Algebraische Strukturen

Verknüpfungen

Motivation

Rechenregeln in $\mathbb{N}_0$

Für alle $x, y, z \in \mathbb{N}_0$ gilt:

- $x + (y + z) = (x + y) + z$
- $0 + x = x$
- $x + y = y + x$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $1 \cdot x = x$
- $x \cdot y = y \cdot x$

Die Operationen $+$ und $\cdot$ sind Beispiele für *Verknüpfungnen*.

Verknüpfungen (Forts.)

Definition

M Menge

Verknüpfung auf M: Abbildung $\bullet \colon M \times M \to M$

Notation:

- für $x, y \in M$: $\quad x \bullet y := \bullet(x, y)$

Verknüpfungen (Forts.)

Beispiele

- auf $\mathbb{N}_0$:
- auf $\mathbb{Z}$:
- auf $\mathbb{Q}$:

Verknüpfungen (Forts.)

Definition

M Menge, $\bullet$ Verknüpfung auf M

- $\bullet$ *assoziativ*: für alle $x, y, z \in M$:

$$x \bullet (y \bullet z) = (x \bullet y) \bullet z$$

- $\bullet$ *kommutativ*: für alle $x, y \in M$:

$$x \bullet y = y \bullet x$$

Verknüpfungen (Forts.)

Definition

M Menge, $\bullet$ Verknüpfung auf M

neutrales Element bzgl. $\bullet$: $e \in M$ so, dass für $x \in M$:

$$e \bullet x = x \bullet e = x$$

Bemerkung

M Menge, $\bullet$ Verknüpfung auf M

es gibt höchstens ein neutrales Element bzgl. $\bullet$

Verknüpfungen (Forts.)

Definition

M Menge, $\bullet$ Verknüpfung auf M, e neutrales Element bzgl. $\bullet$
$x \in M$

- *linksinverses Element* zu x bzgl. $\bullet$: $y \in M$ mit
$$y \bullet x = e$$
- *rechtsinverses Element* zu x bzgl. $\bullet$: $y \in M$ mit
$$x \bullet y = e$$
- *inverses Element* zu x bzgl. $\bullet$: $y \in M$ mit
$$y \bullet x = e = x \bullet y$$

Verknüpfungen (Forts.)

Bemerkung

M Menge

$\bullet$ assoziative Verknüpfung auf M, e neutrales Element bzgl. $\bullet$
$x \in M$

es gibt höchstens ein inverses Element zu x bzgl. $\bullet$

Monoide

Definition

- *Monoid*: besteht aus
  - M Menge
  - $\bullet$ assoziative Verknüpfung auf M
  - e, neutrales Element bezgl. $\bullet$

  Missbrauch von Notation: notiere Monoid wieder als M

  Terminologie und Notationen:
  - *Multiplikation* von M: $\bullet$
    Notation:
- M Monoid

  M heißt *abelsch* (oder *kommutativ*): $\cdot$ ist kommutativ

Monoide (Forts.)

Axiome in Standardnotation

- Monoid M:
  - für $x, y, z \in M$: $x(yz) = (xy)z$
  - es ex. $e \in M$ so, dass für $x \in M$: $ex = e = xe$

- Abelsches Monoid M:

  Zusätzlich:
  - für $x, y \in M$: $xy = yx$

Wir sagen auch: M ist *multiplikativ geschrieben*.

Bei multiplikativer Schreibweise benutzt man oft das Zeichen 1 für das neutrale Element e. Für $x \in M$ und $n \in \mathbb{N}$ schreibt man auch $x^n := x \cdot x \cdot \cdots \cdot x$ (n Faktoren).

Monoide (Forts.)

Bei einem abelschen Monoid M benutzt man oft das Zeichen $+$ für die Verknüpfung.

Wir sagen auch: M ist *additiv geschrieben*.

In diesem Fall schreibt man meistens 0 für das neutrale Element. Für $x \in M$ und $n \in \mathbb{N}$ schreibt man auch $nx := x + x + \cdots + x$ (n Summanden).

Axiome in Standardnotation

- für $x, y, z \in M$: $\quad x + (y + z) = (x + y) + z$
- es ex. $0 \in M$ so, dass für $x \in M$: $\quad 0 + x = x = x + 0$
- für $x, y \in M$: $\quad x + y = y + x$

Monoide (Forts.)

Beispiele

- - $\mathbb{N}$ mit üblicher Addition:
  - $\mathbb{N}$ mit üblicher Multiplikation:
- - $\mathbb{N}_0$ mit üblicher Addition:
  - $\mathbb{N}_0$ mit üblicher Multiplikation:

Monoide (Forts.)

Beispiel

nicht-kommutatives Monoid mit genau drei Elementen:

$\cdot$	1	c_1	c_2
1	1	c_1	c_2
c_1	c_1	c_1	c_1
c_2	c_2	c_2	c_2

Wortmonoid

Definition
A Menge

- Für $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ nennen wir

$$a_1 a_2 \cdots a_n$$

  ein *Wort der Länge n über A*.
- $A^* := \{w \mid w \text{ ist Wort der Länge } n \text{ über } A, n \in \mathbb{N}_0\}$.
  A^* enthält das Wort ϵ der Länge 0.
- Für zwei Wörter $v := a_1 \cdots a_n$ und $w := b_1 \cdots b_m$ über A sei

$$v * w := a_1 \cdots a_n b_1 \cdots b_m$$

  die *Verkettung* oder *Konkatenation* von v und w.
- $(A^*, *)$ ist ein Monoid mit neutralem Element ϵ, das *Wortmonoid* über A.

