorraum über einem Körper $K$. Zu einem Endomorphismus $\varphi \in \mathrm{End}_K(V)$ betrachte man den Einsetzungshomomorphismus $\Phi\colon K[T] \longrightarrow \mathrm{End}_K(V)$, der $\varphi$ anstelle von $T$ einsetzt. Man bestimme $\ker\Phi$ in den Fällen $\varphi = \mathrm{id}$ und $\varphi = 0$.

3. Es bezeichne $R^{\mathbb{N}}$ die Menge aller Folgen $(a_i)_{i\in\mathbb{N}}$ von Elementen $a_i \in R$.

   (i) Man verwende die gleichen Formeln wie im Falle des Polynomrings einer Variablen über $R$, um anstelle von $R^{(\mathbb{N})}$ auf $R^{\mathbb{N}}$ die Struktur eines Ringes zu erklären. Dieser Ring wird mit $R[\![T]\!]$ bezeichnet und heißt Ring der *formalen Potenzreihen* einer Variablen über $R$. Seine Elemente lassen sich als *unendliche* Reihen $\sum_{i=0}^{\infty} a_i T^i$ darstellen.

(ii) Es sei $q \in R[\![T]\!] \cdot T$. Man zeige, dass $\sum_{n=0}^{\infty} q^n$ zu einem wohldefinierten Element $f \in R[\![T]\!]$ Anlass gibt und dass $f \cdot (1-q) = 1$ gilt.

(iii) Man bestimme die Gruppe aller Einheiten in $R[\![T]\!]$.

4. Es seien $\mathfrak{a}, \mathfrak{b} \subset R$ Ideale. Man zeige, dass die folgenden Teilmengen von $R$ wiederum Ideale bilden:

(i) $\mathfrak{a} + \mathfrak{b} = \{a + b\,;\, a \in \mathfrak{a}, b \in \mathfrak{b}\}$

(ii) $\mathfrak{a} \cdot \mathfrak{b}$ = Menge aller endlichen Summen von Produkten $a \cdot b$ mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$

(iii) $\mathfrak{a} \cap \mathfrak{b}$

5. Man zeige, dass $R$ genau dann ein Körper ist, wenn $R$ genau zwei verschiedene Ideale besitzt.

6. Für ein Ideal $\mathfrak{a} \subset R$ zeige man, dass die Menge aller Elemente $a \in R$, zu denen es ein $n \in \mathbb{N}$ mit $a^n \in \mathfrak{a}$ gibt, ebenfalls wieder ein Ideal in $R$ bildet. Dieses wird mit $\operatorname{rad} \mathfrak{a}$ bezeichnet und heißt das *Nilradikal* von $\mathfrak{a}$.

7. Für eine Familie $(a_i)_{i \in I}$ von Elementen in $R$ zeige man:

(i) Es existiert ein kleinstes Ideal $\mathfrak{a} \subset R$ mit $a_i \in \mathfrak{a}$ für alle $i \in I$.

(ii) Es gilt $\mathfrak{a} = \{\sum_{i \in I} r_i a_i\,;\, r_i \in R, r_i = 0 \text{ für fast alle } i \in I\}$.

8. (*Isomorphiesatz*) Es seien $\mathfrak{a} \subset \mathfrak{b} \subset R$ Ideale. Man zeige:

(i) Die kanonische Abbildung $\mathfrak{b} \hookrightarrow R \longrightarrow R/\mathfrak{a}$ besitzt $\mathfrak{a}$ als Kern und induziert eine Injektion $\mathfrak{b}/\mathfrak{a} \hookrightarrow R/\mathfrak{a}$, wobei man $\mathfrak{b}/\mathfrak{a}$ zunächst als Menge der Restklassen $b + \mathfrak{a}$ mit $b \in \mathfrak{b}$ erkläre. Weiter lässt sich $\mathfrak{b}/\mathfrak{a}$ mit seinem Bild in $R/\mathfrak{a}$ identifizieren und als Ideal in $R/\mathfrak{a}$ auffassen.

(ii) Die Projektion $R \longrightarrow R/\mathfrak{b}$ faktorisiert über $R/\mathfrak{a}$, d. h. lässt sich als Komposition $R \xrightarrow{\pi} R/\mathfrak{a} \xrightarrow{f} R/\mathfrak{b}$ schreiben, mit einem Ringhomomorphismus $f$ und der kanonischen Projektion $\pi$.

(iii) $f$ besitzt $\mathfrak{b}/\mathfrak{a}$ als Kern und induziert einen Isomorphismus

$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \xrightarrow{\sim} R/\mathfrak{b}.$$

## 5.2 Teilbarkeit in Integritätsringen

In diesem Abschnitt seien alle Ringe als *Integritätsringe* und damit insbesondere als kommutativ vorausgesetzt. Im Wesentlichen interessieren wir uns für den Polynomring $K[T]$ in einer Variablen $T$ über einem Körper $K$, für den wir Teilbarkeits- und Faktorisierungsaussagen herleiten wollen. Als Ring mit ganz analogen Eigenschaften soll aber auch der Ring $\mathbb{Z}$ der ganzen Zahlen betrachtet werden. Grundlegend ist in beiden Ringen das Verfahren der *Division mit Rest*, welches wir insbesondere benutzen wollen, um den Satz über die eindeutige Primfaktorzerlegung in Polynomringen herzuleiten. Zunächst erinnern wir an dieses Verfahren, wobei wir davon ausgehen, dass die Division mit Rest im Ring $\mathbb{Z}$ der ganzen Zahlen wohlbekannt ist.

