

5 Algebraische Strukturen

In der Mathematik werden Mengen und auf ihnen definierte Operationen und Relationen betrachtet, z. B. $(\mathbb{N}; +, *, \leq)$, $(\mathbb{R}; +, *, \leq)$, (Menge der logischen Ausdrücke; $\neg, \wedge, \vee, =$).

Definition $\circ$ ist **binäre** (zweistellige) **Operation** in der Menge M : $\Leftrightarrow \circ : M \times M \rightarrow M$.

Bezeichnung: Statt $\circ (x, y)$ schreibt man auch $x \circ y$.

Eigenschaften von Operationen

- $\circ$ ist **kommutativ**: $\Leftrightarrow$ für alle $x, y \in M$ gilt: $x \circ y = y \circ x$.
- $\circ$ ist **assoziativ**: $\Leftrightarrow$ für alle $x, y, z \in M$ gilt: $(x \circ y) \circ z = x \circ (y \circ z)$.
- e ist **neutrales Element** in M : $\Leftrightarrow$ für alle $x \in M$ gilt: $x \circ e = e \circ x = x$.
- x^{-1} ist **inverses Element** zu x : $\Leftrightarrow x \circ x^{-1} = x^{-1} \circ x = e$.
- $\circ$ ist **distributiv** bezüglich $\circ'$: $\Leftrightarrow$ für alle $x, y, z \in M$ gilt: $x \circ (y \circ' z) = (x \circ y) \circ' (x \circ z)$.

Definition Σ ist **algebraische Struktur**: $\Leftrightarrow \Sigma = (M; x_1, \dots, x_k; R_1, \dots, R_m; \circ_1, \dots, \circ_n)$, wobei $M \neq \emptyset$ Trägermenge der Struktur, $x_1, \dots, x_k$ ausgezeichnete Elemente von M , $R_1, \dots, R_m$ Relationen in M und $\circ_1, \dots, \circ_n$ Operationen in M sind.

Beispiele: $\Sigma_1 = (\mathbb{N}; 0, 1; \leq, =; +, *)$, $\Sigma_2 = (\mathbb{R}; 0, 1; \leq, =; +, *)$.

Spezielle Strukturen

$(M; \circ)$ ist **Halbgruppe**: $\Leftrightarrow \circ$ ist assoziativ.

$(M; e; \circ)$ ist **Monoid**: $\Leftrightarrow (M; \circ)$ ist Halbgruppe mit neutralem Element e .

$(M; e; \circ)$ ist **Gruppe**: $\Leftrightarrow (M; e; \circ)$ ist Monoid, in dem es zu jedem $x \in M$ ein inverses Element gibt.

$(M; e; \circ)$ ist **abelsche Gruppe**: $\Leftrightarrow (M; e; \circ)$ ist Gruppe, in der das Kommutativgesetz gilt.

Aufgabe:

Man untersuche folgende Strukturen auf ihre Eigenschaften: $(\mathbb{N}; 0; +)$, $(\mathbb{Z}; 0; +)$, $(\mathbb{N}; 1; *)$, $(\{1, -1\}; 1; *)$, $(\mathbb{Q}; 0; +)$, $(\mathbb{Q} \setminus \{0\}; 1; *)$, $(\mathbb{R}; 1; *)$.

Beispiele:

1. Menge aller Restklassen mod 3 und Addition:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Aus dieser Strukturtafel erkennt man, dass $+$ eine Operation in $M = \{[0], [1], [2]\}$ ist, die kommutativ ist und als neutrales Element $[0]$ hat. Jedes Element hat ein Inverses: $[0]$ ist zu sich selbst invers, $[1]$ und $[2]$ sind zueinander invers. Darüber hinaus ist $+$ auch assoziativ. Mithin ist $(M; [0]; +)$ eine abelsche Gruppe (**Restklassengruppe $\mathbb{R}_3$**).

2. Menge aller Restklassen mod 3 und Multiplikation:

*	[1]	[2]
[1]	[1]	[2]
[2]	[2]	[1]

$(M \setminus \{[0]\}; [1]; *)$ ist abelsche Gruppe.

3. Menge der Restklassen mod 4 und Multiplikation:

*	[1]	[2]	[3]
[1]	[1]	[2]	[3]
[2]	[2]	[0]	[2]
[3]	[3]	[2]	[1]

$(\{[1], [2], [3]\}; [1]; *)$ ist keine Gruppe, denn [2] besitzt kein inverses Element.

Bemerkung: Ist der Modul m eine Primzahl, so sind die Restklassen bezüglich der Multiplikation immer Gruppen.

4. Menge der Permutationen S_M und Hintereinanderausführung:

Definition f ist **Permutation** der Menge M : $\Leftrightarrow f$ ist Bijektion von M auf sich.

Sei $M = \{1, 2, 3\}$. Dann ist $S_M = \{f_1, f_2, \dots, f_6\}$ mit $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$,

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ und } f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Daraus ergibt sich für die Hintereinanderausführung folgende Strukturtafel:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Zum Beispiel: $f_4 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_6.$

An der Strukturtafel kann man erkennen, dass $f_1 = \text{id}$ neutrales Element ist, dass zu jeder Permutation eine inverse existiert und dass die Operation nicht kommutativ ist. Das Assoziativgesetz ist erfüllt, weil es bei der Hintereinanderausführung von Abbildungen generell gilt. $(S_M; \text{id}, \circ)$ ist eine Gruppe.

Satz In Gruppen ist die Gleichung $x \circ a = b$ eindeutig lösbar.

Beweis:

Existenz: $x = b \circ a^{-1}$ ist eine Lösung, denn $x \circ a = (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$. (Beim Beweis wurden nacheinander das Assoziativgesetz, die Eigenschaften des inversen und des neutralen Elementes angewendet.)

Eindeutigkeit: Sei $x \circ a = b$. Dann folgt $x = x \circ e = x \circ (a \circ a^{-1}) = (x \circ a) \circ a^{-1} = b \circ a^{-1}$.

Satz In Gruppen gilt $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$

Beweis: $(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1} = (x \circ e) \circ x^{-1} = x \circ x^{-1} = e$.

(Beim Beweis wird maßgeblich der vorangegangene Satz benutzt.)

Strukturen mit zwei Operationen

$(M; e; \circ_1, \circ_2)$ ist **Ring**: $\Leftrightarrow (M; e; \circ_1)$ ist abelsche Gruppe, $(M; \circ_2)$ ist Halbgruppe und $\circ_2$ ist distributiv bezüglich $\circ_1$.

$(M; e_1, e_2; \circ_1, \circ_2)$ ist **Körper**: $\Leftrightarrow (M; e_1; \circ_1)$ und $(M \setminus \{e_1\}; e_2; \circ_2)$ sind abelsche Gruppen, $\circ_2$ ist distributiv bezüglich $\circ_1$.

$(M; \circ_1, \circ_2)$ ist **Verband**: $\Leftrightarrow \circ_1$ und $\circ_2$ sind kommutativ und assoziativ, und für alle $a, b \in M$ gelten die Verschmelzungsregeln $a \circ_1 (a \circ_2 b) = a$ und $a \circ_2 (a \circ_1 b) = a$.

Beispiele:

$(\mathbb{Z}; 0; +, *)$ ist ein Ring; $(\mathbb{R}; 0, 1; +, *)$ und (Menge aller Restklassen mod Primzahl p ; $+, *$) sind Körper, $(\mathbb{N}; 0; +, *)$ ist kein Ring, $(\mathcal{P}(M); \cup, \cap)$ und (Menge aller logischen Ausdrücke; $\wedge, \vee$) sind Verbände.

Zusammenfassung

