

Kapitel 2

Ringe

Eine zentrale Aufgabe der Algebra ist es, Aussagen über die Nullstellen von Polynomen zu machen. Für den Umgang mit Polynomen ist es nützlich, die abstrakten Hintergründe der Addition und Multiplikation zu formalisieren und die Analogien zu den entsprechenden Operationen mit ganzen Zahlen zu nutzen. Das ist der Ursprung der Theorie der Ringe. Als Hilfsmittel in der Körpertheorie sind vor allem die Kriterien für die Irreduzibilität aus 2.3.8 wichtig. Weitergehende Ergebnisse der Idealtheorie stellen die Grundlage für die algebraische Geometrie dar.

2.1 Grundbegriffe

2.1.1 Definition eines Rings

Im Gegensatz zu Gruppen gibt es in einem Ring R zwei Verknüpfungen: Eine Addition, mit der R zu einer abelschen Gruppe wird, und eine Multiplikation mit der R nur eine Halbgruppe sein muss. Die beiden Verknüpfungen sind durch Distributivgesetze gekoppelt. Ausführlich aufgeschrieben hat man folgende

Definition Ein **Ring** ist eine Menge R zusammen mit zwei inneren Verknüpfungen $+$ und \cdot , die folgende Bedingungen erfüllen:

R1 R zusammen mit der Addition $+$ ist eine abelsche Gruppe.

R2 Die Multiplikation \cdot ist assoziativ.

R3 Es gelten die **Distributivgesetze**, d.h. für alle $a, b, c \in R$ ist

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Das neutrale Element $0 \in R$ der Addition heißt **Nullelement** von R .

Wenn deutlich gemacht werden soll, um welche Verknüpfungen es sich handelt, kann man einen Ring als Tripel $(R, +, \cdot)$ schreiben. Um Klammern zu sparen, gilt die übliche Regel „Punkt vor Strich“, zudem lässt man den Malpunkt meist weg.

Offensichtlich ist die Bedingung für die Multiplikation weit schwächer als für die Addition. Für zusätzliche Eigenschaften der Multiplikation gibt es Namen:

Ein Ring heißt **kommutativ**, wenn die Multiplikation kommutativ ist, d. h.

$$a \cdot b = b \cdot a \quad \text{für alle } a, b \in R.$$

Ein Element $1 \in R$ heißt **Einselement**, wenn $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$. Dass beide Bedingungen nötig sind, sieht man am Beispiel 2 aus 1.1.2.

Aus den Distributivgesetzen folgen weitere elementare Regeln über den Zusammenhang von Addition und Multiplikation:

Bemerkung 1 In einem Ring R gilt:

$$a) \quad a0 = 0a = 0, \quad (-a)b = a(-b) = -(ab), \quad (-a)(-b) = ab.$$

$$b) \quad \text{Hat } R \text{ ein Einselement } 1, \text{ so gilt } 1 = 0 \text{ genau dann, wenn } R = \{0\} \text{ der Nullring ist.}$$

$$\text{Beweis } a) \quad a0 = a(0+0) = a0 + a0, \quad 0a = (0+0)a = 0a + 0a,$$

$$ab + (-a)b = (a-a)b = 0, \quad ab + a(-b) = a(b-b) = 0,$$

$$(-a)(-b) = a(-(-b)) = ab.$$

$$b) \quad \text{Ist } R = \{0\}, \text{ so hat offensichtlich } 0 \text{ die Eigenschaft eines Einselements. Ist umgekehrt } 1 = 0, \text{ so folgt } a = 1a = 0a = 0 \text{ für jedes } a \in R. \quad \blacksquare$$

Ein $a \in R$ heißt **rechter** bzw. **linker Nullteiler**, wenn es ein $x \in R$ mit $x \neq 0$ gibt, so dass

$$x \cdot a = 0 \quad \text{bzw.} \quad a \cdot x = 0.$$

Nach der obigen Bemerkung ist 0 sowohl rechter als auch linker Nullteiler. R heißt **nullteilerfrei**, wenn es keine rechten oder linken Nullteiler außer 0 gibt, d. h. wenn aus $a \cdot b = 0$ stets $a = 0$ oder $b = 0$ folgt.

Die Beziehung von einem $a \in R$ zu den Abbildungen

$$r_a : R \rightarrow R, x \mapsto x \cdot a, \quad \text{und} \quad l_a : R \rightarrow R, x \mapsto a \cdot x,$$

ist einfach: a ist genau dann rechter bzw. linker Nullteiler, wenn r_a bzw. l_a nicht injektiv ist.