**Satz 1.** *Zu $a, b \in \mathbb{Z}$ mit $b > 0$ existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = qb + r, \qquad 0 \leq r < b.$$

**Satz 2.** *Zu Polynomen $f, g \in K[T]$, $g \neq 0$, mit Koeffizienten aus einem Körper $K$ existieren eindeutig bestimmte Polynome $q, r \in K[T]$ mit*

$$f = qg + r, \qquad \operatorname{grad} r < \operatorname{grad} g.$$

*Beweis zu Satz* 2. Wir beginnen mit der Existenzaussage. Für $\operatorname{grad} f < \operatorname{grad} g$ gilt die gewünschte Zerlegung trivialerweise mit $q = 0$ und $r = f$. Hat man andererseits

$$m = \operatorname{grad} f \geq \operatorname{grad} g = n,$$

so sei $a$ (bzw. $b$) der höchste Koeffizient von $f$ (bzw. $g$), und man setze

$$q_1 := \frac{a}{b} \cdot T^{m-n}, \qquad f_1 := f - q_1 g.$$

Dann gilt

$$\operatorname{grad}(q_1 g) = \operatorname{grad} q_1 + \operatorname{grad} g = (m - n) + n = m = \operatorname{grad} f$$

nach 5.1/2, und die höchsten Koeffizienten von $q_1 g$ und $f$ stimmen überein. Insbesondere ergibt sich

$$f = q_1 g + f_1, \qquad \operatorname{grad} f_1 < \operatorname{grad} f.$$

Im Falle $\operatorname{grad} f_1 < \operatorname{grad} g$ erhält man die gewünschte Zerlegung mit $q = q_1$ und $r = f_1$. Falls aber $\operatorname{grad} f_1 \geq \operatorname{grad} g$ gilt, so kann man nach dem gerade beschriebenen Verfahren fortfahren und eine Zerlegung

$$f_1 = q_2 g + f_2, \qquad \operatorname{grad} f_2 < \operatorname{grad} f_1,$$

finden usw. Nach endlich vielen Schritten gelangt man schließlich zu einer Zerlegung

$$f_{k-1} = q_k g + f_k$$

mit $\operatorname{grad} f_k < \operatorname{grad} g$. Dann ist

$$f = (q_1 + \ldots + q_k)g + f_k$$

die gewünschte Zerlegung von $f$.

Um nun auch die Eindeutigkeitsaussage herzuleiten, betrachte man Zerlegungen

$$f = qg + r = q'g + r'$$

mit $\operatorname{grad} r, \operatorname{grad} r' < \operatorname{grad} g$. Sodann hat man

$$0 = (q - q')g + (r - r') \qquad \text{bzw.} \qquad (q - q')g = r' - r.$$

Gilt nun $q - q' \neq 0$, so folgt $\operatorname{grad}(q - q') \geq 0$ und damit gemäß 5.1/2

$$\operatorname{grad}((q - q')g) = \operatorname{grad}(q - q') + \operatorname{grad} g \geq \operatorname{grad} g.$$

Andererseits hat man aber

$$\operatorname{grad}(r' - r) \leq \max\{\operatorname{grad} r', \operatorname{grad} r\} < \operatorname{grad} g,$$

was der vorhergehenden Abschätzung widerspricht. Also folgt $q = q'$ und damit $r = r'$. □

Ringe, in denen eine Division wie in den Sätzen 1 oder 2 möglich ist, werden als *euklidische Ringe* bezeichnet, genauer:

**Definition 3.** *Ein Integritätsring $R$ heißt ein* euklidischer Ring, *wenn es eine Abbildung $\delta\colon R - \{0\} \longrightarrow \mathbb{N}$ (eine so genannte Gradfunktion) mit folgender Eigenschaft gibt: Zu $a, b \in R$, $b \neq 0$, existieren jeweils (nicht notwendig eindeutig bestimmte) Elemente $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\delta(r) < \delta(b)$.*

Wir können daher feststellen:

**Korollar 4.** *Der Ring $\mathbb{Z}$ der ganzen Zahlen und der Polynomring $K[T]$ über einem Körper $K$ sind euklidische Ringe. Als Gradfunktion nehme man im ersten Fall den Absolutbetrag, im zweiten den gewöhnlichen Grad von Polynomen.*

**Definition 5.** *Ein Integritätsring $R$ heißt* Hauptidealring, *wenn jedes Ideal $\mathfrak{a} \subset R$ ein Hauptideal ist, also die Gestalt $\mathfrak{a} = (a)$ mit einem Element $a \in R$ besitzt.*

**Satz 6.** *Es sei $R$ ein euklidischer Ring. Dann ist $R$ auch ein Hauptidealring.*

*Beweis.* Es sei $\mathfrak{a} \subset R$ ein Ideal. Um zu zeigen, dass $\mathfrak{a}$ ein Hauptideal ist, dürfen wir $\mathfrak{a} \neq 0$ annehmen, denn anderenfalls gilt $\mathfrak{a} = 0 = (0)$. Sei nun $a \in \mathfrak{a} - \{0\}$ ein Element, für das der "Grad" $\delta(a)$ minimal ist. Wir behaupten, dass dann $\mathfrak{a} = (a)$ gilt. Natürlich gilt $(a) \subset \mathfrak{a}$. Um auch die umgekehrte Inklusion zu zeigen, wählen wir ein Element $a' \in \mathfrak{a}$. Da $R$ euklidisch ist, gibt es Elemente $q, r \in R$ mit $a' = qa + r$, wobei $r$ entweder verschwindet oder $\delta(r) < \delta(a)$ erfüllt. Nun hat man aber $r = a' - qa \in \mathfrak{a}$, so dass aufgrund der Wahl von $a$ notwendig $r = 0$ und damit $a' = qa \in (a)$ folgt. Es gilt daher $\mathfrak{a} \subset (a)$, insgesamt also $\mathfrak{a} = (a)$, und $R$ ist ein Hauptidealring. □

**Korollar 7.** *Der Ring $\mathbb{Z}$ der ganzen Zahlen und der Polynomring $K[T]$ über einem Körper $K$ sind Hauptidealringe.*

Wir wollen als Nächstes den Teilbarkeitsbegriff in einem Integritätsring einführen.

