

# 01. Gruppen, Ringe, Körper

Gruppen, Ringe bzw. Körper sind wichtige abstrakte algebraische Strukturen. Sie entstehen dadurch, dass auf einer Menge  $M$  eine oder mehrere sogenannte "Verknüpfungen" definiert werden, i.e. zwei Elementen der Menge wird ein weiteres Element zugeordnet. Diese Verknüpfungen können streng genommen als Abbildungen  $M \times M \rightarrow M$  geschrieben werden, obwohl in der Praxis zumeist eine andere Schreibweise gewählt wird.

**Definition.** Eine **Gruppe** ist ein Paar  $(G, \circ)$ , bestehend aus einer nichtleeren Menge  $G$  und einer Verknüpfung " $\circ$ " auf  $G$ , d.h. einer Abbildung

$$\circ : G \times G \rightarrow G, (a, b) \mapsto a \circ b$$

sodass folgende Eigenschaften erfüllt sind.

$$(G1) \quad \forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c) \quad (\text{Assoziativgesetz})$$

$$(G2) \quad \exists e \in G \quad (\text{neutrales Element von } G) \quad \text{mit } e \circ a = a \quad \forall a \in G$$

$$(G3) \quad \forall a \in G \quad \exists a' \in G \quad (\text{inverses Element zu } a) \quad \text{mit } a' \circ a = e$$

**Definition.** Eine Gruppe  $(G, \circ)$  heißt **abelsch** (oder **kommutativ**) wenn

$$\forall a, b \in G : a \circ b = b \circ a \quad (\text{Kommutativgesetz})$$

**Bemerkung.** Falls über die vorliegende Verknüpfung Klarheit herrscht, schreibt man für eine Gruppe oft abgekürzt nur  $G$ . Statt  $a \circ b$  schreibt man oft auch  $a \cdot b$  oder  $ab$ , bzw. im Falle einer abelschen Gruppe auch  $a + b$ .

**Bemerkung.** Sei  $(G, \circ)$  eine Gruppe. Dann gilt

- 1) Für ein neutrales Element  $e \in G$  gilt  $a \circ e = a \quad \forall a \in G$ .
- 2) Es gibt **genau ein** neutrales Element  $e \in G$ .

3) Ist  $a'$  inverses Element zu  $a \in G$ , dann gilt  $a \circ a' = e$ .

4) Zu  $a \in G \exists$  **genau ein** inverses Element. Dieses wird bei der Schreibweise  $(G, \circ)$  bzw.  $(G, \cdot)$  mit  $a^{-1}$ , bei der Schreibweise  $(G, +)$  mit  $-a$  bezeichnet.

### **Beweis.**

ad 3) : Zu  $a'$  existiert wegen (G3) ein Element  $a''$  mit  $a'' \circ a' = e$ .  
Damit erhalten wir mit (G1) und (G2)

$$\begin{aligned} a \circ a' &= e \circ (a \circ a') = (a'' \circ a') \circ (a \circ a') = a'' \circ (a' \circ (a \circ a')) = \\ &= a'' \circ ((a' \circ a) \circ a') = a'' \circ (e \circ a') = a'' \circ a' = e \end{aligned}$$

$$\text{ad 1) } a \circ e = a \circ (a' \circ a) = (a \circ a') \circ a = e \circ a = a$$

ad 2) Sei  $e'$  ein weiteres neutrales Element. Dann ist  $e \circ e' = e'$  weil  $e$  neutral ist, und ebenso  $e \circ e' = e$  weil  $e'$  neutral ist. Also  $e = e'$ .

ad 4) Seien  $a', a''$  inverse Elemente zu  $a \in G$ . Dann ist unter Verwendung des bereits Bewiesenen

$$a'' = a'' \circ e = a'' \circ (a \circ a') = (a'' \circ a) \circ a' = e \circ a' = a'. \quad \square$$

**Bemerkung.** (Beweis zur Übung)

$$\forall a, b \in G : (a^{-1})^{-1} = a \quad \text{und} \quad (a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

**Beispiel.** Die Menge  $\mathbb{Z}$  der ganzen Zahlen bildet bezüglich der üblichen Addition die abelsche Gruppe  $(\mathbb{Z}, +)$ .

Neutrales Element ist  $0$ , inverses Element zu  $m \in \mathbb{Z}$  ist  $-m$ .

Analog erhalten wir die abelschen Gruppen  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$  und  $(\mathbb{C}, +)$ .

**Beispiel.** Die Menge  $\mathbb{N}$  der natürlichen Zahlen ist bezüglich der Addition **keine** Gruppe, weil kein neutrales Element und kein inverses Element existiert.

**Beispiel.**  $\mathbb{Q} \setminus \{0\}$  ist bezüglich der üblichen Multiplikation eine abelsche Gruppe. Neutrales Element ist  $1$ , inverses Element zu  $q \in \mathbb{Q} \setminus \{0\}$  ist  $\frac{1}{q}$ .

Analog erhalten wir die bezüglich der Multiplikation abelschen Gruppen  $(\mathbb{R} \setminus \{0\}, \cdot)$  und  $(\mathbb{C} \setminus \{0\}, \cdot)$ , sowie  $(\mathbb{Q}_+, \cdot)$  und  $(\mathbb{R}_+, \cdot)$ .

