Algebra 1

Gruppen — Definition und Beispiele

- Rechnen mit Resten: modulare Addition und Multiplikation.
- Definition

  Es bezeichne $\mathbb{Z}_n$ die Menge der ersten n nichtnegativen ganzen Zahlen,

  $$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

  Für die Addition modulo n verwenden wir das Symbol $\oplus$ und für die Multiplikation modulo n entsprechend $\odot$.

  Schließlich wird für die Menge $\mathbb{Z}_n$ zusammen mit der modularen Addition die Schreibweise $(\mathbb{Z}_n, \oplus)$ verwendet, entsprechend bei modularer Multiplikation $(\mathbb{Z}_n, \odot)$, oder aber $(\mathbb{Z}_n \setminus \{0\}, \odot)$, falls wir die 0 weglassen wollen.
- Beispiele: Tabellen von $(\mathbb{Z}_n, \oplus)$ und $(\mathbb{Z}_n, \odot)$ sowie von $(\mathbb{Z}_n \setminus \{0\}, \odot)$ für einige Werte von n.
- Anmerkung: Man erkennt, daß bestimmte Eigenschaften — wie zum Beispiel die Abgeschlossenheit bezüglich der Verknüpfung — bei $(\mathbb{Z}_n, \oplus)$ für alle untersuchten n vorhanden sind, bei $(\mathbb{Z}_n \setminus \{0\}, \odot)$ hingegen nur für bestimmte n. Offenbar gelten diese Eigenschaften auch für die unendliche Menge aller ganzer Zahlen $\mathbb{Z}$, wenn die Addition als Operator verwendet wird.

  Unterschiedliche Mengen mit verschiedenen Operatoren zur Verknüpfung der Elemente können also gemeinsame Eigenschaften bezüglich des Verhaltens der Operatoren haben. Wir fassen einige besonders charakteristische Eigenschaften zusammen; liegen sie vor, sprechen wir von einer „Gruppe“.
- Definition

  Es sei $G \neq \emptyset$ eine Menge, und es sei $*$ ein binärer Operator auf G, d.h. ein Operator, der zwei Elemente a, b aus G miteinander verknüpft, wobei das Ergebnis als $a * b$ geschrieben wird.

  Es gelte

(V) Verknüpfungsabgeschlossenheit:

$$a * b \in G \qquad \text{für alle } a,\, b \in G;$$

(A) Assoziativität:

$$(a * b) * c = a * (b * c) \qquad \text{für alle } a,\, b,\, c \in G;$$

(N) es existiere ein sogenanntes *neutrales Element* $e \in G$, so daß:

$$a * e = a \qquad \text{und} \qquad e * a = a \qquad \text{für alle } a \in G;$$

(I) zu jedem $a \in G$ existiere ein sogenanntes *inverses Element* $b \in G$ mit:

$$a * b = e \qquad \text{und} \qquad b * a = e.$$

Dann heißt $(G, *)$ eine ***Gruppe***. Gilt zusätzlich

(K) Kommutativität:

$$a * b = b * a \qquad \text{für alle } a,\, b \in G,$$

so heißt $(G, *)$ eine ***kommutative*** oder ***abelsche Gruppe***[1].

- Anmerkung: Die Mächtigkeit $|G|$ der Menge G, also die Anzahl der Elemente von G, heißt die ***Ordnung*** der Gruppe.
- Beispiele (Gruppen/keine Gruppen).
- Anmerkung: Man verwendet die folgenden Kurzschreibweisen.

	additiv	multiplikativ
$a * b$	$a + b$	ab
neutrales Element e	0	1
inverses Element zu a	$-a$	a^{-1}
$a * \beta$, wobei β invers zu b	$a - b$	ab^{-1}
$a * a$	$2a$	a^2
$\alpha * \alpha$, wobei α invers zu a	$2(-a) = -2a$	$(a^{-1})^2 = a^{-2}$

[1] Schwer zu behalten? Keine Panik, denk' an VANIK.

- Anmerkung: Die Schreibweise 0 bzw. 1 für e ist nur möglich, wenn es nicht mehrere neutrale Elemente gibt. Die Schreibweise $(-a)$ bzw. a^{-1} ist nur möglich, wenn es zu a nicht mehrere inverse Elemente gibt.

  Hierzu der folgende Satz.

- Satz

  (a) In einer Gruppe gibt es genau ein neutrales Element.

  (b) Zu jedem Element einer Gruppe ist das inverse Element eindeutig bestimmt.

- Beweis

- Satz

  Es sei G eine Gruppe. (Wir verwenden im folgenden die multiplikative Schreibweise.)

  (a) Für beliebige a, $b \in G$ sind die Gleichungen $ax = b$ und $ya = b$ in G eindeutig lösbar.

  (b) Es gilt $(a^{-1})^{-1} = a$.

  (c) Für beliebige Elemente $a_1, \ldots, a_n \in G$ gilt

  $$(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}.$$

- Beweis