

Formelsammlung

MAA

Jan Caspar, Aktualisiert 21. April 2017

Algebraische Struktur

Man nennt $[(T_1, \dots, T_m), f_1, \dots, f_n]$ eine algebraische Struktur (mit den Trägemengen T_1, \dots, T_m und Operationen f_1, \dots, f_n).

Beispiele

Sehr oft haben wir es mit Strukturen mit einer Trägermenge und einer oder mehreren binären Operationen zu tun. z.B. $[Z, +][N, \cdot][R, +, \cdot][Pot(M), \cup, \cap]$

Relationale Struktur

Man nennt $[(T_1, \dots, T_m), r_1, \dots, r_n]$ eine relationale Struktur (mit den Trägemengen T_1, \dots, T_m und Relationen r_1, \dots, r_n).

Beispiele

e: $[N, \leq], [N_0, []]$, Graph $[G, E]$.

Halbgruppe

Eine binäre Operation \circ heißt assoziativ auf T , falls für alle $x, y, z \in T$ gilt:

$$(x \circ y) \circ z = x \circ (y \circ z).$$

Ist \circ assoziativ auf T , so nennt man $[T, \circ]$ eine **Halbgruppe**.

Beispiele

$[N, +][R, \cdot][Pot(M), \cup]$

Monoid

Ein Element $a \in T$ heißt invertierbar bzgl. \circ , falls es ein $b \in T$ gibt mit

$$a \circ b = b \circ a = \varepsilon.$$

Man nennt b dann das zu a **inverse Element** bzgl. \circ

Falls jedes $a \in T$ bzgl. \circ invertierbar ist, so nennt man ein Monoid $[T, \circ]$ auch **Gruppe**.

Beispiele

$[Z, +][R \setminus \{0\}, \cdot][f : Abij. \rightarrow A, \circ]$

Gruppe

$\varepsilon \in T$ heißt neutrales Element bzgl. \circ , falls für alle $x \in T$ gilt:

$$\varepsilon \circ x = x \circ \varepsilon = x$$

Besitzt T ein neutrales Element bzgl. \circ , so nennt man eine Halbgruppe $[T, \circ]$ auch **Monoid**.

Beispiele

$[N_0, +][R \setminus \{0\}, \cdot][Pot(M), \cup][f : A \rightarrow A, \circ]$

kommutative Strukturen (abelsch)

Eine binäre Operation \circ heißt kommutativ auf T , falls für alle $x, y \in T$ gilt:

$$x \circ y = y \circ x.$$

Ist die Operation \circ kommutativ, spricht man auch von

- einer **kommutativen** Halbgruppe,
- einem **kommutativen** Monoid,
- einer **kommutativen** Gruppe.

Statt kommutativ sagt man auch **abelsch**, z.B. abelsche Gruppe

Permutationen

Sei $M \neq \emptyset$ eine Menge. f ist Permutation von M genau dann wenn:

$$f : M \rightarrow M \text{ ist bijektiv}$$

Seien f und g Permutationen von M , dann ist $f \circ g : M \rightarrow M, x \mapsto f(g(x))$ eine **Permutation**.

Hintereinanderausführung

- $f \circ g$ heißt **Hintereinanderausführung** (f nach g)
- ist assoziativ.
- Bzgl. \circ gibt es ein neutrales Element, die identische Funktion $\varepsilon : M \rightarrow M, x \mapsto x$
- Zu jeder Permutation f existiert die inverse Permutation f^{-1}
mit: $\forall_{x \in M} (f \circ f^{-1})(x) = f(f^{-1}(x)) = x$ und $\forall_{x \in M} (f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$
d.h. $f \circ f^{-1} = f^{-1} \circ f = \varepsilon$

Symmetrische Gruppe

Die Permutationen einer Menge M bilden mit der Hintereinanderausführung \circ eine Gruppe, genannt, die **symmetrische** Gruppe von M , in Zeichen S_M .

- Wir schreiben $S_n := S_{1,2,\dots,n}$ für $n \in N$. Das sind die Permutationen der ersten n natürlichen Zahlen.
- Die S_n hat $n!$ Elemente.