**Definition 8.** *Es seien $a, b$ Elemente eines Integritätsrings $R$.*

(i) *Man sagt, $a$* teile *$b$ oder $a$ sei ein* Teiler *von $b$, in Zeichen $a \mid b$, wenn es ein $c \in R$ mit $ac = b$ gibt. Ist $a$ kein Teiler von $b$, so schreibt man $a \nmid b$.*

(ii) *$a$ und $b$ heißen* assoziiert, *wenn es eine Einheit $e \in R^*$ mit $ae = b$ gibt.*

Es ist also $a$ genau dann ein Teiler von $b$, wenn $b \in (a)$ bzw. $(b) \subset (a)$ gilt. Beispielsweise teilt $T + 1$ das Polynom $T^2 - 1$ in $K[T]$, und man hat $a \mid b$ sowie $b \mid a$, falls $a$ und $b$ assoziiert sind. Genauer kann man feststellen:

**Bemerkung 9.** *Für Elemente $a, b$ eines Integritätsrings $R$ ist äquivalent*:

(i) *$a \mid b$ und $b \mid a$.*

(ii) *$(a) = (b)$.*

(iii) *$a$ und $b$ sind assoziiert.*

*Beweis.* Wir zeigen lediglich, dass aus (ii) Bedingung (iii) folgt, alle anderen Implikationen ergeben sich mittels direkter Verifikation aus Definition 8. Gelte also $(a) = (b)$. Dann gibt es Elemente $c, d \in R$ mit $ac = b$ und $a = bd$. Hieraus folgt $a = bd = acd$, also $a \cdot (1 - cd) = 0$. Gilt nun $a \neq 0$, so folgt $cd = 1$, da $R$ ein Integritätsring ist, und es sind $c, d$ Einheiten in $R$. Folglich sind $a$ und $b$ assoziiert. Gleiches gilt aber auch im Falle $a = 0$, denn man hat dann insbesondere $b = ac = 0$. □

**Definition 10.** *Es sei $R$ ein Integritätsring und $p \in R$ ein Element, welches keine Einheit und von Null verschieden ist.*

(i) *$p$ heißt* irreduzibel, *wenn aus einer Gleichung $p = ab$ mit $a, b \in R$ stets folgt, dass $a$ oder $b$ eine Einheit in $R$ ist. Anderenfalls nennt man $p$* reduzibel.

(ii) *$p$ heißt* Primelement, *wenn aus $p \mid ab$ mit $a, b \in R$ stets $p \mid a$ oder $p \mid b$ folgt oder, in äquivalenter Formulierung, wenn aus $ab \in (p)$ stets $a \in (p)$ oder $b \in (p)$ folgt.*

Es ist also $p$ genau dann irreduzibel, wenn aus einer Relation $p \in (a)$ mit $a \in R$ entweder $(a) = (p)$ oder $(a) = R$ folgt. Weiter sieht man mit Induktion, dass ein Primelement $p \in R$ genau dann ein Produkt $a_1 \cdot \ldots \cdot a_r$ von Elementen aus $R$ teilt, wenn es einen der Faktoren $a_i$ teilt.

**Bemerkung 11.** *Es sei $R$ ein Integritätsring. Dann ist jedes Primelement von $R$ auch irreduzibel.*

*Beweis.* Sei $p \in R$ ein Primelement und seien $a, b \in R$ mit $p = ab$. Dann teilt $p$ das Produkt $ab$, und es folgt, dass $p$ einen der beiden Faktoren teilt, etwa $p \mid a$, d. h. es gibt eine Gleichung $a = pc$ mit $c \in R$. Setzt man dies in die Gleichung $p = ab$ ein, so erhält man $p = pcb$ bzw. $p(1 - cb) = 0$. Da $R$ ein Integritätsring und $p$ von Null verschieden ist, folgt hieraus $cb = 1$, d. h. $b$ ist eine Einheit. Mithin ist $p$ irreduzibel. Alternativ hätten wir auch die Beziehungen $a \mid p$ (wegen

$p = ab$) und $p \mid a$ verwenden können. Mit Bemerkung 9 folgt hieraus, dass $a$ und $p$ assoziiert sind. □

Wir werden sogleich zeigen, dass in Hauptidealringen auch die Umkehrung von Bemerkung 11 gilt. Insbesondere dürfen wir dann Primzahlen in $\mathbb{Z}$, die ja gemeinhin als *irreduzible* Elemente definiert werden, auch als *Primelemente* bezeichnen.

