



more: bigdev.de/teaching

Algebraische Strukturen

Algebraische Strukturen - Intro

Ziel: Abstraktion der Rechenstrukturen $+$, \cdot hin zu allgemeinen Rechenregeln.

Bsp. a) $(\mathbb{N}; +)$: $(a+b)+c = a+(b+c)$ (assoziativ)

$$a+b = b+a \quad (\text{kommutativ})$$

b) $(\mathbb{Z}; \cdot)$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (assoziativ)

$$a \cdot b = b \cdot a \quad (\text{kommutativ})$$

c) $(\mathbb{N}; -)$: $1-2 = -1 \notin \mathbb{N}$ (\mathbb{N} nicht abgeschlossen bzgl. $-$)
 $2-(3-2) \neq (2-3)-2$ (nicht assoziativ)

d) $(\mathbb{Z}; -)$

Funktion



Def. Eine Menge M zusammen mit einer Operation

$\circ: M \times M \rightarrow M$, $\circ(m, n) =: m \circ n$ heißt **algebraische**

Struktur.

Bsp. a) $(\mathbb{Z}, +)$

b) (\mathbb{Q}, \cdot)

c) $(\mathbb{N}, -)$

Algebraische Strukturen - Gruppen

Def. Eine algebraische Struktur (G, \circ) heißt **Gruppe**

\Leftrightarrow (Ab) G ist bzgl. \circ abgeschlossen:

$$\forall a, b : G. \exists c : G. a \circ b = c$$

(Ass) Assoziativität:

$$\forall a, b, c : G. a \circ (b \circ c) = (a \circ b) \circ c$$

(Neu) Neutrales Element:

$$\exists n : G. \forall a : G. a \circ n = a = n \circ a$$

(Inv) Inverses Element:

$$\forall a : G. \exists \bar{a} : G. a \circ \bar{a} = n = \bar{a} \circ a$$

Wenn das Kommutativgesetz gilt, dann nennt man das eine „kommutative Gruppe“ oder eine „abelsche Gruppe“.

(Kom) $\forall a, b : G. a \circ b = b \circ a$



Ist $(\mathbb{N}, +)$ oder $(\mathbb{Z}, +)$ eine Gruppe?

$(\mathbb{N}, +)$ Nein

$(\mathbb{Z}, +)$ Ja

Algebraische Strukturen - Halbgruppen

Def. Eine algebraische Struktur (S, \circ) heißt **Halbgruppe**
: \Leftrightarrow (Ab) und (Ass) sind erfüllt.

Ü

Was sind (Halb-) Gruppen?

- | | | | Begründung |
|--|--|--|----------------|
| a) $(\mathbb{N}_0, +)$ | <input checked="" type="checkbox"/> Halbgruppe | <input type="checkbox"/> Gruppe | lVR gilt nicht |
| b) (\mathbb{N}_0, \cdot) | <input checked="" type="checkbox"/> Halbgruppe | <input type="checkbox"/> Gruppe | lVR - -- |
| c) $(\mathbb{Z}, +)$ | <input type="checkbox"/> Halbgruppe | <input checked="" type="checkbox"/> Gruppe | alle gelten |
| d) (\mathbb{Z}, \cdot) | <input checked="" type="checkbox"/> Halbgruppe | <input type="checkbox"/> Gruppe | lVR gilt nicht |
| e) $(\mathbb{Z}, :)$ | <input type="checkbox"/> Halbgruppe | <input type="checkbox"/> Gruppe | |
| f) (\mathbb{Q}, \cdot) | <input checked="" type="checkbox"/> Halbgruppe | <input type="checkbox"/> Gruppe | |
| g) $(\mathbb{Q}, :)$ | <input type="checkbox"/> Halbgruppe | <input type="checkbox"/> Gruppe | |
| h) $(\mathbb{Q} \setminus \{0\}, \cdot)$ | <input type="checkbox"/> Halbgruppe | <input checked="" type="checkbox"/> Gruppe | |

Algebraische Strukturen – Restklassen

Ü

Bilden Sie die Verknüpfungstafel für $(\mathbb{Z}_4, +)$.

\oplus	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ab ✓
 Ass ✓ \Rightarrow Gruppe
 Neu ✓
 Inv ✓

Satz. $(\mathbb{Z}_m, +)$ ist eine abelsche Gruppe.

Beweis.

