Einführung in die Theoretische Informatik

Woche 4

Harald Zankl

Institut für Informatik @ UIBK

Wintersemester 2014/2015

Zusammenfassung der letzten LV

Modus Ponens

$$\frac{A \to B \quad A}{B}\ MP$$

Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

$$\begin{array}{ll} (1) & A \to (B \to A) \\ (2) & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\ (3) & (\neg A \to \neg B) \to (B \to A) \end{array}$$

Satz

Das Axiomensystem mit Inferenzregel MP ist vollständig und korrekt für die Aussagenlogik: $A_1, \dots, A_n \models B$ *gdw.* $A_1, \dots, A_n \vdash B$

Konjunktive und Disjunktive Normalformen

Definition

Eine Wahrheitsfunktion $f\colon \{\mathrm{T},\mathrm{F}\}^n \to \{\mathrm{T},\mathrm{F}\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet

Definition

1. Formel A ist in konjunktiver Normalform (KNF), wenn A eine Konjunktion von Disjunktionen von Literalen ist
2. Formel A ist in disjunktiver Normalform (DNF), wenn A eine Disjunktion von Konjunktionen von Literalen ist

Folgerung

Für jede Formel A existiert eine DNF D und eine KNF K, sodass $A \equiv D \equiv K$ gilt.

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare, Verschlüsselung und Sicherheit

Algebraische Strukturen

Definition (Algebra)

Eine **Algebra** $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Trägern (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Algebraische Strukturen

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Trägern (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Algebraische Strukturen

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Trägern (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Algebraische Strukturen

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Trägern (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Beispiel

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und $\bullet$ gegeben durch:

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \dots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a\rangle$ mit $A = \{a, b, c, d\}$

$$x_1 \qquad a \qquad b \qquad \bullet(x_1, x_2) \qquad x_1 \bullet x_2 \qquad a \bullet b \qquad a \bullet (x_3 \bullet a)$$

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$

x_1 ✓ $\quad a \quad b \quad \bullet(x_1, x_2) \quad x_1 \bullet x_2 \quad a \bullet b \quad a \bullet (x_3 \bullet a)$

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$

x_1 ✓ a ✓ b $\bullet(x_1, x_2)$ $x_1 \bullet x_2$ $a \bullet b$ $a \bullet (x_3 \bullet a)$

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$

x_1 ✓ a ✓ b ✗ $\bullet(x_1, x_2)$ $x_1 \bullet x_2$ $a \bullet b$ $a \bullet (x_3 \bullet a)$

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a\rangle$ mit $A = \{a, b, c, d\}$

x_1 ✓ $\quad a$ ✓ $\quad b$ ✗ $\quad \bullet(x_1, x_2)$ ✓ $\quad x_1 \bullet x_2 \quad a \bullet b \quad a \bullet (x_3 \bullet a)$

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$

$$x_1 ✓ \quad a ✓ \quad b ✗ \quad \bullet(x_1, x_2) ✓ \quad x_1 \bullet x_2 ✓ \quad a \bullet b \quad a \bullet (x_3 \bullet a)$$

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$

x_1 ✓ a ✓ b ✗ $\bullet(x_1, x_2)$ ✓ $x_1 \bullet x_2$ ✓ $a \bullet b$ ✗ $a \bullet (x_3 \bullet a)$

Definition (Algebraische Ausdrücke)

Sei $\mathcal{A}$ eine Algebra. Nullstellige Operationen werden auch Konstanten genannt. Wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und definieren algebraische Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $E_1, \ldots, E_n$ algebraische Ausdrücke und $\circ$ eine Operation, dann ist $\circ(E_1, \ldots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$

x_1 ✓ a ✓ b ✗ $\bullet(x_1, x_2)$ ✓ $x_1 \bullet x_2$ ✓ $a \bullet b$ ✗ $a \bullet (x_3 \bullet a)$ ✓

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Beispiel (Äquivalenz)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a\rangle$ mit $A = \{a, b, c, d\}$ und $\bullet$ gegeben durch:

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

$x_1 \approx a \qquad x_1 \approx x_1 \bullet x_2 \qquad x_1 \approx a \bullet (x_1 \bullet a) \qquad a \approx a \bullet (x_1 \bullet a) \qquad x_1 \bullet x_2 \approx a \bullet (x_3 \bullet a)$

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Beispiel (Äquivalenz)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und $\bullet$ gegeben durch:

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

$x_1 \approx a$ ✗ $\quad x_1 \approx x_1 \bullet x_2 \quad x_1 \approx a \bullet (x_1 \bullet a) \quad a \approx a \bullet (x_1 \bullet a) \quad x_1 \bullet x_2 \approx a \bullet (x_3 \bullet a)$

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Beispiel (Äquivalenz)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und $\bullet$ gegeben durch:

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

$x_1 \approx a$ ✗ $\quad x_1 \approx x_1 \bullet x_2$ ✗ $\quad x_1 \approx a \bullet (x_1 \bullet a) \quad a \approx a \bullet (x_1 \bullet a) \quad x_1 \bullet x_2 \approx a \bullet (x_3 \bullet a)$

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Beispiel (Äquivalenz)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und $\bullet$ gegeben durch:

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

$x_1 \approx a$ ✗ $\quad x_1 \approx x_1 \bullet x_2$ ✗ $\quad x_1 \approx a \bullet (x_1 \bullet a)$ ✓ $\quad a \approx a \bullet (x_1 \bullet a) \quad x_1 \bullet x_2 \approx a \bullet (x_3 \bullet a)$

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Beispiel (Äquivalenz)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und $\bullet$ gegeben durch:

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

$x_1 \approx a$ ✗ $\quad x_1 \approx x_1 \bullet x_2$ ✗ $\quad x_1 \approx a \bullet (x_1 \bullet a)$ ✓ $\quad a \approx a \bullet (x_1 \bullet a)$ ✗ $\quad x_1 \bullet x_2 \approx a \bullet (x_3 \bullet a)$

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra $\mathcal{A}$.

- Ersetzen von Variablen in E durch Werte aus Träger liefert Instanz E'.
- E und F sind äquivalent, wenn für alle Instanzen E' und F' deren Auswertung in $\mathcal{A}$ übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Beispiel (Äquivalenz)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und $\bullet$ gegeben durch:

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

$x_1 \approx a$ ✗ $\quad x_1 \approx x_1 \bullet x_2$ ✗ $\quad x_1 \approx a \bullet (x_1 \bullet a)$ ✓ $\quad a \approx a \bullet (x_1 \bullet a)$ ✗ $\quad x_1 \bullet x_2 \approx a \bullet (x_3 \bullet a)$ ✗

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- $0 \in A$ heißt Nullelement für $\circ$, wenn

$$\text{für alle } a \in A \text{ gilt } a \circ 0 = 0 \circ a = 0$$

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- $0 \in A$ heißt Nullelement für $\circ$, wenn

$$\text{für alle } a \in A \text{ gilt } a \circ 0 = 0 \circ a = 0$$

- $1 \in A$ heißt Einselement (neutrales Element) für $\circ$, wenn

$$\text{für alle } a \in A \text{ gilt } a \circ 1 = 1 \circ a = a$$

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- $0 \in A$ heißt Nullelement für $\circ$, wenn
$$\text{für alle } a \in A \text{ gilt } a \circ 0 = 0 \circ a = 0$$
- $1 \in A$ heißt Einselement (neutrales Element) für $\circ$, wenn
$$\text{für alle } a \in A \text{ gilt } a \circ 1 = 1 \circ a = a$$
- $b \in A$ heißt Inverses von a, wenn 1 das neutrale Element für $\circ$ und
$$a \circ b = b \circ a = 1$$

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- $0 \in A$ heißt Nullelement für $\circ$, wenn
$$\text{für alle } a \in A \text{ gilt } a \circ 0 = 0 \circ a = 0$$
- $1 \in A$ heißt Einselement (neutrales Element) für $\circ$, wenn
$$\text{für alle } a \in A \text{ gilt } a \circ 1 = 1 \circ a = a$$
- $b \in A$ heißt Inverses von a, wenn 1 das neutrale Element für $\circ$ und
$$a \circ b = b \circ a = 1$$

Bemerkung

Nullelement, Einselement, bzw. Inverses existieren nicht immer.