**Satz 12.** *Es sei $R$ ein Hauptidealring und $p \in R$ von 0 verschieden und keine Einheit. Dann ist äquivalent*:

(i) *$p$ ist irreduzibel.*

(ii) *$p$ ist ein Primelement.*

*Beweis.* Wir haben nur noch die Implikation (i) $\Longrightarrow$ (ii) zu zeigen. Sei also $p \in R$ ein irreduzibles Element, und gelte $p \mid ab$ sowie $p \nmid a$ für zwei Elemente $a, b \in R$. Um $p \mid b$ zu zeigen, betrachte man das Ideal

$$Ra + Rp := \{ra + sp\,;\, r, s \in R\}$$

in $R$, welches aufgrund unserer Voraussetzung über $R$ ein Hauptideal ist, etwa $Ra + Rp = Rd$. Insbesondere gilt $a, p \in Rd$ und folglich $d \mid a$, $d \mid p$. Nun ist $p$ aber irreduzibel. Daher folgt aus $d \mid p$ bzw. einer Gleichung $p = cd$, dass $c$ oder $d$ eine Einheit ist. Ist nun $c$ eine Einheit, so können wir $d = c^{-1}p$ schreiben, und man erhält $p \mid a$ aus $d \mid a$, im Widerspruch zu $p \nmid a$. Somit bleibt nur der Fall übrig, dass $d$ eine Einheit ist, d. h. es gilt $Ra + Rp = R$ und, nach Multiplikation mit $b$, die Gleichung $Rab + Rpb = Rb$. Es existieren also $r, s \in R$ mit $rab + spb = b$. Wegen $p \mid ab$ folgt hieraus wie gewünscht $p \mid b$. □

**Korollar 13.** *In einem Hauptidealring $R$ lässt sich jedes Element $a \in R - \{0\}$, welches keine Einheit ist, als endliches Produkt von Primelementen schreiben.*

*Beweis.* Da jedes irreduzible Element von $R$ bereits prim ist, genügt es, eine Faktorisierung in irreduzible Elemente zu konstruieren. Sei also $a \in R - \{0\}$ eine Nichteinheit. Wir gehen indirekt vor und nehmen an, dass sich $a$ nicht als endliches Produkt irreduzibler Elemente schreiben lässt. Dann ist $a$ reduzibel, und man kann $a$ folglich als Produkt $a_1 a_1'$ zweier Nichteinheiten aus $R$ schreiben. Da $a$ keine endliche Faktorisierung in irreduzible Elemente besitzt, gilt dasselbe für mindestens einen der beiden Faktoren $a_1, a_1'$, etwa für $a_1$, und wir können $a_1$ wiederum als Produkt $a_2 a_2'$ zweier Nichteinheiten aus $R$ schreiben. Fährt man auf diese Weise fort, so erhält man eine Folge von Elementen

$$a = a_0, a_1, a_2, \ldots \in R,$$

so dass $a_{i+1}$ jeweils ein Teiler von $a_i$, aber nicht assoziiert zu $a_i$ ist. Mit anderen Worten, man erhält eine aufsteigende Folge von Idealen

$$(a) = (a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots,$$

wobei es sich hier gemäß Bemerkung 9 jeweils um echte Inklusionen handelt. Man prüft nun leicht nach, dass die Vereinigung einer aufsteigenden Folge von Idealen wiederum ein Ideal ergibt. Wir können also durch $\mathfrak{b} = \bigcup_{i=0}^{\infty}(a_i)$ ein Ideal in $R$ definieren, und zwar ein Hauptideal, da $R$ ein Hauptidealring ist. Folglich existiert ein Element $b \in \mathfrak{b}$ mit $\mathfrak{b} = (b)$. Nach Definition von $\mathfrak{b}$ gibt es dann einen Index $i_0 \in \mathbb{N}$ mit $b \in (a_{i_0})$, und es folgt

$$\mathfrak{b} = (b) \subset (a_{i_0}) \subset (a_i) \subset \mathfrak{b}$$

für $i \geq i_0$, also $(a_{i_0}) = (a_i)$ für $i \geq i_0$, im Widerspruch dazu, dass die Kette der Ideale $(a_i)$ echt aufsteigend ist. □

Als Nächstes wollen wir zeigen, dass Faktorisierungen in Primelemente im Wesentlichen eindeutig sind.

**Lemma 14.** *In einem Integritätsring $R$ habe man die Gleichung*

$$p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

*für Primelemente $p_1, \ldots, p_r \in R$ und irreduzible Elemente $q_1, \ldots, q_s \in R$. Dann gilt $r = s$, und nach Umnummerierung der $q_1, \ldots, q_s$ existieren Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in R^*$ mit $q_i = \varepsilon_i p_i$ für $i = 1, \ldots, r$, d. h. $p_i$ ist jeweils assoziiert zu $q_i$.*

*Beweis.* Aus $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ folgt insbesondere $p_1 \,|\, q_1 \cdot \ldots \cdot q_s$. Da $p_1$ ein Primelement ist, gibt es ein $i$ mit $p_1 \,|\, q_i$, und wir können durch Umnummerierung der $q_1, \ldots, q_s$ annehmen, dass $i = 1$ und somit $p_1 \mid q_1$ gilt. Man hat also eine Gleichung $q_1 = \varepsilon_1 p_1$, wobei $\varepsilon_1$ aufgrund der Irreduzibilität von $q_1$ eine Einheit ist. Da wir uns in einem Integritätsring befinden, ergibt sich hieraus

$$p_2 \cdot \ldots \cdot p_r = \varepsilon_1 q_2 \cdot \ldots \cdot q_s.$$

In gleicher Weise zeigt man nun, dass $p_2$ zu einem der Elemente $q_2, \ldots, q_s$ assoziiert ist usw. Man kann also $q_1, \ldots, q_s$ so umnummerieren, dass $p_i$ für $i = 1, \ldots, r$ jeweils zu $q_i$ assoziiert ist. Insbesondere folgt $r \leq s$. Nach "Auskürzen" aller $p_i$ aus der Gleichung $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ verbleibt eine Gleichung des Typs

$$1 = q_{r+1} \cdot \ldots \cdot q_s,$$

welche zeigt, dass das System der $q_{r+1}, \ldots, q_s$ aus Einheiten besteht. Da alle $q_i$ zugleich irreduzibel sind, also keine Einheiten sein können, ist das System leer, und es gilt folglich $r = s$. □