Denn gibt es ein $x \neq 0$ mit $x \cdot a = 0$ bzw. $a \cdot x = 0$, so ist $r_a(x) = r_a(0) = 0$ bzw. $l_a(x) = l_a(0) = 0$.

Gibt es umgekehrt $x, y \in R$ mit $x \neq y$ derart, dass

$$r_a(x) = r_a(y), \quad \text{d. h. } x \cdot a = y \cdot a, \quad \text{so folgt } (x - y) \cdot a = 0,$$

analog für l_a .

Damit ergibt sich die folgende

Bemerkung 2 Für einen Ring R sind folgende Bedingungen gleichwertig:

- i) R ist nullteilerfrei.
- ii) $R \setminus \{0\}$ ist multiplikativ abgeschlossen.
- iii) Für $a, x, y \in R$ und $a \neq 0$ gelten die Kürzungsregeln

$$x \cdot a = y \cdot a \Rightarrow x = y \quad \text{und} \quad a \cdot x = a \cdot y \Rightarrow x = y.$$

Schließlich nennt man einen Ring **Integritätsring**, wenn er folgende Bedingungen erfüllt:

- 1) R hat ein Einselement $1 \neq 0$.
- 2) R ist kommutativ.
- 3) R ist nullteilerfrei.

2.1.2 Einheiten, Körper, Unterringe

Im Gegensatz zur Addition haben Ringelemente im Allgemeinen kein Inverses bezüglich der Multiplikation. Das führt zu einer neuen

Definition Ist R ein Ring mit 1 , so heißt ein $a \in R$ **Einheit**, wenn es ein $\tilde{a} \in R$ gibt mit

$$a\tilde{a} = \tilde{a}a = 1.$$

Ist R nicht kommutativ, so sind in der Tat beide Bedingungen nötig (Beispiel 5 in 2.1.4).

Bemerkung In einem Ring R mit 1 ist die Menge

$$R^\times := \{a \in R : a \text{ ist Einheit}\} \subset R$$

bezüglich der Multiplikation eine Gruppe. R^\times heißt **Einheitengruppe** von R .

Beweis R^\times ist multiplikativ abgeschlossen, denn sind $a, b \in R^\times$, so gibt es $\tilde{a}, \tilde{b} \in R$ mit

$$a\tilde{a} = \tilde{a}a = b\tilde{b} = \tilde{b}b = 1, \text{ also } (ab)(\tilde{b}\tilde{a}) = (\tilde{b}\tilde{a})(ab) = 1.$$

Außerdem ist $1 \in R^\times$ und zu $a \in R^\times$ ist \tilde{a} ein Inverses. ■

Ist $1 \neq 0$, so gilt $R^\times \subset R^* := R \setminus \{0\}$. Besonders wichtig ist der Extremfall $R^\times = R^*$, d.h. jedes $a \neq 0$ hat als Element der Gruppe R^\times nach 1.1.3 ein eindeutiges Inverses $a^{-1} \in R^\times$. Das führt zur folgenden

Definition Ein **Körper** ist eine Menge K zusammen mit zwei inneren Verknüpfungen $+$ und \cdot , die folgende Bedingungen erfüllen:

K1 K zusammen mit der Addition ist eine abelsche Gruppe mit neutralem Element 0 und Inversem $-a$ von a .

K2 $K \setminus \{0\}$ zusammen mit der Multiplikation ist eine abelsche Gruppe mit neutralem Element 1 und Inversem a^{-1} von a .

K3 Für $a, b, c \in K$ gilt das Distributivgesetz

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

Sind diese Bedingungen mit Ausnahme der Kommutativität der Multiplikation in **K2** erfüllt, so spricht man von einem **Schiefkörper** (in diesem Fall muss man das Distributivgesetz **K3** auch in der anderen Reihenfolge fordern).

In 2.1.13 werden wir zeigen, dass man jeden Integritätsring R zu einem Körper $Q(R)$, dem Quotientenkörper, erweitern kann. Ist R endlich, so ist die Erweiterung gar nicht nötig:

Lemma Ein endlicher Integritätsring ist ein Körper.