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- $0 \in A$ heißt Nullelement für $\circ$, wenn
$$\text{für alle } a \in A \text{ gilt } a \circ 0 = 0 \circ a = 0$$
- $1 \in A$ heißt Einselement (neutrales Element) für $\circ$, wenn
$$\text{für alle } a \in A \text{ gilt } a \circ 1 = 1 \circ a = a$$
- $b \in A$ heißt Inverses von a, wenn 1 das neutrale Element für $\circ$ und
$$a \circ b = b \circ a = 1$$

Bemerkung

Nullelement, Einselement, bzw. Inverses existieren nicht immer.

Beispiel (Algebra $\mathcal{A}$ bezüglich $\bullet$)

Nullelement: ✗ Einselement: a Inverses von $a/b/c/d$ ist $a/d/c/b$

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A
2. Angenommen e und u sind neutrale Elemente für $\circ$

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A
2. Angenommen e und u sind neutrale Elemente für $\circ$
3. Wir zeigen, dass $e = u$

$$\begin{aligned} e &= e \circ u && \text{da } u \text{ Einselement} \\ &= u && \text{da } e \text{ Einselement} \end{aligned}$$

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A
2. Angenommen e und u sind neutrale Elemente für $\circ$
3. Wir zeigen, dass $e = u$

$$\begin{aligned} e &= e \circ u && \text{da } u \text{ Einselement} \\ &= u && \text{da } e \text{ Einselement} \end{aligned}$$

$\blacksquare$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel (Algebra $\mathcal{A}$)

1. $\bullet$ ist nicht assoziativ, da z.B. $d \bullet (d \bullet d) \neq (d \bullet d) \bullet d$
2. $\longrightarrow \langle A, \bullet \rangle$ ist keine Halbgruppe
3. $\longrightarrow \langle A, \bullet, a \rangle$ ist kein Monoid
4. $\longrightarrow \langle A, \bullet, a \rangle$ ist keine Gruppe
5. $\bullet$ ist nicht kommutativ, da z.B. $c \bullet d \neq d \bullet c$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ $\langle \mathbb{N}, \times \rangle$ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ $\langle \mathbb{N}, \times, 1 \rangle$ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓
- Gruppe: $\langle \mathbb{N}, +, 0 \rangle$ $\langle \mathbb{N}, \times, 1 \rangle$ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓
- Gruppe: $\langle \mathbb{N}, +, 0 \rangle$ ✗ $\langle \mathbb{N}, \times, 1 \rangle$ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓
- Gruppe: $\langle \mathbb{N}, +, 0 \rangle$ ✗ $\langle \mathbb{N}, \times, 1 \rangle$ ✗ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

- $\langle A; \circ \rangle$ Halbgruppe, wenn $\circ$ assoziativ
- $\langle A; \circ, 1 \rangle$ Monoid, wenn $\langle A; \circ \rangle$ eine Halbgruppe mit Einselement 1
- $\langle A; \circ, 1 \rangle$ Gruppe, wenn $\langle A; \circ, 1 \rangle$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen kommutativ, wenn $\circ$ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓
- Gruppe: $\langle \mathbb{N}, +, 0 \rangle$ ✗ $\langle \mathbb{N}, \times, 1 \rangle$ ✗ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ *ein Monoid ist, dann ist das Inverse eindeutig*

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$b = b \circ 1 \qquad \text{1 ist neutrales Element}$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1\rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Inverses von } a
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Inverses von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1\rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Inverses von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ \\
&= 1 \circ c && b \text{ ist Inverses von } a
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Inverses von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ \\
&= 1 \circ c && b \text{ ist Inverses von } a \\
&= c && \text{1 ist neutrales Element}
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$\begin{aligned} b &= b \circ 1 && \text{1 ist neutrales Element} \\ &= b \circ (a \circ c) && c \text{ ist Inverses von } a \\ &= (b \circ a) \circ c && \text{Assoziativität von } \circ \\ &= 1 \circ c && b \text{ ist Inverses von } a \\ &= c && \text{1 ist neutrales Element} \end{aligned}$$