Man sagt, in einem Integritätsring $R$ gelte der *Satz von der eindeutigen Primfaktorzerlegung*, oder auch $R$ sei *faktoriell*, wenn sich jede Nichteinheit $a \in R - \{0\}$ als Produkt von Primelementen in $R$ schreiben lässt. Gemäß Lemma 14 ist eine solche Faktorisierung von $a$ (im Wesentlichen) eindeutig. Benutzen wir weiter, dass jedes Primelement aufgrund von Bemerkung 11 irreduzibel

ist, so kann man mit Lemma 14 schließen, dass sich in einem faktoriellen Ring jede von Null verschiedene Nichteinheit auf (im Wesentlichen) eindeutige Weise als Produkt irreduzibler Elemente schreiben lässt. Man kann darüber hinaus zeigen, dass umgekehrt die letztere Eigenschaft in einem Integritätsring dessen Faktorialität impliziert. Wir wollen jedoch auf Beweise nicht weiter eingehen, sondern nur noch Korollar 13 in neuer Sprechweise formulieren.

**Satz 15.** *Jeder Hauptidealring ist faktoriell, insbesondere also der Ring $\mathbb{Z}$ der ganzen Zahlen sowie der Polynomring $K[T]$ einer Variablen $T$ über einem Körper $K$.*

Man kann Primfaktorzerlegungen in einem faktoriellen Ring $R$ weiter standardisieren, indem man in jeder Klasse assoziierter Primelemente eines auswählt und damit ein Repräsentantensystem $P \subset R$ aller Primelemente betrachtet. Man kann dann annehmen, dass in Primfaktorzerlegungen, abgesehen von Einheiten, nur die Primelemente $p \in P$ vorkommen, und man kann darüber hinaus gleiche Primfaktoren zu Potenzen zusammenfassen. Es besitzt dann jedes Element $a \in R - \{0\}$ eine Primfaktorzerlegung der Form

$$a = \varepsilon \prod_{p \in P} p^{\mu_p(a)}$$

mit einer Einheit $\varepsilon \in R^*$ und Exponenten $\mu_p(a) \in \mathbb{Z}$, die für fast alle $p \in P$ trivial sind. Die Eindeutigkeit der Primfaktorzerlegung besagt dann, dass $\varepsilon$ und die $\mu_p(a)$ jeweils eindeutig durch $a$ bestimmt sind. Im Übrigen sieht man unmittelbar ein, dass für Elemente $a, b \in R - \{0\}$ die Teilbarkeitsbedingung $a \,|\, b$ genau dann erfüllt ist, wenn $\mu_p(a) \leq \mu_p(b)$ für alle $p \in P$ gilt.

In $\mathbb{Z}$ gibt es nur die Einheiten 1 und $-1$, und es ist üblich, $P$ als das System aller positiven Primelemente zu definieren. Im Polynomring $K[T]$ über einem Körper $K$ dagegen besteht die Einheitengruppe aufgrund von 5.1/2 aus allen nicht-trivialen konstanten Polynomen, stimmt also mit der Einheitengruppe $K^*$ von $K$ überein. Daher gibt es zu jedem Primpolynom genau ein assoziiertes Primpolynom, welches *normiert* ist, d. h. 1 als höchsten Koeffizienten besitzt, und man definiert $P$ als das System aller normierten Primpolynome.

Wie gewöhnlich lässt sich für zwei von Null verschiedene Elemente $a, b \in R$ mit Primfaktorzerlegung

$$a = \varepsilon \prod_{p \in P} p^{\mu_p(a)}, \qquad b = \delta \prod_{p \in P} p^{\mu_p(b)}$$

der *größte gemeinsame Teiler*

$$\mathrm{ggT}(a, b) = \prod_{p \in P} p^{\min(\mu_p(a), \mu_p(b))}$$

erklären. Dies ist ein gemeinsamer Teiler $d$ von $a$ und $b$ mit der charakterisierenden Eigenschaft, dass aus $t \,|\, a$ und $t \,|\, b$ stets $t \,|\, d$ folgt.

Entsprechend kann man zu $a$ und $b$ das *kleinste gemeinsame Vielfache*

$$\mathrm{kgV}(a,b) = \prod_{p\in P} p^{\max(\mu_p(a),\mu_p(b))}$$

betrachten. Dies ist ein gemeinsames Vielfaches $v$ von $a$ und $b$, so dass jedes weitere gemeinsame Vielfache von $a$ und $b$ auch ein Vielfaches von $v$ ist. Man beachte jedoch, dass die Elemente $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$ nur bis auf Einheiten wohldefiniert sind, da sie außer von $a$ und $b$ noch von der speziellen Wahl von $P$ abhängen.

In Hauptidealringen lässt sich der größte gemeinsame Teiler zweier Elemente $a,b \in R$ idealtheoretisch charakterisieren, was vielfach von Nutzen ist. Hierzu betrachtet man

$$Ra + Rb := \{ra + sb\,;\, r,s \in R\}$$

als Ideal in $R$, wobei die definierenden Eigenschaften eines Ideals leicht zu verifizieren sind.