Beweis Ist $a \in R$ mit $a \neq 0$ gegeben, so betrachten wir die Abbildung

$$l_a : R \rightarrow R, x \mapsto ax.$$

In einem Integritätsring ist l_a injektiv, ist R endlich auch surjektiv. Also gibt es ein $b \in R$ mit $ab = 1$. ■

Nun zum nächsten grundlegenden Begriff:

Definition Ist R ein Ring und $S \subset R$ eine Teilmenge, so heißt S **Unterring** von R , wenn gilt:

- 1) Für $a, b \in S$ ist auch $a + b \in S$ und $a \cdot b \in S$.
- 2) S mit den von R geerbten Verknüpfungen $+$ und \cdot ist wieder ein Ring.

Diese Definition folgt dem allgemeinen Schema für eine Unterstruktur. Für die Praxis verwendet man wieder ein der speziellen Situation angepasstes handlicheres Kriterium:

Bemerkung Eine Teilmenge $S \subset R$ ist genau dann Unterring, wenn folgendes gilt:

- a) $S \neq \emptyset$.
- b) $a, b \in S \Rightarrow a - b \in S$ und $a \cdot b \in S$.

Der *Beweis* folgt sofort aus dem entsprechenden Kriterium für Untergruppen in 1.1.6.

Ist schließlich K ein Körper, so heißt $L \subset K$ ein **Unterkörper**, wenn L ein Körper und ein Unterring ist. K heißt dann **Oberkörper** von L . Man nennt $K \supset L$ auch **Körpererweiterung**. Damit beschäftigen wir uns ausführlich in Kapitel 3.

Wie bei Gruppen sieht man, dass der Durchschnitt beliebig vieler Unterringe S eines Ringes R wieder ein Unterring ist. Also kann man für eine Teilmenge $M \subset R$ den von M **erzeugten Unterring**

$$\text{Erz}(M) := \bigcap_{M \subset S \subset R} S$$

erklären. Ist $S \subset R$ Unterring und $a \in R$, so ist die Notation

$$S[a] := \text{Erz}(S \cup \{a\})$$

üblich. Man sagt dafür, a wird zu S **adjungiert**. Wie $S[a]$ mit Hilfe von Polynomen genauer beschrieben werden kann, zeigen wir in 3.1.3.

2.1.3 Ringhomomorphismen

Die mit Addition und Multiplikation verträglichen Abbildungen zwischen Ringen nennt man wieder „Homomorphismen“:

Definition Sind $(R, +, \cdot)$ und $(R', +', \cdot')$ Ringe, so heißt eine Abbildung

$$\varphi : R \rightarrow R'$$

Ringhomomorphismus, wenn für alle $a, b \in R$ gilt:

$$\varphi(a + b) = \varphi(a) +' \varphi(b) \quad \text{und} \quad \varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b).$$

Die Begriffe **Monomorphismus**, **Epimorphismus**, **Isomorphismus**, **Endomorphismus** und **Automorphismus** erklärt man wie bei Gruppen (1.2.1).

Ist $\varphi : R \rightarrow R'$ ein Ringhomomorphismus, so heißt

$$\text{Ker } \varphi = \{a \in R : \varphi(a) = 0\} \subset R$$

der **Kern** von φ und $\text{Im } \varphi = \varphi(R) \subset R'$ das **Bild** von φ . Man beachte, dass bei der Definition des Kerns nur das neutrale Element der Addition vorkommt.

Wir notieren einige elementare Eigenschaften von Ringhomomorphismen:

Bemerkung a) Ist $\varphi : R \rightarrow R'$ ein Ringhomomorphismus, so sind $\text{Ker } \varphi \subset R$ und $\text{Im } \varphi \subset R'$ Unterringe.

b) Sind $\varphi : R \rightarrow R'$ und $\psi : R' \rightarrow R''$ Ringhomomorphismen, so ist auch $\psi \circ \varphi : R \rightarrow R''$ Ringhomomorphismus.

c) Ist $\varphi : R \rightarrow R'$ Ringisomorphismus (d.h. bijektiver Homomorphismus), so ist $\varphi^{-1} : R' \rightarrow R$ Ringisomorphismus.

d) Ist $S \subset R$ Unterring, so ist die Inklusion $\iota : S \rightarrow R$ Ringhomomorphismus.

e) Ein Ringhomomorphismus $\varphi : R \rightarrow R'$ ist genau dann injektiv, wenn $\text{Ker } \varphi = \{0\}$.

Die *Beweise* sind ganz einfach.

