

WS 2015/16

# Diskrete Strukturen

## Kapitel 5: Algebraische Strukturen (Grundlagen)

Hans-Joachim Bungartz

Lehrstuhl für wissenschaftliches Rechnen  
Fakultät für Informatik  
Technische Universität München

[http://www5.in.tum.de/wiki/index.php/Diskrete\\_Strukturen\\_-\\_Winter\\_15](http://www5.in.tum.de/wiki/index.php/Diskrete_Strukturen_-_Winter_15)

- Algebraische Strukturen
  - **Grundlagen**
  - Gruppen
  - Endliche Körper



- Die **Algebra** als Teilgebiet der Mathematik befasst sich mit **algebraischen Strukturen**, d.h. mit Mengen und darauf definierten Operationen, von denen nur bekannt ist, dass sie gewisse Eigenschaften (wie z.B. Assoziativität, Kommutativität, Distributivität, Idempotenz, ...) besitzen.
- Welche Eigenschaften jede Operation hat, wird durch **Axiome** festgelegt.



- Algebra (als Struktur):

**Definition:** Eine Algebra besteht aus einer **Trägermenge**  $S$  und einer Menge  $\Phi$  von **Operatoren** (oder **Operationen**) auf  $S$  (der Operatorenmenge).

Ein Operator der **Stelligkeit (arity)**  $m \in \mathbb{N}$  ist eine Abbildung  $S^m \rightarrow S$ .



- Beispiele:
  - $\langle \mathbb{N}, + \rangle$ ,  $\langle \mathbb{Z}, + \rangle$ ,  $\langle \mathbb{N}, +, * \rangle$  sind Algebren.
  - Sei  $Q = \{x \in \mathbb{N} \mid x \text{ ist Quadratzahl}\}$ .  
 $\langle Q, * \rangle$  ist eine Algebra.  
 $\langle Q, + \rangle$  ist keine Algebra.
  - $\langle \{\mathbf{true}, \mathbf{false}\}, \wedge, \vee, \neg \rangle$  ist eine Algebra.
  - Sei  $U$  eine Menge.  $\langle 2^U, \cup, \cap \rangle$  ist eine Algebra.
  - Sei  $F(U)$  die Menge aller Abbildungen  $U \rightarrow U$ .  $\langle F(U), \circ \rangle$  ist eine Algebra (die Operation  $\circ$  bezeichnet die Komposition von Abbildungen).



- Multiplikationstafeln:

Algebren mit zweistelligen Operatoren lassen sich über ihre **Multiplikationstafeln** (Operationstafeln) darstellen.

Beispiel:  $\langle \{\mathbf{true}, \mathbf{false}\}, \wedge, \vee \rangle$

$\vee$	T	F
T	T	T
F	T	F

$\wedge$	T	F
T	T	F
F	F	F



- Neutrales und inverses Element:

**Definition:** Sei  $\langle S, \circ \rangle$  eine Algebra. Ein Element  $e \in S$  heißt **linksneutrales (bzw. rechtsneutrales) Element** für den Operator  $\circ$ , falls

$$\forall a \in S: e \circ a = a \text{ (bzw. } \forall a \in S: a \circ e = a \text{)}.$$

Ein **neutrales Element** ist ein Element, welches sowohl links- als auch rechtsneutral ist.



- Neutrales und inverses Element:

**Definition:** Sei  $\langle S, \circ \rangle$  eine Algebra mit einem neutralen Element  $e$  und sei  $a \in S$ .

Ein Element  $x \in S$  ist ein **rechtsinverses** (bzw. **linksinverses**) **Element** von  $a$ , falls  $a \circ x = e$  (bzw.  $x \circ a = e$ ).

Ist  $x$  sowohl rechts- als auch linksinverses Element zu  $a$ , so heißt es **inverses Element** zu  $a$ .





- Neutrales und inverses Element:

## Beispiele:

- Die Algebra  $\langle \{a, b\}, \circ \rangle$  mit

$\circ$	$a$	$b$
$a$	$a$	$a$
$b$	$b$	$b$

hat **rechtsneutrale Elemente**  $a$  und  $b$ ,  
jedoch **keine** linksneutralen Elemente.