**Satz 16.** *Es seien $a,b$ zwei von Null verschiedene Elemente eines Hauptidealrings $R$. Für den größten gemeinsamen Teiler $d = \mathrm{ggT}(a,b)$ gilt dann*

$$Ra + Rb = Rd.$$

*Insbesondere gibt es eine Gleichung $ra + sb = d$ mit Elementen $r,s \in R$, die notwendig teilerfremd sind, d. h. $\mathrm{ggT}(r,s) = 1$ erfüllen.*

*Beweis.* Das Ideal $Ra + Rb \subset R$ ist ein Hauptideal, etwa $Ra + Rb = Rd'$. Dann folgt wegen $a,b \in Rd'$, dass $d'$ ein gemeinsamer Teiler von $a,b$ und damit auch von $d$ ist. Andererseits besteht wegen $Ra + Rb = Rd'$ eine Gleichung des Typs $ra + sb = d'$ mit gewissen Elementen $r,s \in R$. Dies zeigt, dass jeder gemeinsame Teiler von $a,b$ auch ein Teiler von $d'$ ist. Insbesondere gilt also $d \,|\, d'$. Zusammen mit $d' \,|\, d$ ergibt sich gemäß Bemerkung 9, dass $d$ und $d'$ assoziiert sind. Somit gilt $Ra + Rb = Rd$, wie behauptet, und man hat eine Gleichung des Typs $ra + sb = d$. Letztere besagt, dass jeder gemeinsame Teiler von $a,b$, multipliziert mit $\mathrm{ggT}(r,s)$, einen Teiler von $d$ ergibt. Dies ist aber nur im Falle $\mathrm{ggT}(r,s) = 1$ möglich. □

Abschließend wollen wir noch aus Satz 16 eine spezielle Eigenschaft von Primelementen in Hauptidealringen folgern.

**Korollar 17.** *Es sei $R$ ein Hauptidealring und $p \in R - \{0\}$. Dann ist äquivalent:*

(i) *$p$ ist ein Primelement.*
(ii) *Der Restklassenring $R/(p)$ ist ein Körper.*

*Beweis.* Sei zunächst $p$ ein Primelement. Insbesondere ist $p$ dann keine Einheit und somit $R/(p)$ nicht der Nullring. Um einzusehen, dass $R/(p)$ ein Körper ist, wähle man $\overline{a} \in R/(p) - \{0\}$. Es ist zu zeigen, dass es ein $\overline{b} \in R/(p)$ mit $\overline{b} \cdot \overline{a} = 1$

gibt oder, in äquivalenter Formulierung, dass es zu $a \in R - (p)$ eine Gleichung der Form

$$ba + rp = 1$$

mit $b, r \in R$ gibt. Letzteres folgt aber aus Satz 16, da $a$ und $p$ offenbar teilerfremd sind.

Wenn andererseits $p$ kein Primelement ist, so ist $p$ entweder eine Einheit, oder aber es gibt von Null verschiedene Nichteinheiten $a, b \in R$ mit $p \nmid a$, $p \nmid b$, sowie $p \mid ab$. Im ersten Fall ist der Restklassenring $R/(p)$ der Nullring. Im zweiten sind die Restklassen $\overline{a}, \overline{b} \in R/(p)$ zu $a, b$ von Null verschieden, erfüllen aber $\overline{a} \cdot \overline{b} = 0$. Es ist also $R/(p)$ in beiden Fällen kein Integritätsring und damit insbesondere kein Körper. □

Als Anwendung sehen wir, dass für $p \in \mathbb{Z}$ der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ genau dann ein Körper ist, wenn $p$ prim ist. Insbesondere ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{N}$ ein Körper mit $p$ Elementen.

Genauso folgt für einen Körper $K$ und Polynome $f \in K[T]$, dass der Restklassenring $K[T]/(f)$ genau dann ein Körper ist, wenn $f$ prim ist. In $\mathbb{R}[T]$ sind beispielsweise die Polynome $T - 1$ und $T^2 + 1$ irreduzibel und damit auch prim. Es gilt

$$\mathbb{R}[T]/(T-1) \simeq \mathbb{R}, \qquad \mathbb{R}[T]/(T^2+1) \simeq \mathbb{C},$$

wie man leicht mit Hilfe des Homomorphiesatzes 5.1/10 zeigen kann. Im Übrigen kann man zeigen, dass die primen Polynome in $\mathbb{R}[T]$ gerade aus allen Polynomen vom Grad 1 sowie den nullstellenfreien Polynomen vom Grad 2 gebildet werden.

Schließlich wollen wir noch die so genannte *Charakteristik* eines Körpers definieren. Ist $K$ ein Körper, so gibt es einen eindeutig bestimmten Ringhomomorphismus $\varphi\colon \mathbb{Z} \longrightarrow K$. Dieser bildet eine natürliche Zahl $n$ ab auf die $n$-fache Summe $n \cdot 1_K$ des Einselementes $1_K \in K$ und entsprechend $-n$ auf $-(n \cdot 1_K)$. Der Kern von $\varphi$ ist ein Ideal in $\mathbb{Z}$, also ein Hauptideal, und wird damit von einem eindeutig bestimmten Element $p \in \mathbb{N}$ erzeugt. Es ist $p$ entweder 0 oder ansonsten die kleinste positive natürliche Zahl mit $p \cdot 1_K = 0$. Man nennt $p$ die *Charakteristik* von $K$; diese ist entweder 0 oder aber prim, wie man ähnlich wie im zweiten Teil des Beweises zu Korollar 17 sehen kann.