Dass $\text{Ker } \varphi \subset R$ ein Unterring ist, sieht man so: Ist $\varphi(a) = \varphi(b) = 0$, so folgt

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0 \quad \text{und} \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = 0 \cdot 0 = 0. \quad \blacksquare$$

Da Ringe mit der Addition abelsche Gruppen sind, müssen Ringhomomorphismen die Nullelemente ineinander überführen. Existieren zusätzlich Einselemente, so muss das nicht der Fall sein. Etwa für

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z} \quad \text{mit} \quad \varphi(n) = 0 \quad \text{für alle } n \in \mathbb{Z}$$

ist $\varphi(1) = 0 \neq 1$. Unter einer zusätzlichen Voraussetzung kann man mehr sagen:

Lemma 1 *Ist $\varphi : R \rightarrow R'$ ein surjektiver Ringhomomorphismus, und $1 \in R$ ein Einselement, so ist $\varphi(1) \in R'$ ein Einselement in R' . Gibt es insbesondere ein Einselement $1' \in R'$, so folgt $\varphi(1) = 1'$.*

Beweis Zu $b \in R'$ gibt es ein $a \in R$ mit $b = \varphi(a)$. Dann folgt

$$\varphi(1) \cdot b = \varphi(1) \cdot \varphi(a) = \varphi(1 \cdot a) = \varphi(a) = b$$

und analog $b \cdot \varphi(1) = b$. Da neutrale Elemente in Halbgruppen nach der Bemerkung in 1.1.1 eindeutig sind, folgt $\varphi(1) = 1'$. Im extremen Fall eines Nullrings $R' = \{0'\}$ ist $\varphi(1) = 0'$. \blacksquare

Ringhomomorphismen haben für Körper zusätzliche Eigenschaften:

Lemma 2 *Sei K ein Körper, R ein Ring und $\varphi : K \rightarrow R$ ein Ringhomomorphismus. Dann ist entweder $\varphi(a) = 0$ für alle $a \in K$ oder φ ist injektiv und $\varphi(K)$ ist ein Körper mit Einselement $\varphi(1)$.*

Ist auch R ein Körper, so ist $\varphi(K) \subset R$ ein Unterkörper und $\varphi(1) = 1$.

Beweis Angenommen φ ist nicht injektiv. Dann gibt es nach Teil e) der obigen Bemerkung ein $a \in K \setminus \{0\} = K^\times$ mit $\varphi(a) = 0$. Daraus folgt

$$\varphi(1) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = 0 \quad \text{und} \quad \varphi(b) = \varphi(1 \cdot b) = \varphi(1) \cdot \varphi(b) = 0$$

für alle $b \in K$. Ist φ injektiv, so ergibt sich ein Isomorphismus $K \rightarrow \varphi(K)$, also ist $\varphi(K)$ ein Körper. Ist auch R ein Körper, so ist die Beschränkung

$$\varphi^\times : K^\times \rightarrow R^\times$$

ein Homomorphismus von multiplikativen Gruppen, also $\varphi^\times(1) = 1$. \blacksquare

2.1.4 Beispiele

Das für die späteren Untersuchungen wichtigste Beispiel eines Ringes ist der Polynomring, dafür ist Abschnitt 2.1.5 reserviert. Wir geben zunächst einige andere Beispiele.

Beispiel 1 Die ganzen Zahlen \mathbb{Z} mit Addition und Multiplikation bilden einen Integritätsring. Ein formaler Beweis dieser Eigenschaften stützt sich auf die PEANO-Axiome. Die dazu nötigen „Peano-Spielereien“ findet man etwa bei [ArM, 10.2] oder [Eb, Kap. 1].

Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ aus 1.1.8 ist kommutativ mit Einselement $1 + m\mathbb{Z}$, und genau dann nullteilerfrei, wenn m eine Primzahl ist. Die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ ist die Primrestklassengruppe aus 1.3.14.

Beispiel 2 \mathbb{Z} ist ein Unterring des Körpers

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$

der rationalen Zahlen. In 2.1.13 werden wir in Analogie zu $\mathbb{Z} \subset \mathbb{Q}$ für jeden Integritätsring R einen Quotientenkörper $Q(R)$ konstruieren.

Mit Hilfsmitteln der Analysis (etwa Cauchy-Folgen oder Dedekindschen Schnitten) erhält man den Körper \mathbb{R} der reellen Zahlen als Oberkörper von \mathbb{Q} (siehe dazu etwa [Fi₄, 1.3.4]). Wir werden in Kapitel 3 sehen, dass es noch viele Körper K mit $\mathbb{Q} \subset K \subset \mathbb{R}$ gibt, man nennt sie **Zwischenkörper**.