Abbildungsmonoid

Bemerkung

M Menge

$\mathrm{Abb}(M, M)$ ist Monoid mit Verknüpfung $(g, f) \mapsto g \circ f$

und neutralem Element id_M.

Bemerkung

Sei M Menge und $f \in \mathrm{Abb}(M, M)$.

- f besitzt Rechtsinverses $\Leftrightarrow$ f ist surjektiv.
- f besitzt Linksinverses $\Leftrightarrow$ f ist injektiv.
- f besitzt Inverses $\Leftrightarrow$ f ist bijektiv.

Invertierbare Elemente

Definition

- M Monoid, $x \in M$
  - x *invertierbar* in M: es gibt ein inverses Element zu x bzgl. $\cdot$
  - x invertierbar

    Inverse zu x in M: das zu x inverse Element y bzgl. $\cdot$
    Notation:
  - *Menge der invertierbaren Elemente* in M:

$$M^{\times} = \{x \in M \mid x \text{ invertierbar}\}$$

Invertierbare Elemente (Forts.)

Beispiel

- ${\mathbb{N}_0}^\times = \{1\}$
- 0 einziges invertierbare Element in $\mathbb{N}_0$
- A Menge: $(A^*)^\times = \{\epsilon\}$

Proposition

M Monoid

- für $x, y \in M^\times$: $\quad xy \in M^\times$ mit $(xy)^{-1} = y^{-1}x^{-1}$
- $\quad 1 \in M^\times$ mit $1^{-1} = 1$
- für $x \in M^\times$: $\quad x^{-1} \in M^\times$ mit $(x^{-1})^{-1} = x$

Gruppen

Definition

- *Gruppe*:
  Monoid, in dem jedes Eleement invertierbar ist.
- *Abelsche Gruppe*:
  abelsches Monoid, in dem jedes Element invertierbar ist.

Gruppen (Forts.)

Beispiel

- - $\mathbb{Z}$ mit üblicher Addition:
  - $\mathbb{Z}$ mit üblicher Multiplikation:
- - $\mathbb{Q}$ mit üblicher Addition:
  - $\mathbb{Q}$ mit üblicher Multiplikation:
  -

Gruppen (Forts.)

Definition

A abelsche Gruppe

Subtraktion von A: Verknüpfung $(x, y) \mapsto x + (-y)$ auf A
Notation: $-$

Gruppe der invertierbaren Elemente

Definition
M Monoid

Einheitengruppe von M
(oder *Gruppe der invertierbaren Elemente*):
Gruppe $M^\times$ mit Multiplikation gegeben durch diejenige von M.

Beispiel

- $\mathbb{Z}^\times = \{1, -1\}$
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
- A Menge:
  $S_A := \mathrm{Abb}(A, A)^\times$, die *symmetrische Gruppe auf* A.
  $S_A = \{f \in \mathrm{Abb}(A, A) \mid f \text{ ist invertierbar}\}$.

Untergruppen

Definition

G Gruppe, $U \subseteq G$.

U heißt *Untergruppe* von G, falls gilt:

- $e \in U$.
- Für alle $x, y \in G$ ist auch $x \cdot y^{-1} \in G$.

Untergruppen (Forts.)

Beispiele

- Für $n \in \mathbb{Z}$ ist
$$n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$$
eine Untergruppe von $(\mathbb{Z}, +)$.

  Z.B. ist
  - $2\mathbb{Z}$ die Menge der gerande Zahlen.
  - $0\mathbb{Z} = \{0\}$.
  - $1\mathbb{Z} = \mathbb{Z}$.
- Sei A eine Menge und $a \in A$. Dann ist
$$S_{A,a} := \{f \in S_A \mid f(a) = a\}$$
eine Untergruppe von S_A.
- $(\mathbb{N}, +)$ ist keine Untergruppe von $(\mathbb{Z}, +)$.

Ringe und Körper

Definition

Ring: Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass gilt:

- $(R, +)$ abelsche Gruppe
- $(R, \cdot)$ Monoid
- für alle $x, y, z \in R$ gilt:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$$

Die letzten beiden Axiome heißen die *Distributivgesetze*.

Ringe und Körper (Forts.)

- R Ring

  R *kommutativ*: $\cdot$ kommutativ

- *Körper*: kommutativer Ring K mit
  - $1 \neq 0$
  - jedes Element von $K \setminus \{0\}$ ist invertierbar

Ringe und Körper (Forts.)

Beispiele

- $\mathbb{Z}$ mit üblicher Addition und Multiplikation:
- $\mathbb{Q}$ mit üblicher Addition und Multiplikation:

Ringe und Körper (Forts.)

Beispiel

Körper mit genau zwei Elementen:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$