## Aufgaben

1. Man betrachte die folgenden Polynome $f, g \in \mathbb{R}[T]$ und dividiere jeweils $f$ mit Rest durch $g$:
   (i) $f = T^6 + 3T^4 + T^3 - 2$, $g = T^2 - 2T + 1$,
   (ii) $f = T^n - 1$, $g = T - 1$, mit $n \in \mathbb{N} - \{0\}$,
   (iii) $f = T^n + T^{n-1} + \ldots + 1$, $g = T + 1$, mit $n \in \mathbb{N} - \{0\}$.
2. Es seien $a, b$ von Null verschiedene Elemente eines Hauptidealrings $R$. Man zeige $Ra \cap Rb = Rv$ für $v = \mathrm{kgV}(a, b)$.

3. Man bestimme alle Unterringe von $\mathbb{Q}$.
4. Es sei $R$ ein Integritätsring und $p \in R - \{0\}$. Man zeige, dass $p$ genau dann prim ist, wenn $R/(p)$ ein Integritätsring ist.
5. Man bestimme die Primfaktorzerlegung des Polynoms $T^4 - 1$ im Polynomring $\mathbb{R}[T]$.
6. Man zeige, dass der Polynomring $\mathbb{Z}[T]$ kein Hauptidealring ist.
7. Man zeige, dass $\mathbb{Z} + \mathbb{Z}i = \{x + yi \in \mathbb{C}\,;\, x, y \in \mathbb{Z}\}$ einen Unterring des Körpers der komplexen Zahlen bildet und ein Hauptidealring ist.
8. Man zeige, dass es in $\mathbb{Z}$ unendlich viele paarweise nicht-assoziierte Primelemente gibt. Gleiches gilt für den Polynomring $K[T]$ über einem Körper $K$.
9. Es sei $\mathbb{F}$ ein endlicher Körper der Charakteristik $p$, wobei $p$ den Kern des kanonischen Ringhomomorphismus $\mathbb{Z} \longrightarrow \mathbb{F}$ erzeugt. Man zeige:
   (i) $p$ ist eine Primzahl.
   (ii) Es besteht $\mathbb{F}$ aus $p^r$ Elementen, wobei $r$ eine geeignete natürliche Zahl ist.
10. Es sei $K$ ein Körper und $A$ eine $K$-Algebra mit $\dim_K A < \infty$. Für ein Element $a \in A$ zeige man: Es existiert ein eindeutig bestimmtes normiertes Polynom $f \in K[T]$ kleinsten Grades mit $f(a) = 0$.

## 5.3 Nullstellen von Polynomen

Es sei $K$ ein Körper (oder allgemeiner ein kommutativer Ring) und $A$ eine $K$-Algebra. Ein Element $t \in A$ heißt *Nullstelle* eines Polynoms $f \in K[T]$, wenn $f(t) = 0$ gilt, d. h. wenn das Bild von $f$ unter dem Einsetzungshomomorphismus $K[T] \longrightarrow A$, der $t$ anstelle der Variablen $T$ einsetzt (vgl. 5.1/7), trivial ist. Um ein Beispiel zu geben, betrachte man den Endomorphismenring $A$ eines $K$-Vektorraums $V$; dieser wird zu einer $K$-Algebra unter dem Ringhomomorphismus $K \longrightarrow A$, $c \longmapsto c \cdot \mathrm{id}_V$. Für $\dim_K V > 1$ ist leicht zu sehen, dass das Polynom $T^2 \in K[T]$ außer dem Nullelement $0 \in A$ noch weitere Nullstellen besitzt, sogar unendlich viele, wenn $K$ unendlich viele Elemente hat. Die Gleichung $\varphi^2 = 0$ für einen Endomorphismus $\varphi\colon V \longrightarrow V$ ist nämlich gleichbedeutend mit $\operatorname{im}\varphi \subset \ker\varphi$.

Wir wollen uns zunächst aber nur für Nullstellen von Polynomen $f \in K[T]$ in $K$ interessieren, wobei wir $K$ als Körper voraussetzen. Aufgrund der Nullteilerfreiheit von $K$ sind dann stärkere Aussagen möglich, beispielsweise ist das Nullelement $0 \in K$ die einzige Nullstelle in $K$ zu $T^2 \in K[T]$.

**Satz 1.** *Sei $\alpha \in K$ Nullstelle eines Polynoms $f \in K[T]$. Dann existiert ein Polynom $g \in K[T]$ mit*

$$f = (T - \alpha) \cdot g,$$

*wobei $g$ durch diese Gleichung eindeutig bestimmt ist.*

*Beweis.* Division mit Rest von $f$ durch $(T - \alpha)$ führt zu einer Gleichung

$$f = (T - \alpha) \cdot g + r$$

mit $r \in K$. Setzt man hierin $\alpha$ anstelle von $T$ ein, so ergibt sich wegen $f(\alpha) = 0$ unmittelbar $r = r(\alpha) = 0$ und damit die gewünschte Gleichung $f = (T - \alpha) \cdot g$. Die Eindeutigkeit von $g$ folgt aus der Nullteilerfreiheit von $K$ oder aus der Eindeutigkeit der Division mit Rest; vgl. 5.2/2. □

**Korollar 2.** *Sei $f \in K[T]$, $f \neq 0$. Dann besitzt $f$ nur endlich viele paarweise verschiedene Nullstellen $\alpha_1, \ldots, \alpha_r \in K$, wobei $r \leq \operatorname{grad} f$ gilt. Weiter existieren $n_1, \ldots, n_r \in \mathbb{N} - \{0\}$ sowie ein Polynom $g \in K[T]$ ohne Nullstellen in $K$ mit*

$$f = \prod_{i=1}^{r} (T - \alpha_i)^{n_i} \cdot g.$$

*Dabei sind die Exponenten $n_i$ sowie das Polynom $g$ eindeutig durch $f$ bestimmt.*