Die wichtigste Körpererweiterung von \mathbb{R} sind die komplexen Zahlen $\mathbb{C} \supset \mathbb{R}$. Ihre geometrische Beschreibung als **Zahlenebene** \mathbb{R}^2 mit der „lateralen“ Einheit $\mathbf{i} = \sqrt{-1}$ wurde von GAUSS in [Ga₄, Nr. 30-32] ausgeführt, vgl. auch [W₂].

Der Vektorraum \mathbb{R}^2 hat über \mathbb{R} die Basis $(1, 0)$ und $(0, 1)$, wir setzen $1 := (1, 0)$ als „reelle Einheit“ und $\mathbf{i} := (0, 1)$ als „imaginäre Einheit“. Dann ist als Vektorraum

$$\mathbb{C} = \mathbb{R}^2 = \{a + b\mathbf{i} : a, b \in \mathbb{R}\}$$

bezüglich der Addition eine abelsche Gruppe. Die Multiplikation ist dadurch festgelegt, dass $\mathbf{i}^2 = -1$ sein soll, also

$$(a + b\mathbf{i})(c + d\mathbf{i}) := (ac - bd) + (ad + bc)\mathbf{i}.$$

Damit ist $1 = 1 + 0\mathbf{i}$ Einselement. Das Inverse erhält man aus der Rechnung

$$\frac{1}{a + b\mathbf{i}} = \frac{a - b\mathbf{i}}{(a + b\mathbf{i})(a - b\mathbf{i})} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\mathbf{i}.$$

Die Gültigkeit der Körperaxiome lässt sich durch elementare Rechnungen überprüfen. Diese lassen sich vereinfachen durch Benutzung des aus der linearen Algebra bekannten Rings $M(2 \times 2, \mathbb{R})$ der reellen 2×2 -Matrizen und der injektiven Abbildung

$$\varphi : \mathbb{C} \rightarrow M(2 \times 2, \mathbb{R}), \quad a + b\mathbf{i} \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Für $z = a + b\mathbf{i}$ und $z' = c + d\mathbf{i}$ gilt offensichtlich

$$\varphi(z + z') = \varphi(z) + \varphi(z') \quad \text{und} \quad \varphi(z \cdot z') = \varphi(z) \cdot \varphi(z').$$

Daraus folgt, dass $\varphi(\mathbb{C}) \subset M(2 \times 2, \mathbb{R})$ ein Unterring und somit \mathbb{C} ein Ring ist.

Diese Beziehung hat auch einen geometrischen Hintergrund. Der Körper \mathbb{C} operiert auf $\mathbb{R}^2 = \mathbb{C}$ durch Multiplikation, das wird durch die entsprechende Matrix beschrieben:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac - bd \\ bc + ad \end{pmatrix}.$$

Wie wir in Kapitel 3 sehen werden, gibt es zwischen \mathbb{R} und \mathbb{C} keinen echten Zwischenkörper. Dagegen gibt es zwischen \mathbb{Z} und \mathbb{C} viele interessante Zwischenringe, etwa den Ring

$$\mathbb{Z} + \mathbb{Z}\mathbf{i} := \{m + n\mathbf{i} : m, n \in \mathbb{Z}\} \subset \mathbb{C}$$

der **ganzen Gaußschen Zahlen** (mehr dazu in 2.4.2).

Zu $z = a + b\mathbf{i} \in \mathbb{C}$ heißt $\bar{z} := a - b\mathbf{i} \in \mathbb{C}$ die **komplex konjugierte** Zahl. Und weiter heißt

$$N(z) := z \cdot \bar{z} = a^2 + b^2 \in \mathbb{R}$$

die **Norm** von z . Es gelten die Rechenregeln

$$\overline{z + z'} = \bar{z} + \bar{z'}, \quad \overline{z \cdot z'} = \bar{z} \cdot \bar{z'}, \quad N(z \cdot z') = N(z) \cdot N(z'), \quad z^{-1} = \frac{\bar{z}}{N(z)}.$$

Aus der Norm erhält man den **Absolutbetrag**

$$|z| = \sqrt{z \cdot \bar{z}} = \sqrt{a^2 + b^2}.$$

Man kann die Multiplikation auch schön mit Polarkoordinaten in \mathbb{R}^2 beschreiben, das findet man z.B. in [Fi₁, 1.3.4].