Null und Eins

- Das neutrale Element einer Gruppe wird auch **Einselement** genannt.
- In **additiver Schreibweise** bezeichnet man das Operationssymbol in einer Struktur manchmal mit $+$. Das neutrale Element nennt man dann das **Nullelement**. Es gilt:

$$0 + a = a + 0 = a$$

- In einer Gruppe $[T, \circ]$ bezeichnet man das inverse Element von a mit a^{-1} , in additiver Schreibweise mit $-a$.

Ring

Eine Algebra $[T, +, \circ]$ heißt **Ring**, wenn

- $[T, +]$ eine **abelsche** Gruppe und
- $[T, \circ]$ eine Halbgruppe ist, und
- wenn für alle $a, b, c \in T$ gilt:
 $a \circ (b + c) = a \circ b + a \circ c$
 $(b + c) \circ a = b \circ a + c \circ a$. („Distributivgesetz“)

Ist $[T, +, \circ]$ ein Ring und \circ kommutativ, so ist $[T, +, \circ]$ ein **kommutativer Ring**.

Gibt es ein Einselement bzgl. \circ , dann ist es ein **Ring mit Einselement**.

Beispiel

$[Z, +, \cdot]$

Polynomringe

Polynome mit Addition und Multiplikation (aus der Schule bekannt) bilden einen **kommutativen Ring mit Einselement**.

Körper

Ein kommutativer Ring $[T, +, \circ]$ heißt **Körper**, falls $[T \setminus \{0\}, \circ]$ eine Gruppe ist.

Unterstruktur

Sei $[T, f_1, \dots, f_n]$ algebraische Struktur einer gewissen Klasse und $U \subseteq T, U \neq \emptyset$. Ist $[U, f_1, \dots, f_n]$ eine Struktur derselben Klasse, so nennt man $[U, f_1, \dots, f_n]$ eine **Unterstruktur** von $[T, f_1, \dots, f_n]$.

Wichtig:

Die Operationen f_j müssen **abgeschlossen** auf U sein, d.h. falls f_j eine k -stellige Funktion ist, dann muss für alle $x_1, \dots, x_k \in U$ gelten: $f(x_1, \dots, x_k) \in U$.

Beispiele

- $[Z, +]$ Untergruppe von $[R, +]$
- $[Z, +, \cdot]$ Unterring von $[R, +, \cdot]$ (Kein Unterkörper!)
- $[Q, +, \cdot]$ Unterkörper von $[R, +, \cdot]$
- $[G, +, \cdot]$ Unterring von $[Z, +, \cdot]$, wobei $G = \{\dots, -4, -2, 0, 2, 4, 6, \dots\} = 2Z$

Isomorphismus

Isomorph bedeutet:

- gleich „bis auf die Bezeichnung der Objekte“
- nicht unterscheidbar aus der Sicht der Algebra
- alle „algebraischen Eigenschaften“ bleiben erhalten (z.B. Ordnung eines Elements)
- Verknüpfungstabellen sind identisch (bis auf Umbenennung und Umstellung der Objekte)

Graphisomorphismus

Um zu beweisen, dass zwei Graphen isomorph sind, ist es notwendig, dass folgende Bedingungen erfüllt sind:

- Beide Graphen haben dieselbe Anzahl Knoten und Kanten.
- Knoten mit denselben Eingangs- und Ausgangsgraden lassen sich einander zuordnen. Diese Bedingungen sind nicht hinreichend.

Tabelle mit Knoten aufstellen

- OutDeg und InDeg für Knoten von ersten Graph aufstellen
- Knoten von zweiten Graphen zuordnen anhand von erster Tabelle (gleiche In und Out Degrees)

Sei $G = [V, \rightarrow]$ ein Graph.

$$InDeg(v) := |\{w \in V | w \rightarrow v\}| \text{ (Eingangsgrad)}$$
$$OutDeg(v) := |\{w \in V | v \rightarrow w\}| \text{ (Ausgangsgrad)}$$

pq Formel

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Rechnen mit Restklassen

\sim_n ist „verträglich“ mit $+$ und \cdot und damit eine **Kongruenzrelation**.

$$[x]_n + [y]_n := [x + y]_n$$

$$[x]_n * [y]_n := [x \cdot y]_n$$

Eigenschaften der Restklassenoperationen

- $[Z_n, +, \cdot]$ ist kommutativer Ring mit Einselement
- $a \in Z_n$ ist invertierbar $\iff ggT(a, n) = 1$ (a und n teilerfremd)
- Falls p Primzahl, dann $[Z_p, +, \cdot]$ ist (endlicher) Körper.