∎

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe
2. $\langle A; \cdot, 1 \rangle$ ein Monoid

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe
2. $\langle A; \cdot, 1 \rangle$ ein Monoid
3. $\cdot$ distribuiert über $+$ (von links und von rechts), das heißt für alle $a, b, c \in A$ gilt:

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

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe
2. $\langle A; \cdot, 1 \rangle$ ein Monoid
3. $\cdot$ distribuiert über $+$ (von links und von rechts), das heißt für alle $a, b, c \in A$ gilt:

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

Definition (Körper)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Körper, wenn

1. $\mathcal{A}$ ein Ring
2. $\langle A \setminus \{0\}; \cdot, 1 \rangle$ eine kommutative Gruppe

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, ^{-}, 0, 1 \rangle$ heißt Boolesche Algebra wenn gilt:

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \overline{}, 0, 1 \rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0 \rangle$ und $\langle B; \cdot, 1 \rangle$ sind kommutative Monoide

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, ^{-}, 0, 1 \rangle$ heißt **Boolesche Algebra** wenn gilt:

1. $\langle B; +, 0 \rangle$ und $\langle B; \cdot, 1 \rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:

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

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \overline{}, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:

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

3. Für alle $a \in B$ gilt

$$a + \overline{a} = 1 \qquad a \cdot \overline{a} = 0$$

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \overline{}, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad a + (b \cdot c) = (a + b) \cdot (a + c)$$
3. Für alle $a \in B$ gilt
$$a + \overline{a} = 1 \qquad a \cdot \overline{a} = 0$$

Das Element $\overline{a}$ heißt das Komplement oder die Negation von a

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \overline{}, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad a + (b \cdot c) = (a + b) \cdot (a + c)$$
3. Für alle $a \in B$ gilt
$$a + \overline{a} = 1 \qquad a \cdot \overline{a} = 0$$

Das Element $\overline{a}$ heißt das Komplement oder die Negation von a

Konventionen

- Wir lassen $\cdot$ oft weg und schreiben ab statt $a \cdot b$
- Wir verwenden die folgende Präzedenz:
Komplement ($\overline{}$) bindet am stärksten, und $\cdot$ bindet stärker als $+$

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Boolesche Variablen sind Boolesche Ausdrücke

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Boolesche Variablen sind Boolesche Ausdrücke
2. Wenn A und B Boolesche Ausdrücke sind, dann sind

$$\overline{A} \qquad (A \cdot B) \qquad (A + B)$$

   Boolesche Ausdrücke

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Boolesche Variablen sind Boolesche Ausdrücke
2. Wenn A und B Boolesche Ausdrücke sind, dann sind

$$\overline{A} \qquad (A \cdot B) \qquad (A + B)$$

   Boolesche Ausdrücke

Beispiel

Die folgenden Ausdrücke sind Boolesche Ausdrücke:

$$x_1 \quad x_2 \quad x_1 + x_2 \quad x_1 \cdot x_2 \quad x_1 \cdot (x_1 + x_2) \quad x_1(x_1 + x_2) \quad x_1\overline{(x_1 + x_2)}$$

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, {}^{-}, \varnothing, M \rangle$$

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \bar{\ }, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, ^{-}, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \bar{\ }, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge
3. $\bar{\ }$ die Komplementärmenge (bezüglich M)

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \bar{\ }, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge
3. $\bar{\ }$ die Komplementärmenge (bezüglich M)

Diese Algebra nennt man Mengenalgebra.

Definitionen

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \bar{\ }, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge
3. $\bar{\ }$ die Komplementärmenge (bezüglich M)

Diese Algebra nennt man Mengenalgebra.