(Ab) $\overline{a} \oplus \overline{b} = \overline{a+b} \text{ mod } m \quad \checkmark$

(Ass) $\overline{a} \oplus (\overline{b} \oplus \overline{c}) = \overline{a} \oplus \overline{b+c} = \overline{a+(b+c)} = \overline{(a+b)+c} = \overline{(a+b)} \oplus \overline{c} \quad \checkmark$

(Neu) $\overline{a} \oplus 0 = \overline{a+0} = \overline{a} = \overline{0+a} = 0 \oplus \overline{a} \quad \checkmark$

(Inv) Es ist \overline{a} ist $\overline{m-a}$ invers: $\overline{a} \oplus \overline{m-a} = \overline{a+(m-a)} = \overline{m} = \overline{0} \quad \checkmark$

(Kom) $\overline{a} \oplus \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} \oplus \overline{a} \quad \checkmark$

\Rightarrow Gruppe (abelsich)

Jetzt untersuchen wir (\mathbb{Z}_m, \cdot) also mit der Multiplikation

ü

Bilden Sie die Verknüpfungstafeln von

a) (\mathbb{Z}_4, \cdot)

b) (\mathbb{Z}_5, \cdot)

und entscheiden Sie, ob es sich um (Halb-) Gruppen handelt.

a)

-	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(Ab)

✓

(Ass)

✓

(Neu)

✓

(Inv)

✗

→ Halbgruppe

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(Ab)

✓

(Ass)

✓

(Neu)

✓

→ Halbgruppe

Satz. (\mathbb{Z}_m, \cdot) ist eine kommutative Halbgruppe.

↖ i.A. keine Gruppe



Algebraische Strukturen - Ringe

Wir betrachten jetzt zwei Operationen auf einer Menge:

Def. Eine Struktur $(R, +, \cdot)$ heißt **Ring**: \Leftrightarrow

- (1) $(R, +)$ ist eine kommutative Gruppe
- (2) (R, \cdot) ist Abgruppe

(Dis) Distributivität:

$$\forall a, b, c \in R: a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

$$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

ü

Zeigen Sie, dass $(\mathbb{Z}_m, +, \cdot)$ ein Ring ist.

Algebraische Strukturen - Inverse in Restklassen

- Wdh: $(\mathbb{Z}_m, +)$ kommutative Gruppe
 (\mathbb{Z}_m, \cdot) kommutative Gruppe mit Einselement
 $(\mathbb{Z}_m, +, \cdot)$ kommutativer Ring mit Einselement

Was fehlt?

Sei $a \in \mathbb{Z}_m \setminus \{0\}$:

$$a \cdot x \equiv 1 \pmod{m}$$

$$\Leftrightarrow m \mid (a \cdot x - 1)$$

$$\Leftrightarrow \exists q \in \mathbb{Z}, m \cdot q = a \cdot x - 1$$

Diophantische
Gleichung! 

$$ax - mq = 1$$

$$ax + m(-q) = 1$$

$$ax + my = 1$$

d.h.

Satz. $a \in \mathbb{Z}_m$ invertierbar $\Leftrightarrow \text{ggT}(a, m) = 1$

Ü

Welche Elemente sind invertierbar?

a) in \mathbb{Z}_8 : 1; 3; 5; 7

b) in \mathbb{Z}_5 : alle

Satz. $(\mathbb{Z}_m \setminus \{0\}, \cdot)$ Gruppe $\Leftrightarrow m = \text{Prim}$

Wie berechnet man a^{-1} ?

Löse
$$ax + my = 1$$
 ← Diophantische Gleichung. Dann ist $a^{-1} = x$.

ü

Ist 5 in \mathbb{Z}_{123} invertierbar? Bestimmen Sie ggf. das Inverse zu 5.

Algebraische Strukturen - Körper

Def. Eine algebraische Struktur $(K, +, \cdot)$ mit mindestens 2 Elementen heißt **Körper** \Leftrightarrow

(1) $(K, +)$ ist kommutative Gruppe

(2) $(K \setminus \{0\}, \cdot)$ ist kommutative Gruppe

(3) (0) is

Satz. $(\mathbb{Z}_m, +, \cdot)$ Körper $\Leftrightarrow m = \text{Prim}$

ii

Ist $(\mathbb{Z}_{3881}, +, \cdot)$ ein Körper?

wenn $3881 = \text{Prim}$, dann ja (cont nein)