Erweiterter Euklidischer Algorithmus

Findet den größten gemeinsamen Teiler (GCD) von zwei positiven ganzen Zahlen. (Benötigt für Inverse, a^{-1} mit $a * a^{-1} = 1 \bmod n$ für a^{-1} existiert nur wenn $\text{ggT}(a,n)=1$)

$\text{ggT}(a,b)$ $d = s * a + t * b$, wobei d der GGT ist.

Folglich wenn a und b teilerfremd sind $1 = s * a + t * b$

1. Setze

$m = a$
 $n = b$
 $s = 1$
 $t = 0$
 $u = 0$
 $v = 1$

2. Berechne q und r mit $m = q * n + r$ (Division mit Rest)
3. Setze

$m = n$
 $n = r$
 $u_{neu} = s - q * u$
 $v_{neu} = t - q * v$

4. Setze

$s = u$
 $t = v$
 $u = u_{neu}$
 $v = v_{neu}$

5. Falls $n > 0$ gehe zu Schritt 2

Für a = 37 und b = 16

37	=	1 * 37 + 0
16	=	0 * 37 + 1 * 16 (q = 2)
5	=	1 * 37 - 2 * 16 (q = 3)
1	=	(-3) * 37 + 7 * 16 (q = 5)
0	=	16 * 37 - 37 * 16

$\text{ggT}(37, 16) = 1 = (-3) * 37 + 7 * 16$

Komplexe Zahlen

$[\mathbb{C}, +, \cdot]$ ist ein Körper.

$i^2 = -1, i^3 = -i \mid i^4 = 1, i^5 = i; i^{-1} = \frac{1}{i} = -i$

Kartesische Koordinaten / Polarkoordinaten

- Kartesische Koordinaten: (x, y) $x = r \cos(\phi), y = r \sin(\phi)$
- Polarkoordinaten $[r; \phi]$ $r = \sqrt{x^2 + y^2} = |z|, \phi = \arctan(\frac{y}{x})$
- $x + yi = r(\cos(\phi) + i \sin(\phi))$

Rechenoperationen

$z_1 = a + bi$ $z_2 = c + di$ bzw. $z_1 = [r_1; \phi_1]$ $z_2 = [r_2; \phi_2]$

$z_1 \pm z_2$	$z_1 * z_2$	$\frac{z_1}{z_2}$	
$a \pm c + (b \pm d)i$	$a \pm c + (b \pm d)i$	Bruch erweitern mit z_2^*	karth.
ungünstig	$[r_1 * r_2; \phi_1 + \phi_2]$	$[\frac{r_1}{r_2}; \phi_1 - \phi_2]$	polar

konjugiert Komplex
 $z = a + i * b \rightarrow z^* = a - i * b$

Potenzieren

$z^n = [r^n; n\phi]$ d.h.
 $z^n = r^n(\cos(n\phi) + i \sin(n\phi))$

Betrag

$|z| = \sqrt{x^2 + y^2}$

Newton-Algorithmus

1. wähle Näherungsgrenze & Startwerte
2. Setze Startwert in Funktion und erste Ableitung ein
3. dividiere Funktionswert durch den Funktionswert der ersten Ableitung $\frac{f(x_n)}{f'(x_n)} = \overline{x}$
4. von Startwert das Ergebnis der Division von 3. abziehen ($x = x - \overline{x}$), wieder Funktionswerte mit neuem Wert dividieren so lange bis Näherung ausreicht.

Sonstiges

- $a \circ b := (b - 1)(a + 1)$ ist nicht kommutativ auf \mathbb{R}
- Hintereinanderausführung von totalen Funktionen ist assoziativ.
- $[\mathbb{N}, *]$ ist keine abelsche Gruppe.
- In $[\mathbb{Z}_9, *]$ gilt $3 * 7 = 3$
- In jeder Gruppe $[G, \circ]$ gilt **nicht:** $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$
- In einem Monoid mit neutralen Element e gibt es ein a mit $a \circ a = e$
- Falls e das neutrale Element in einer Gruppe ist, dann ist $e^{-1} = e$
- Jede Algebra ist zu sich selbst isomorph
- Die Gleichung $|z^2| = 1$ hat nicht genau 2 komplexe Lösungen