*Beweis.* Man betrachte Zerlegungen der Form

$$f = \prod_{i=1}^{r} (T - \alpha_i)^{n_i} \cdot g$$

mit paarweise verschiedenen Nullstellen $\alpha_1, \ldots, \alpha_r$ von $f$ (wobei $r$ variieren darf), Exponenten $n_i \in \mathbb{N} - \{0\}$ und einem Polynom $g \in K[T]$. Dann gilt stets

$$\operatorname{grad} f = \sum_{i=1}^{r} n_i + \operatorname{grad} g,$$

und wir können eine solche Zerlegung finden, für die grad g minimal ist. Dann ist $g$ aber wie gewünscht ohne Nullstellen in $K$, da man ansonsten gemäß Satz 1 von $g$ einen Linearfaktor der Form $T - \alpha$ abspalten könnte und dies zu einer Zerlegung mit einem echt kleineren Grad von $g$ führen würde. Man erkennt dann, dass $\alpha_1, \ldots, \alpha_r$ aufgrund der Nullteilerfreiheit von $K$ die einzigen Nullstellen von $f$ sind und dass $r \leq \operatorname{grad} f$ gilt.

Die Faktoren $(T - \alpha_i)$ sind irreduzibel und damit insbesondere prim. Die Eindeutigkeitsaussage folgt daher leicht aus der Eindeutigkeit der Primfaktorzerlegung in $K[T]$. Man benutze dabei, dass in der Primfaktorzerlegung von $g$ lediglich Faktoren vom Grad $\geq 2$ vorkommen können, da $g$ keine Nullstellen in $K$ besitzt. □

In der vorstehenden Situation nennt man $n_i$ die *Vielfachheit* der Nullstelle $\alpha_i$. Weiter bezeichnet man einen Körper $K$ als *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $f \in K[T]$ (mindestens) eine Nullstelle in $K$ besitzt. In der Zerlegung von Korollar 2 ist $g$ dann konstant. Man kann daher sagen, dass ein Körper $K$ genau dann algebraisch abgeschlossen ist, wenn sich jedes nicht-konstante Polynom $f \in K[T]$ als Produkt von Linearfaktoren, d. h. Polynomen vom Grad 1 schreiben lässt oder, in äquivalenter Weise, wenn die

irreduziblen Polynome in $K[T]$ gerade die Polynome vom Grad 1 sind. Wir wollen in diesem Zusammenhang den so genannten *Fundamentalsatz der Algebra* formulieren.

**Theorem 3.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Der Beweis erfordert Hilfsmittel, die über die lineare Algebra hinausgehen. Er wird üblicherweise im Rahmen der Funktionentheorie- oder Algebra-Vorlesungen geführt. Als Beispiel wollen wir hier nur noch anfügen, dass die Polynome

$$T^2 - 2 \in \mathbb{Q}[T],$$
$$T^2 + 1 \in \mathbb{R}[T],$$
$$T^2 + T + 1 \in \mathbb{F}_2[T]$$

keine Nullstellen in den jeweiligen Körpern besitzen. Da es sich um Polynome vom Grad 2 handelt, folgt hieraus, dass diese irreduzibel und damit prim sind.

## Aufgaben

1. Es sei $K$ ein Körper. Für ein Polynom $f = \sum_{i\in\mathbb{N}} a_i T^i \in K[T]$ definiere man dessen Ableitung durch $f' := \sum_{i>0} i a_i T^{i-1}$, wobei $ia_i$ jeweils als $i$-fache Summe von $a_i$ zu verstehen ist. Man zeige: Ein Element $\alpha \in K$ ist genau dann eine mehrfache Nullstelle (d. h. der Ordnung $> 1$) von $f$, wenn $\alpha$ Nullstelle von $\mathrm{ggT}(f, f')$ ist.
2. Es sei $K$ ein Körper und $A$ eine $K$-Algebra. Für Polynome $f, g \in K[T] - \{0\}$ und $h = \mathrm{ggT}(f, g)$ zeige man: Ist $a \in A$ eine gemeinsame Nullstelle von $f$ und $g$, so ist $a$ auch Nullstelle von $h$. (Hinweis: Man benutze die in 5.2/16 beschriebene Charakterisierung des größten gemeinsamen Teilers.)
3. Für eine komplexe Zahl $\alpha = u + iv \in \mathbb{C}$ mit Realteil $u$ und Imaginärteil $v$ sei die zugehörige konjugiert komplexe Zahl definiert durch $\overline{\alpha} = u - iv$. Man zeige, dass ein normiertes Polynom $f \in \mathbb{R}[T]$ genau dann prim ist, wenn es von der Form $f = T - \alpha$ mit $\alpha \in \mathbb{R}$ oder $f = (T - \alpha)(T - \overline{\alpha})$ mit $\alpha \in \mathbb{C} - \mathbb{R}$ ist. (Hinweis: Man betrachte die Abbildung $\mathbb{C} \longrightarrow \mathbb{C}$, $\alpha \longmapsto \overline{\alpha}$, welche die Eigenschaften eines $\mathbb{R}$-Algebraisomorphismus besitzt, und setze diese fort zu einem $\mathbb{R}[T]$-Algebraisomorphismus $\mathbb{C}[T] \longrightarrow \mathbb{C}[T]$.)