Gruppe

Unter einer Gruppe $(G, \diamond)$ versteht man eine Menge G, auf der eine binäre Operation $\diamond$ definiert ist:

$$\diamond : G \times G \longmapsto G \,,$$

d.h. jedem Elementepaar $(a, b) : \; a, b \in G$ ist ein Element $a \diamond b \in G$ zugeordnet. Ferner müssen folgende Eigenschaften gelten:

- Assoziativität: $(a \diamond b) \diamond c = a \diamond (b \diamond c) \quad \forall a, b, c \in G$
- Neutrales Element: Es existiert ein eindeutig bestimmtes neutrales Element $e \in G$, d.h.

$$e \diamond a = a \diamond e = a \quad \forall a \in G$$

- Inverses Element: Zu jedem Element $a \in G$ existiert ein eindeutig bestimmtes inverses Element $a^{-1} \in G$ mit

$$a \diamond a^{-1} = a^{-1} \diamond a = e$$

Man nennt eine Gruppe eine kommutative oder abelsche Gruppe, wenn die Operation $\diamond$ kommutativ ist:

$$a \diamond b = b \diamond a \qquad \forall a, b \in G$$

Wenn aus dem Zusammenhang ersichtlich ist, welche Operation verwendet wird, schreibt man häufig statt $(G, \diamond)$ nur G.

Beispiel

Die bijektiven reellen Funktionen $f : \mathbb{R} \to \mathbb{R}$ bilden bezüglich der Hintereinanderschaltung $\circ$ eine Gruppe.

Verifizierung der Gruppenaxiome

- Assoziativität:

$$((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$$

- Neutrales Element: Identität

$$e : x \mapsto x$$

- Inverses Element: Umkehrfunktion

$$f^{-1} : f(x) \mapsto x$$

Gegenbeispiel zur Kommutativität: $f \circ g \neq g \circ f$ für

$$f : x \mapsto 2x, \quad g : x \mapsto x + 1$$

$f(g(x)) = 2(x + 1) \neq 2x + 1 = g(f(x))$

Beispiel

Abelsche Gruppe

$$\mathbb{Z}_n = \mathbb{Z} \bmod n$$

der Restklassen $\{0, 1, \ldots, n-1\}$ mit der Addition modulo n als Gruppenoperation

Illustration der Gruppenaxiome für $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

- Assoziativität

$$\begin{aligned} (1 + 2 \bmod 4) + 3 \bmod 4 &= 3 + 3 \bmod 4 = 6 \bmod 4 = 2 \\ 1 + (2 + 3 \bmod 4) \bmod 4 &= 1 + (5 \bmod 4) \bmod 4 = 1 + 1 \bmod 4 = 2 \quad \checkmark \end{aligned}$$

- Neutrales Element 0

$$3 + 0 \bmod 4 = 0 + 3 \bmod 4 = 3$$

- Inverses Element

$$0 = 1 + 3 \bmod 4 = 2 + 2 \bmod 4 = 3 + 1 \bmod 4$$

Die Multiplikation modulo 4 definiert keine Gruppenstruktur, denn beispielsweise gilt

$$\begin{aligned} 2 &= 2 \cdot 1 \text{ mod } 4 = 2 \bmod 4 \\ &= 2 \cdot 3 \text{ mod } 4 = 6 \bmod 4 \end{aligned}$$

$\Longrightarrow$ keine Eindeutigkeit des neutralen Elements $(1 \neq 3)$

Gruppentafel

Die Operation $\diamond$ auf einer endlichen Gruppe $G = \{g_1, \ldots, g_n\}$ kann durch die Verknüpfungsmatrix A definiert werden:

$$A: \quad a_{j,k} = g_j \diamond g_k$$

Für eine abelsche (kommutative) Gruppe ist A symmetrisch:

$$g_j \diamond g_k = g_k \diamond g_j \quad \Longleftrightarrow \quad A = A^{\mathrm{t}}\,.$$

Die erste nicht-abelsche Gruppe hat 6 Elemente und kann mit den Permutationen von $\{1, 2, 3\}$ identifiziert werden.

Beispiel

Gruppentafeln für Gruppen mit ≤ 4 Elementen

$\diamond$	e	a
e	e	a
a	a	e

$\diamond$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\diamond$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\diamond$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a