30 Ringe und Körper

30.1 Motivation

- Häufig gibt es auf einer Menge zwei Verknüpfungen: eine „Addition“ und eine „Multiplikation“.
- Beispiele:
  - $(\mathbb{Z}, +, \cdot)$ – hier gibt es sogar noch eine Division mit Rest.
  - $(\mathbb{R}, +, \cdot)$ – hier gibt es auch eine Division.
- Lassen sich diese Konzepte algebraisch abstrahieren?

30.2 Definition: Ring

Eine Menge R mit zwei Verknüpfungen $+, \cdot$ auf R heißt **Ring**, wenn gilt:

a) $(R, +)$ ist eine kommutative Gruppe.

b) $(R, \cdot)$ ist eine Halbgruppe.

c) *Distributivgesetze:*

$$\left.\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}\right\} \quad \forall a, b, c \in R$$

Ist $(R, \cdot)$ sogar ein Monoid, so heißt $(R, +, \cdot)$ **Ring mit Einselement**.

Gilt neben (a)–(c) noch

d) *Kommutativgesetz der Multiplikation:*

$$a \cdot b = b \cdot a \qquad \forall a, b \in R\ ,$$

so heißt $(R, +, \cdot)$ **kommutativer Ring.**

30.3 Konventionen

In einem Ring $(R, +, \cdot)$ bezeichnet man häufig

- das neutrale Element der Addition als **Nullelement** (0),
- das neutrale Element der Multiplikation (sofern es existiert) als **Einselement** (1),
- das additive Inverse zu a mit $-a$,
- das multiplikative Inverse zu a (sofern es existiert) mit $\frac{1}{a}$.

Um Klammern zu sparen, vereinbart man „Punkt- vor Strichrechnung".

30.4 Beispiele

a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.

Außerdem kann man ganze Zahlen mittels der $\leq$-Beziehung *vergleichen*. Das ermöglicht die **Division mit Rest** (vgl. MfI 1, 6.2).

Zu jeder Zahl $a \in \mathbb{Z}$ und jeder Zahl $b \in \mathbb{Z}$, $b > 0$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

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

Man nennt q den **Quotienten** und r den **Rest** der Division von a durch b. Dabei heißt a **Dividend** und b **Divisor**.

Ist der Rest bei der Division von a durch b gleich 0, so ist a durch b **teilbar** (vgl. MfI 1, 6.3).

b) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind ebenfalls kommutative Ringe mit Eins. Wir betrachten sie später genauer.

c) Die Menge $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m (wobei $m \in \mathbb{N}$) bildet mit der modularen Addition (vgl. 29.19 und MfI 1, 7.8ff.)

$$[a] + [b] := [a + b]$$

sowie der Multiplikation („modulare Multiplikation", vgl. MfI 1, 7.12ff.)

$$[a] \cdot [b] := [a \cdot b] \qquad (*)$$

den **Restklassenring** $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$. Auch er ist kommutativ. Er besitzt das Einselement [1].

Zum Nachweis, dass die Multiplikation $(*)$ auf der Basis der Multiplikation ganzer Zahlen sinnvoll definiert ist, zeigen wir, dass das Ergebnis unabhängig davon ist, welche ganzen Zahlen aus den jeweiligen Kongruenzklassen gewählt werden: Für ganze Zahlen a, b sei $a' = a + q_1 m$ und $b' = b + q_2 m$ mit $q_1, q_2 \in \mathbb{Z}$, d. h. $a, a' \in [a] = a + m\mathbb{Z}$ (bzw. $[a'] = [a]$) und $b, b' \in [b] = b + m\mathbb{Z}$ (bzw. $[b'] = [b]$). Dann ist

$$\begin{aligned} a' \cdot b' &= (a + q_1 m) \cdot (b + q_2 m) \\ &= a \cdot b + (aq_2 + bq_1 + q_1 q_2 m)m \ , \end{aligned}$$

also $a \cdot b, a' \cdot b' \in [a \cdot b] = ab + m\mathbb{Z}$ (bzw. $[a' \cdot b'] = [a \cdot b]$). □

d) Weitere wichtige Beispiele folgen später: für kommutative Ringe (Polynomringe, Kap. 31) und für nichtkommutative Ringe (Matrizen, Kap. 35).

30.5 Satz: Unterringkriterium

Es sei $(R, +, \cdot)$ ein Ring und $S \subset R$. Dann ist $(S, +, \cdot)$ genau dann ein Ring, wenn

a) $(S, +)$ eine Untergruppe von $(R, +)$ ist (vgl. 29.7)

b) $(S, \cdot)$ abgeschlossen ist: $a \cdot b \in S \quad \forall a, b \in S$.

Beweis: analog zu Satz 29.7.

30.6 Beispiel

$(m\mathbb{Z}, +, \cdot)$ $(m \in \mathbb{N})$ ist Unterring von $(\mathbb{Z}, +, \cdot)$, denn

a) $(m\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Z}, +)$ (vgl. 29.8b)

b) $(m\mathbb{Z}, \cdot)$ ist abgeschlossen:
Für $a, b \in m\mathbb{Z}$ existieren $q_1, q_2 \in \mathbb{Z}$ mit $a = q_1 m, b = q_2 m$, also

$$ab = (q_1 m)(q_2 m) = (q_1 q_2 m)m \in m\mathbb{Z} \ .$$

30.7 Definition: Körper

Eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$ auf K heißt **Körper**, wenn gilt:

a) $(K, +, \cdot)$ ist ein kommutativer Ring mit einem Einselement, das ungleich dem Nullelement ist.

b) *Inverse Elemente:* Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein a^{-1} mit $a^{-1}a = 1$.