- Neutrales und inverses Element:
  - Die neutralen Elemente der Addition bzw. Multiplikation auf den natürlichen/ganzen Zahlen sind 0 bzw. 1.
  - In  $\langle \mathbb{Z}, + \rangle$  hat jedes Element  $x$  ein inverses Element:  $-x$ .
  - In  $\langle \mathbb{R} \setminus \{0\}, * \rangle$  hat jedes Element  $x$  ein inverses Element:  $1/x$ .
  - In  $\langle \mathbb{Z} \setminus \{0\}, * \rangle$  haben nur die Elemente 1 und  $-1$  ein inverses Element.



- Halbgruppen, Monoide, Gruppen:

**Definition:** Eine Algebra  $A = \langle S, \circ \rangle$  mit einem zweistelligen Operator  $\circ$  heißt **Halbgruppe**, falls  $\circ$  **assoziativ ist**, also gilt:

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

**Beispiele:**

- $\langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{N}, * \rangle, \langle \mathbb{Z}, * \rangle, \langle 2^U, \cup \rangle, \langle F(U), \circ \rangle$  sind Halbgruppen.
- $\langle \{\mathbf{true}, \mathbf{false}\}, \rightarrow \rangle$  ist keine Halbgruppe.

**Gegenbeispiel?**



- Halbgruppen, Monoide, Gruppen:  
 Welche der beiden folgenden, durch ihre Multiplikationstabellen beschriebenen Algebren mit  $S = \{a_1, a_2\}$  sind Halbgruppen?

$\circ$	$a_1$	$a_2$
$a_1$	$a_1$	$a_1$
$a_2$	$a_2$	$a_2$

$\circ$	$a_1$	$a_2$
$a_1$	$a_2$	$a_2$
$a_2$	$a_1$	$a_1$



- Halbgruppen, Monoide, Gruppen:

**Definition:** Eine Algebra  $A = \langle S, \circ \rangle$  mit einem zweistelligen Operator  $\circ$  heißt **Monoid**, falls  $\circ$  **assoziativ ist und es ein neutrales Element gibt.**

**Beispiele:**

- $\langle \mathbb{N}_0, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{N}, * \rangle, \langle 2^U, \cup \rangle, \langle 2^U, \cap \rangle, \langle F(U), \circ \rangle$  sind Monoide. **Was sind die neutralen Elemente?**
- $\langle \mathbb{N}, + \rangle$  ist Halbgruppe aber kein Monoid.
- $\langle \mathbb{Z} \setminus \{0\}, + \rangle$  ist keine Algebra. **Warum?**



- Halbgruppen, Monoide, Gruppen:

**Definition:** Eine Algebra  $A = \langle S, \circ \rangle$  mit einem zweistelligen Operator  $\circ$  heißt **Gruppe**, falls  $\circ$  assoziativ ist, es ein neutrales Element gibt und jedes Element ein inverses Element besitzt.

**Beispiele:**

- $\langle \mathbb{N}_0, + \rangle$  ist Monoid, aber keine Gruppe.
- $\langle \mathbb{Z}, + \rangle$ ,  $\langle \mathbb{Q} \setminus \{0\}, * \rangle$  und  $\langle \mathbb{R} \setminus \{0\}, * \rangle$  sind Gruppen.
- $\langle B(U), \circ \rangle$  ist Gruppe.



