# Algebraische Strukturen

**Motivation:** Bereits sehr einfache algebraische Strukturen, insbesondere Gruppen, liefern ein sehr interessantes Betätigungsfeld in der Mathematik. Sie sind grundlegend für andere Bereiche, z. B. Vektorrechnung und haben auch Anwendung in der Kryptographie etc.

## I Gruppen

**Definition:** Eine Menge $G$ zusammen mit einer Verknüpfung $\circ$ nennt man Gruppe $:\Leftrightarrow$

A1: $\exists\, e \in G$ mit $e \circ x = x \quad \forall\, x \in G$

A2: $\forall\, x \in G \quad \exists\, x^{-1} \in G$ so dass $x^{-1} \circ x = e$

A3: $\forall\, x, y, z \in G$ gilt: $(x \circ y) \circ z = x \circ (y \circ z)$

**Bemerkung:** A1 nennt man "Existenz eines Neutralen"

A2 " " "Existenz von Inversen"

A3 " " Assoziativitätsgesetz

**Satz 1:** Sei $(G,\circ)$ ein Gruppe. Dann gilt

a) $x \circ e = x \quad \forall x \in G$

b) $x \circ x^{-1} = e \quad \forall x \in G$

**Beweis:** b) Sei $(x^{-1})^{-1}$ das Inverse von $x^{-1}$.

$x^{-1}$ ist wieder das Inverse von $x$

d.h. $(x^{-1})^{-1} \circ x^{-1} = e$ und $x^{-1} \circ x = e$

($x$ ist hier ein beliebiges Element aus $g$).

$$x \circ x^{-1} \overset{A1}{=} (e \circ x) \circ x^{-1} \overset{A2}{=} \left(\left[(x^{-1})^{-1} \circ x^{-1}\right] \circ x\right) \circ x^{-1} =$$

$$\overset{A3}{=} \left((x^{-1})^{-1} \circ \left[x^{-1} \circ x\right]\right) \circ x^{-1} \overset{A2}{=} \left((x^{-1})^{-1} \circ e\right) \circ x^{-1} =$$

$$\overset{A3}{=} (x^{-1})^{-1} \circ \left(e \circ x^{-1}\right) \overset{A1}{=} (x^{-1})^{-1} \circ x^{-1} \overset{A2}{=} e$$

a) $x \circ e \overset{A2}{=} x \circ (x^{-1} \circ x) \overset{A3}{=} (x \circ x^{-1}) \circ x \overset{b)}{=} e \circ x \overset{A1}{=} x$

(Rechnung gilt $\forall x \in G$)

Alle drei Gruppenaxiome gehen in den Beweis ein. Lässt man eines fallen, gelten die Aussagen i. A. nicht mehr.

**Satz 2:** "Das neutrale Element sowie die Inversen sind eindeutig", präziser:

a) Sei $(G,\circ)$ Gruppe mit neutralem Element $e$.
Falls $\tilde{1} \circ x = x \quad \forall x \in G$ so ist $\tilde{1} = e$.

b) Falls $\bar{x} \circ x = e$ so ist $\bar{x} = x^{-1}$

**Beweis:** a) $e = 1 \circ e = 1$ (Annahme, Satz 1 a)) □

b) $\bar{x} = \bar{x} \circ e = \bar{x} \circ (x \circ x^{-1}) \overset{A3}{=} (\bar{x} \circ x) \circ x^{-1} =$ (Satz 1a), Satz 1b), ←)

$= e \circ x^{-1} \overset{A1}{=} x^{-1}$ (Annahme) □

**Notation:** a) Wenn klar ist, welche Verknüpfung gemeint ist, müssen wir sie nicht nennen. Man sagt dann auch "G ist Gruppe" statt "(G,∘) ist Gruppe"

b) Wir schreiben $ab$ statt $a \circ b$.

c) Klammern lassen wir ganz weg. Wegen A3 ist das o.k.