Definitionen

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Binäre Algebra

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$

Definition

Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, ^{-}, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, ^{-}$ wie folgt definiert:

Binäre Algebra

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$

Definition

Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \bar{\ }, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, \bar{\ }$ wie folgt definiert:

$+$	1	0
1	1	1
0	1	0

$\cdot$	1	0
1	1	0
0	0	0

$\bar{\ }$	
1	0
0	1

Binäre Algebra

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$

Definition

Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \overline{}, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, \overline{}$ wie folgt definiert:

$+$	1	0
1	1	1
0	1	0

$\cdot$	1	0
1	1	0
0	0	0

$\overline{}$	
1	0
0	1

Diese Algebra nennt man binäre Algebra

Binäre Algebra

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$

Definition

Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \overline{}, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, \overline{}$ wie folgt definiert:

$+$	1	0
1	1	1
0	1	0

$\cdot$	1	0
1	1	0
0	0	0

$\overline{}$	
1	0
0	1

Diese Algebra nennt man binäre Algebra

Lemma

Die binäre Algebra ist eine Boolesche Algebra

Sei Frm die Menge der aussagenlogischen Formeln

Definition

Wir betrachten die Algebra $\mathcal{F}rm$

$$\langle \mathsf{Frm}; \vee, \wedge, \neg, \mathsf{False}, \mathsf{True} \rangle$$

Wobei die Zeichen wie in der Aussagenlogik interpretiert werden

Sei Frm die Menge der aussagenlogischen Formeln

Definition

Wir betrachten die Algebra $\mathcal{F}rm$

$$\langle \mathsf{Frm}; \vee, \wedge, \neg, \mathsf{False}, \mathsf{True} \rangle$$

Wobei die Zeichen wie in der Aussagenlogik interpretiert werden

Lemma

Die Algebra $\mathcal{F}rm$ ist eine Boolesche Algebra

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

zurück

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

▸ zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$

- $\mathcal{P}(A) =$
- $A \cap B =$
- $A \cup B =$
- $A \times B =$
- $\overline{A} =$
- $\overline{B} =$

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$

- $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \ldots, \{a, b, c, d\}\}$
- $A \cap B =$
- $A \cup B =$
- $A \times B =$
- $\overline{A} =$
- $\overline{B} =$

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$

- $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \dots, \{a, b, c, d\}\}$
- $A \cap B = \{a, d\}$
- $A \cup B =$
- $A \times B =$
- $\overline{A} =$
- $\overline{B} =$

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$

- $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \ldots, \{a, b, c, d\}\}$
- $A \cap B = \{a, d\}$
- $A \cup B = \{a, b, c, d, e\}$
- $A \times B =$
- $\overline{A} =$
- $\overline{B} =$

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$

- $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \ldots, \{a, b, c, d\}\}$
- $A \cap B = \{a, d\}$
- $A \cup B = \{a, b, c, d, e\}$
- $A \times B = \{(a, a), (a, d), (a, e), (b, a), \ldots, (c, e), (d, a), (d, d), (d, e)\}$
- $\overline{A} =$
- $\overline{B} =$

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$ und $M = \{a, b, c, d, e, f\}$.

- $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \ldots, \{a, b, c, d\}\}$
- $A \cap B = \{a, d\}$
- $A \cup B = \{a, b, c, d, e\}$
- $A \times B = \{(a, a), (a, d), (a, e), (b, a), \ldots, (c, e), (d, a), (d, d), (d, e)\}$
- $\overline{A} =$
- $\overline{B} =$

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$ und $M = \{a, b, c, d, e, f\}$.

- $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \ldots, \{a, b, c, d\}\}$
- $A \cap B = \{a, d\}$
- $A \cup B = \{a, b, c, d, e\}$
- $A \times B = \{(a, a), (a, d), (a, e), (b, a), \ldots, (c, e), (d, a), (d, d), (d, e)\}$
- $\overline{A} = \{e, f\}$
- $\overline{B} =$

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in A\}$
- $\overline{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

▸ zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$ und $M = \{a, b, c, d, e, f\}$.

- $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \ldots, \{a, b, c, d\}\}$
- $A \cap B = \{a, d\}$
- $A \cup B = \{a, b, c, d, e\}$
- $A \times B = \{(a, a), (a, d), (a, e), (b, a), \ldots, (c, e), (d, a), (d, d), (d, e)\}$
- $\overline{A} = \{e, f\}$
- $\overline{B} = \{b, c, f\}$