Natürlich kann man \mathbb{R}^2 auch durch die Multiplikation

$$(a, b) \cdot (c, d) := (a \cdot c, b \cdot d)$$

zu einem kommutativen Ring mit Einselement $(1, 1)$ machen. Allerdings wimmelt es dann von Nullteilern, etwa

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

Beispiel 3 Es ist naheliegend eine zur Körpererweiterung $\mathbb{R} \subset \mathbb{R}^2 = \mathbb{C}$ analoge Konstruktion $\mathbb{R} \subset \mathbb{R}^n$ mit $n \geq 3$ zu versuchen. In 3.1.8 werden wir mit Hilfe des „Fundamentalsatzes der Algebra“ zeigen, dass dies unmöglich ist. Dass es für ungerades n nicht geht, kann man schon daraus folgern, dass ein reelles Polynom ungeraden Grades eine reelle Nullstelle hat. Es gilt (vgl. [Eb, Kap. 6]):

Ist $\mathbb{R} \subset \mathbb{R}^n = K$ eine Körpererweiterung mit ungeradem n , so ist $n = 1$.

Beweis $\mathbb{R}^n = K$ bedeutet, dass K sowohl ein Körper, als auch ein \mathbb{R} -Vektorraum der Dimension n ist. Für jedes $a \in K$ ist daher die Abbildung

$$F : \mathbb{R}^n \rightarrow \mathbb{R}^n, \quad x \mapsto a \cdot x,$$

ein Vektorraum-Endomorphismus, denn für $x, y \in \mathbb{R}^n$ und $\rho \in \mathbb{R}$ ist

$$a \cdot (x + y) = a \cdot x + a \cdot y \quad \text{und} \quad a \cdot (\rho \cdot x) = \rho \cdot (a \cdot x).$$

Da n ungerade ist, hat das charakteristische Polynom von F eine reelle Nullstelle λ , es gibt also einen Eigenvektor $0 \neq x \in \mathbb{R}^n$. Aus $ax = \lambda x$ folgt $(a - \lambda \cdot 1)x = 0$. Da K nullteilerfrei ist, muss $a = \lambda \cdot 1 \in \mathbb{R}$ sein. ■

In Beispiel 6 zeigen wir, wie \mathbb{R}^4 zum Schiefkörper der Quaternionen gemacht werden kann.

Für größeres n hat es nur noch Sinn im \mathbb{R}^n nach sogenannten **Divisionsalgebren** zu suchen. Man kann zeigen, dass dafür n eine Potenz von 2 sein muss, noch genauer: Es geht höchstens für $n = 1, 2, 4$ oder 8. Im \mathbb{R}^8 hat man die Struktur der **Oktaven** von CAYLEY, sie ist nicht mehr assoziativ. All das findet man sehr schön ausgeführt in [Eb, Kap. 7 und Kap. 10].

Beispiel 4 Ist M eine nicht leere Menge und R ein Ring, so kann man in der Menge $\text{Abb}(M, R)$ der Abbildungen $f : M \rightarrow R$ durch

$$(f + g)(x) := f(x) + g(x) \quad \text{und} \quad (f \cdot g)(x) := f(x) \cdot g(x)$$

für alle $x \in R$ eine Addition und eine Multiplikation erklären; wie man leicht sieht, wird $\text{Abb}(M, R)$ dadurch zu einem Ring.

Ist $M = \{1, \dots, n\}$, so ist

$$\text{Abb}(M, R) = R \times \dots \times R =: R^n$$

ein direktes Produkt; man nennt R^n den **Produkttring**.

Ist $M \subset \mathbb{R}^n$ offen und $R = \mathbb{R}$, so ist

$$\mathcal{C}(M, \mathbb{R}) := \{f \in \text{Abb}(M, \mathbb{R}) : f \text{ stetig}\} \subset \text{Abb}(M, \mathbb{R})$$

ein Unterring. Ein $f \in \mathcal{C}(M, \mathbb{R})$ ist genau dann Einheit, wenn $f(x) \neq 0$ für alle $x \in M$.

In $\mathcal{C}(M, \mathbb{R})$ gibt es viele Nullteiler. Ist etwa $M = \mathbb{R}$ und

$$f(x) = \begin{cases} 0 & \text{für } x \leq 0 \\ x & \text{für } x > 0 \end{cases}, \quad g(x) = \begin{cases} x & \text{für } x \leq 0 \\ 0 & \text{für } x > 0 \end{cases},$$

so ist $(f \cdot g)(x) = 0$ für alle $x \in \mathbb{R}$, also folgt $f \cdot g = 0$.