- Einschub – **Modulare Arithmetik:**

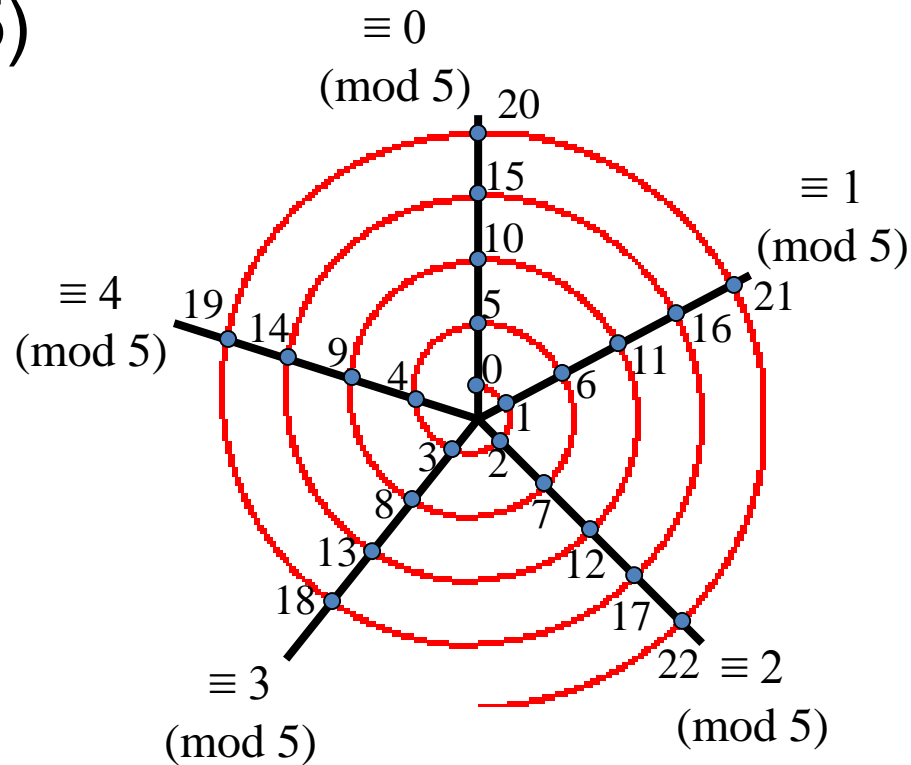
**Definition:** Sei  $m \in \mathbb{N}$ . Zwei Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  gdw.

- die Differenz  $(x - y)$  durch  $m$  teilbar ist,
- es  $k \in \mathbb{Z}$  gibt mit  $x = y + k m$ ,
- sie bei Division durch  $m$  den gleichen Rest haben.

Die Kongruenz modulo  $m$  ist eine Äquivalenzrelation auf  $\mathbb{Z}$ . Sie wird  $x \equiv_m y$  oder  $x \equiv y \bmod m$  geschrieben.



- Einschub **Modulare Arithmetik:**
  - Spiralvisualisierung der Äquivalenzklassen (mod 5)





- Einschub **Modulare Arithmetik:**

**Definition:** Seien  $x, y, m \in \mathbb{N}$ .

$(x \bmod y)$  bezeichnet den Rest der Division  $x : y$ .

$x +_m y$  ist eine Abkürzung für  $(x + y) \bmod m$ .

$x *_m y$  ist eine Abkürzung für  $(x * y) \bmod m$ .



- Zurück zu Gruppen:

**Beispiele:** Sei  $\mathbb{Z}_n = \{0, \dots, n - 1\}$ ,  $n \geq 2$ .

- $\langle \mathbb{Z}_n, +_n \rangle$  ist eine Gruppe:
  - 0 ist neutrales Element.
  - $(n - a)$  ist inverses Element von  $a$  für alle  $a \neq 0$ .
- $\langle \mathbb{Z}_5 \setminus \{0\}, *_5 \rangle$  ist eine Gruppe:
  - 1 ist neutrales Element;
  - 1 ist inverses Element von 1; 3 von 2; 2 von 3; 4 von 4.
- $\langle \mathbb{Z}_4 \setminus \{0\}, *_4 \rangle$  ist keine Gruppe:
  - 2 hat kein inverses Element.



- Abelsche Gruppen:

**Definition:** Eine Gruppe (ein Monoid, eine Halbgruppe) heißt **abelsch oder kommutativ**, falls  $\circ$  kommutativ ist, also gilt:

$$\forall a, b \in S: a \circ b = b \circ a.$$

**Beispiele:**

- $\langle \mathbb{Z}, + \rangle$ ,  $\langle \mathbb{R} \setminus \{0\}, * \rangle$  und  $\langle \mathbb{Z}_n, +_n \rangle$  sind abelsch.
- $\langle B(U), \circ \rangle$  ist nicht abelsch.

**Gegenbeispiel?**



## Praktische Anwendungen in der Informatik:

- Endliche Gruppen in der Computeralgebra
- Modulo-Rechnen in der Algorithmik (z.B. Index-Arithmetik)