**Beispiel.**  $(\mathbb{Z} \setminus \{0\}, \cdot)$  ist **keine** Gruppe, da es zwar ein neutrales Element gibt, aber nicht immer ein inverses Element.

**Beispiel.** Sei  $M \neq \emptyset$  eine Menge und  $S(M) = \{f : M \rightarrow M : f \text{ ist bijektiv}\}$ . Dann ist  $S(M)$  bezüglich der Verknüpfung von Abbildungen "o" eine Gruppe.

Neutrales Element ist die identische Abbildung  $\text{id}_M : M \rightarrow M$ ,  $x \mapsto \text{id}_M(x) = x$ . Das inverse Element zu  $f \in S(M)$  ist die inverse Abbildung  $f^{-1}$ .  $S(M)$  ist im allgemeinen nicht abelsch, und heißt die **symmetrische Gruppe** der Menge  $M$ .

Ist speziell  $M = \{1, 2, \dots, n\}$ , dann schreibt man kurz  $S_n$  für  $S(M)$ . Ein Element  $\sigma \in S_n$  heißt **Permutation** der Zahlen  $1, 2, \dots, n$ .

**Definition.** Ein **Ring** ist ein Tripel  $(R, +, \cdot)$  bestehend aus einer nichtleeren Menge  $R$  und zwei Verknüpfungen " + " und "  $\cdot$  " so dass folgende Eigenschaften erfüllt sind.

(R1)  $(R, +)$  ist abelsche Gruppe mit neutralem Element  $0$

(R2)  $\forall \alpha, \beta, \gamma \in R$  gilt  $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma) \quad , \quad (\beta + \gamma) \cdot \alpha = (\beta \cdot \alpha) + (\gamma \cdot \alpha)$$

**Bemerkung.**  $(R, +, \cdot)$  ist ein **kommutativer Ring** wenn

$$\alpha \cdot \beta = \beta \cdot \alpha \quad \forall \alpha, \beta \in R$$

$(R, +, \cdot)$  ist ein **Ring mit Einselement** wenn

$$\exists 1 \in R \text{ sodass } 1 \cdot \alpha = \alpha \quad \forall \alpha \in R$$

**Beispiel.**  $(\mathbb{Z}, +, \cdot)$  mit der üblichen Addition und Multiplikation ganzer Zahlen ist ein kommutativer Ring mit Einselement.

**Beispiel.** Sei  $M \neq \emptyset$  eine Menge und sei  $F(M, \mathbb{R})$  die Menge aller Abbildungen  $M \rightarrow \mathbb{R}$ .

Zu  $f, g : M \rightarrow \mathbb{R}$  seien die Abbildungen  $f + g$ ,  $f \cdot g$  wie folgt erklärt

$$(f + g)(x) = f(x) + g(x) \quad \forall x \in M$$

$$(f \cdot g)(x) = f(x) \cdot g(x) \quad \forall x \in M$$

(Dabei sind auf den rechten Seiten jeweils die übliche Addition und Multiplikation reeller Zahlen zu verstehen)

Dann ist  $F(M, \mathbb{R})$  ein kommutativer Ring mit Einselement.

Neutrales Element bzgl. der Addition ist die **Nullabbildung**  $0 : M \rightarrow \mathbb{R}$  mit  $0(x) = 0 \in \mathbb{R} \quad \forall x \in M$ .

Einselement bzgl. der Multiplikation ist die Abbildung  $1 : M \rightarrow \mathbb{R}$  mit  $1(x) = 1 \in \mathbb{R} \quad \forall x \in M$ .

**Definition.** Ein **Körper** ist ein Tripel  $(K, +, \cdot)$  bestehend aus einer nichtleeren Menge  $K$  und zwei Verknüpfungen „+“ und „ $\cdot$ “ sodass folgende Eigenschaften erfüllt sind.

(K1)  $(K, +)$  ist abelsche Gruppe mit neutralem Element  $0$ , das zu  $a \in K$  inverse Element wird mit  $-a$  bezeichnet

(K2)  $(K \setminus \{0\}, \cdot)$  ist abelsche Gruppe mit neutralem Element  $1$ , das zu  $a \in K \setminus \{0\}$  inverse Element wird mit  $a^{-1}$  oder mit  $\frac{1}{a}$  bezeichnet

(K3)  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ ,  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

**Bemerkung.** Oft schreibt man nur  $K$ , wenn klar ist, welche Verknüpfungen gemeint sind. Statt  $a \cdot b$  schreibt man oft auch  $ab$  und verwendet die Konvention, dass die Multiplikation stärker bindet als die Addition, also etwa  $a \cdot (b + c) = a \cdot b + a \cdot c$ .

Statt  $a + (-b)$  schreibt man  $a - b$ , statt  $ab^{-1}$  auch  $\frac{a}{b}$ .

**Beispiel.**  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  und  $(\mathbb{C}, +, \cdot)$  sind bzgl. der üblichen Addition und Multiplikation von Zahlen Körper.

**Beispiel.**  $(\mathbb{Z}, +, \cdot)$  ist **kein** Körper.

**Beispiel.** Auf der zweielementigen Menge  $K = \{0, 1\}$  kann eine Körperstruktur wie folgt definiert werden.

$$0 + 0 = 1 + 1 = 0 \quad , \quad 1 + 0 = 0 + 1 = 1$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \quad , \quad 1 \cdot 1 = 1$$