Ist $M \subset \mathbb{C}$ offen und zusammenhängend (in der komplexen Funktionentheorie sagt man dafür **Gebiet**), so ist

$$\mathcal{O}(M) := \{f \in \text{Abb}(M, \mathbb{C}) : f \text{ holomorph}\} \subset \text{Abb}(M, \mathbb{C})$$

ein Unterring, weil Summen und Produkte holomorpher Funktionen wieder holomorph sind. Wie bei den stetigen Funktionen ist $f \in \mathcal{O}(M)$ genau dann Einheit, wenn f in M keine Nullstelle hat. Im Gegensatz zu $\mathcal{C}(M, \mathbb{R})$ ist $\mathcal{O}(M)$ ein Integritätsring, denn ist $0 \neq f \in \mathcal{O}(M)$, so hat f höchstens isolierte Nullstellen (wie man in der Funktionentheorie mit Hilfe des Identitätssatzes beweist).

Beispiel 5 Sei G eine abelsche Gruppe, die Verknüpfung wird als Addition geschrieben. Mit

$$\text{End}(G) := \{ \varphi : G \rightarrow G : \varphi \text{ Homomorphismus} \}$$

bezeichnen wir die Menge der Endomorphismen von G . Eine Addition in $\text{End}(G)$ ist erklärt durch

$$(\varphi + \psi)(a) := \varphi(a) + \psi(a),$$

als Multiplikation dient die Hintereinanderschaltung $\varphi \circ \psi$. Bezüglich der Addition ist $\text{End}(G)$ eine abelsche Gruppe, die Hintereinanderschaltung ist assoziativ und

$$\begin{aligned} (\varphi \circ (\psi_1 + \psi_2))(a) &= \varphi(\psi_1(a) + \psi_2(a)) = (\varphi \circ \psi_1)(a) + (\varphi \circ \psi_2)(a) \\ &= (\varphi \circ \psi_1 + \varphi \circ \psi_2)(a). \end{aligned}$$

Analog zeigt man das andere Distributivgesetz, also ist $\text{End}(G)$ ein Ring; er heißt **Endomorphismenring** von G . Einselement ist die identische Abbildung, Einheiten sind die Automorphismen.

Ist V ein Vektorraum über einem Körper K , so hat man analog den **Endomorphismenring** $\text{End}(V)$. Als Beispiel betrachten wir den \mathbb{R} -Vektorraum $V = \mathbb{R}[X]$ der Polynome mit reellen Koeffizienten (vgl. 2.1.5). Er hat die abzählbare Basis $(1, X, X^2, \dots, X^k, \dots)$. Wir geben zwei wichtige Endomorphismen an:

Die Differentiation ergibt:

$$D : \mathbb{R}[X] \rightarrow \mathbb{R}[X], \quad a_n X^n + \dots + a_1 X + a_0 \mapsto n a_n X^{n-1} + \dots + a_1,$$

durch Integration erhält man

$$I : \mathbb{R}[X] \rightarrow \mathbb{R}[X], \quad b_m X^m + \dots + b_1 X + b_0 \mapsto \frac{b_m}{m+1} X^{m+1} + \dots + \frac{b_1}{2} X^2 + b_0 X.$$

Der Endomorphismus D ist nicht injektiv (den Kern bilden die konstanten Polynome) und I ist nicht surjektiv (die konstanten Polynome liegen nicht im Bild). Offensichtlich ist

$$D \circ I = \text{id}_{\mathbb{R}[X]}, \quad \text{aber} \quad I \circ D \neq \text{id}_{\mathbb{R}[X]},$$

also ist D Linksinverses von I und I Rechtsinverses von D , aber D und I sind keine Einheiten im Ring $\text{End}(\mathbb{R}[X])$!

In einem beliebigen Körper K kann man Probleme mit den ganzzahligen Faktoren bekommen (vgl. 3.1.1). Ein analoges Beispiel erhält man allgemein, indem man D und I auf der Basis $(1, X, \dots, X^k, \dots)$ von $K[X]$ durch

$$D(X^k) := X^{k-1}, \quad D(1) := 0 \quad \text{und} \quad I(X^k) := X^{k+1}$$

erklärt. In einem endlich-dimensionalen Vektorraum geht das nicht:

Ist $\dim_K V < \infty$ und sind $F, G \in \text{End}(V)$ gegeben mit $F \circ G = \text{id}_V$, so sind F, G Isomorphismen, also Einheiten im Endomorphismenring.