30.8 Bemerkungen

a) $(K, +, \cdot)$ besteht somit aus den kommutativen Gruppen $(K, +)$ und $(K \setminus \{0\}, \cdot)$, zwischen denen ein Distributivgesetz gilt.

b) Statt $K \setminus \{0\}$ schreibt man auch K^*.

c) Falls $(K^*, \cdot)$ nur eine *nichtkommutative* Gruppe ist, bezeichnet man $(K, +, \cdot)$ als **Schiefkörper**.

d) Englische Bezeichnung für einen Körper: *field*.

30.9 Beispiele

a) $(\mathbb{Z}, +, \cdot)$ ist *kein* Körper, da zu $a \in \mathbb{Z}^*$ im Allgemeinen kein a^{-1} existiert.

b) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

Weitere Beispiele folgen später.

30.10 Satz: Eigenschaften von Körpern

In einem Körper $(K, +, \cdot)$ gilt:

a) $a \cdot 0 = 0$ für alle $a \in K$

b) *Nullteilerfreiheit:* Sind $a, b \in K$ mit $a \neq 0$ und $b \neq 0$, so ist auch $a \cdot b \neq 0$. Das heißt: Aus $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.

Beweis:

a) Da 0 neutrales Element für + ist, gilt

$$\begin{aligned} a \cdot 0 + 0 &= a \cdot 0 \\ &= a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0 \quad \text{(Distributivität)} \end{aligned}$$

Addition von $-a \cdot 0$ auf beiden Seiten ergibt die Behauptung.

b) Es seien $a \neq 0$, $b \neq 0$. Angenommen, es gilt $a \cdot b = 0$. Dann folgt

$$b = (a^{-1}a)b = a^{-1} \underbrace{(ab)}_{0} = a^{-1} \cdot 0 \overset{\text{(a)}}{=} 0$$

im Widerspruch zu $b \neq 0$. □

Bemerkung: Satz 30.10a impliziert, dass man in Körpern nicht durch 0 dividieren darf: $q := \frac{a}{b}$ bedeutet $a = q \cdot b$. Gilt hierin $b = 0$, so folgt $a = 0$. Für $a = 0$ ist jedoch $a = q \cdot b$ für jedes $q \in K$ erfüllt. Also ist auch der Ausdruck $\frac{0}{0}$ sinnlos.

30.11 Der Körper der komplexen Zahlen

Hier wird nur das Nötigste angegeben – ausführlich werden komplexe Zahlen in MfI 1, Kap. 9 behandelt.

Definition: Es sei $\mathbb{C} := \{(a, b) \mid a, b \in \mathbb{R}\}$, und wir führen auf $\mathbb{C}$ folgende Operationen ein:

a) *Addition:*

$$(a, b) + (c, d) := (a + c, b + d) \quad \forall a, b, c, d \in \mathbb{R}$$

b) *Multiplikation:*

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc) \quad \forall a, b, c, d \in \mathbb{R}\ .$$

Dann ist $(\mathbb{C}, +, \cdot)$ ein Körper mit dem Nullelement $(0, 0)$ und dem Einselement $(1, 0)$.

Eigenschaften:

a) **Einbettung von $\mathbb{R}$:** Die Teilmenge $\{(a,0) \mid a \in \mathbb{R}\}$ ist bezüglich Addition und Multiplikation abgeschlossen und isomorph dem Körper $(\mathbb{R}, +, \cdot)$. Man identifiziert daher $(a,0)$ mit der reellen Zahl a.

b) **Imaginäre Einheit:** $\mathrm{i} := (0,1)$. Es gilt $\mathrm{i}^2 = -1$.

c) Damit lassen sich komplexe Zahlen darstellen als

$$(a,b) = a + \mathrm{i}b \quad \forall a, b \in \mathbb{R} \; .$$

d) Es sei $z := a + \mathrm{i}b$. Dann heißt a **Realteil**, b **Imaginärteil** von z. Man schreibt

$$a = \operatorname{Re} z \; , \qquad\qquad b = \operatorname{Im} z \; .$$

$\bar{z} := a - \mathrm{i}b$ heißt **konjugiertes Element** zu z.

e) $|z| := \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$ heißt **Betrag** der komplexen Zahl $z = a + \mathrm{i}b$.

f) *Division* mithilfe des komplex Konjugierten:

$$\begin{aligned} \frac{a + \mathrm{i}b}{c + \mathrm{i}d} &= \frac{a + \mathrm{i}b}{c + \mathrm{i}d} \cdot \frac{c - \mathrm{i}d}{c - \mathrm{i}d} \\ &= \frac{(ac + bd) + \mathrm{i}(bc - ad)}{c^2 + d^2} \\ &= \frac{ac + bd}{c^2 + d^2} + \mathrm{i}\frac{bc - ad}{c^2 + d^2} \; . \end{aligned}$$

30.12 Endliche Körper

a) Der Restklassenring $(\mathbb{Z}_m, +, \cdot)$ (vgl. 30.4c) ist ein Körper dann und nur dann, wenn er nullteilerfrei ist. Man kann zeigen, dass dies genau dann der Fall ist, wenn m eine Primzahl ist (vgl. MfI 1, 7.17).

b) Allgemein heißt ein endlicher Körper mit q Elementen **Galoisfeld** (nach Evariste Galois, 1811–1832).

Man kann zeigen: Für $q \in \mathbb{N}$ gibt es ein Galoisfeld genau dann, wenn $q = p^m$ mit einer Primzahl p und einer natürlichen Zahl m. Für jedes solche q ist das zugehörige Galoisfeld bis auf Isomorphie eindeutig bestimmt und wird mit $\mathrm{GF}(q)$ bezeichnet.

Es gilt also für Primzahlen p:

$$\mathrm{GF}(p) = \mathbb{Z}_p \; .$$