Das weiß man aus der linearen Algebra, denn aus $F \circ G = \text{id}_V$ folgt durch Betrachtung der Dimensionen, dass F surjektiv und G injektiv ist (vgl. etwa [Fi₁, 2.2.4]).

Beispiel 6 Im vorhergehenden Beispiel hatten wir den Endomorphismenring einer abelschen Gruppe betrachtet, ein Spezialfall sind Vektorräume V über einem Körper K . Ist $\dim_K V = n < \infty$, so wird nach Wahl einer Basis jeder Endomorphismus durch eine $n \times n$ -Matrix beschrieben, das ergibt nach den Regeln der linearen Algebra [Fi₁, 2.6.4] einen Ringisomorphismus

$$\text{End}_K(V) \xrightarrow{\cong} M(n \times n; K).$$

Der **Matrizenring** $M(n \times n; K)$ hat als Einselement die Einheitsmatrix E_n , für $n \geq 2$ ist er nicht kommutativ und hat Nullteiler. Man kennt die Einheiten:

$$(M(n \times n; K))^\times = GL(n; K) = \{A \in M(n \times n; K) : \det A \neq 0\}.$$

Der Matrizenring ist sehr nützlich, weil man viele Ringe als Unterringe realisieren kann, das nennt man **Matrixdarstellung** (in Analogie zur Permutationsdarstellung von Gruppen in 1.4.6). Wir wollen den Nutzen einer solchen Darstellung am Beispiel der Konstruktion der von HAMILTON im Jahre 1843 erfundenen **Quaternionen** \mathbb{H} als Erweiterung des Körpers der komplexen Zahlen vorführen (vgl. dazu auch [Eb, Kap. 7]).

Es ist naheliegend, die Konstruktion folgendermaßen zu beginnen: Die Addition in $\mathbb{H} = \mathbb{R}^4$ ist die Addition im Vektorraum. Zur Definition der Multiplikation betrachten wir zunächst die kanonische Basis

$$\mathbf{e} := e_1, \mathbf{i} := e_2, \mathbf{j} := e_3, \mathbf{k} := e_4.$$

Darauf wird die Multiplikation erklärt wie in der Quaternionengruppe (Beispiel 4 aus 1.1.9) durch die Tafel

\cdot	\mathbf{e}	\mathbf{i}	\mathbf{j}	\mathbf{k}
\mathbf{e}	\mathbf{e}	\mathbf{i}	\mathbf{j}	\mathbf{k}
\mathbf{i}	\mathbf{i}	$-\mathbf{e}$	\mathbf{k}	$-\mathbf{j}$
\mathbf{j}	\mathbf{j}	$-\mathbf{k}$	$-\mathbf{e}$	\mathbf{i}
\mathbf{k}	\mathbf{k}	\mathbf{j}	$-\mathbf{i}$	$-\mathbf{e}$

Das Produkt beliebiger Elemente aus \mathbb{H} erhält man daraus, indem man nach dem Distributivgesetz ausmultipliziert:

$$\begin{aligned} (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \cdot (a'\mathbf{e} + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = \\ (aa' - bb' - cc' - dd')\mathbf{e} + (ab' + ba' + cd' - dc')\mathbf{i} \\ + (ac' - bd' + ca' + db')\mathbf{j} + (ad' + bc' - cb' + da')\mathbf{k}. \end{aligned} \quad (*)$$

Aber nun beginnt der Ärger mit dem Nachweis der Axiome. Schon um das Inverse zu finden, muss man ein Gleichungssystem für die vier Unbekannten a', b', c', d' lösen. Der Leser möge das zur Übung in Angriff nehmen.

Wir kommen zurück auf den Trick von CAYLEY, der schon in Beispiel 4 aus 1.1.9 bei der Definition der Quaternionengruppe verwendet wurde, nämlich die Benutzung des Rings $M(2 \times 2; \mathbb{C})$. Dazu betrachten wir die Abbildung

$$\mathbb{C} \times \mathbb{C} \xrightarrow{\varphi} M(2 \times 2; \mathbb{C}), (z, w) \mapsto \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}.$$

Lehrbuch der Algebra

Mit lebendigen Beispielen, ausführlichen Erläuterungen
und zahlreichen Bildern

Fischer, G.

2017, XIII, 494 S. 156 Abb., 95 Abb. in Farbe.,

Hardcover

ISBN: 978-3-658-19365-2