Diskrete Strukturen

Vorlesung 9: Algebraische Strukturen & Verbände

11. Dezember 2018

Nächste Termine — Modul “Diskrete Strukturen”

Hörsaalübung (Mo. 9:15)	Vorlesung (Di. 17:15)
10.12. Hörsaalübung Übung Götze 13.12. 7:30 Uhr	11.12. Alg. Strukturen, Verbände (4. Abgabe + 5. Übungsblatt)
17.12. Hörsaalübung 5. Übungswoche	18.12. Boolesche Algebren, Gruppen
24.12.	25.12.
31.12.	1.1.
7.1.	8.1. Körper (5. Abgabe + 6. Übungsblatt)
14.1. Hörsaalübung 6. Übungswoche	15.1. Graphen und Bäume
21.1.	22.1. Planarität von Graphen (6. Abgabe + 7. Übungsblatt)
28.1. Hörsaalübung 7. Übungswoche	29.1. Färbbarkeit von Graphen
4.2. Tutorium (Klausurvorbereitung)	5.2. Arithmetik

Vorlesungsstruktur

1. Mathematische Grundlagen
   - Aussagen- und Prädikatenlogik
   - Naive Mengenlehre
   - Relationen und Funktionen

2. Diskrete Strukturen
   - Algebraische Strukturen
   - Bäume und Graphen
   - Arithmetik

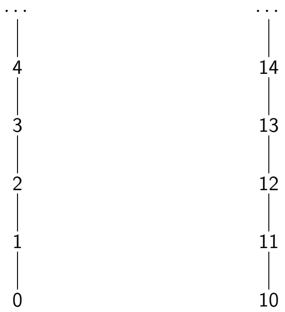
Heutige Vorlesung

- Algebraische Strukturen und Isomorphie
- Korrespondenz Ordnungsstruktur & algebraische Darstellung
- Unterstruktur
- Charakterisierung Distributivität
- Einführung Boolesche Algebren

Bitte Fragen direkt stellen!

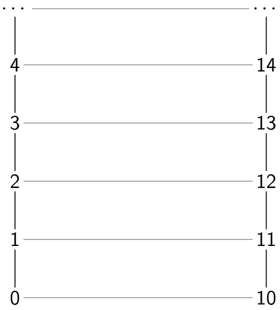
Motivation

- bisher nur Korrespondenz via Bijektion
  (für jede Äquivalenzrelation gibt es eine Zerlegung, . . .)
- häufig möchte man jedoch strukturerhaltende “Gleichheit”, die Umbenennungen der Elemente ignoriert



Motivation

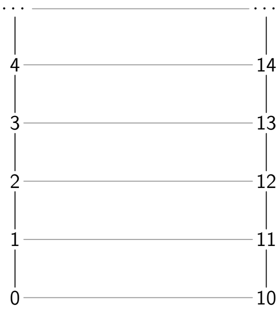
- bisher nur Korrespondenz via Bijektion
  (für jede Äquivalenzrelation gibt es eine Zerlegung, ...)
- häufig möchte man jedoch strukturerhaltende “Gleichheit”, die Umbenennungen der Elemente ignoriert



Algebraische Strukturen — Grundlagen

Motivation

- bisher nur Korrespondenz via Bijektion
  (für jede Äquivalenzrelation gibt es eine Zerlegung, ...)
- häufig möchte man jedoch strukturerhaltende “Gleichheit”, die Umbenennungen der Elemente ignoriert
- Ziel: “gleich” rechnen in strukturäquivalenten Mengen
- daher zunächst Formalisierung ‘algebraische Struktur’



Motivation:

- wir können auch “Mengen” von komplizierten Objekten betrachten
- Beispiele

$$\begin{aligned}\mathrm{Verb} &= \{(M, \preceq) \mid (M, \preceq) \text{ Verband}\}\\ \mathrm{Zerl} &= \{(M, \mathcal{M}) \mid \mathcal{M} \text{ Zerlegung von } M\}\\ \text{Äq} &= \{(M, \equiv) \mid {\equiv} \text{ Äquivalenzrelation auf } M\}\end{aligned}$$

§9.1 Theorem

Die Funktion $f \colon \text{Äq} \to \text{Zerl}$ mit

$$f\big((M, \equiv)\big) = \big(M, (M/{\equiv})\big)$$

für alle $(M, \equiv) \in \text{Äq}$ ist bijektiv

§9.1 Theorem

Die Funktion $f\colon \text{Äq} \to \text{Zerl}$ mit

$$f\big((M, \equiv)\big) = \big(M, (M/{\equiv})\big)$$

für alle $(M, \equiv) \in \text{Äq}$ ist bijektiv

Beweis (direkt).

Für jede Äquivalenzrelation $\equiv$ auf M ist $(M/{\equiv})$ eine Zerlegung von M gemäß §5.6. Also gilt $f((M, \equiv)) \in \text{Zerl}$.

§9.1 Theorem

Die Funktion $f\colon \text{Äq} \to \text{Zerl}$ mit

$$f\big((M, \equiv)\big) = \big(M, (M/{\equiv})\big)$$

für alle $(M, \equiv) \in \text{Äq}$ ist bijektiv

Beweis (direkt).

Für jede Äquivalenzrelation $\equiv$ auf M ist $(M/{\equiv})$ eine Zerlegung von M gemäß §5.6. Also gilt $f((M, \equiv)) \in \text{Zerl}$.

Des Weiteren gibt es nach §5.7 eine Funktion $g\colon \text{Zerl} \to \text{Äq}$, so dass $f \mathbin{;} g = \text{id}_{\text{Äq}}$ und $g \mathbin{;} f = \text{id}_{\text{Zerl}}$ (siehe §5.8).

§9.1 Theorem

Die Funktion $f\colon \text{Äq} \to \text{Zerl}$ mit

$$f\big((M, \equiv)\big) = \big(M, (M/{\equiv})\big)$$

für alle $(M, \equiv) \in \text{Äq}$ ist bijektiv

Beweis (direkt).

Für jede Äquivalenzrelation $\equiv$ auf M ist $(M/{\equiv})$ eine Zerlegung von M gemäß §5.6. Also gilt $f((M, \equiv)) \in \text{Zerl}$.

Des Weiteren gibt es nach §5.7 eine Funktion $g\colon \text{Zerl} \to \text{Äq}$, so dass $f\,;g = \text{id}_{\text{Äq}}$ und $g\,;f = \text{id}_{\text{Zerl}}$ (siehe §5.8).

Damit ist f invertierbar und deshalb nach §6.2 bijektiv. $\square$

Kurzeinführung:

- algebraische Struktur ist eine Menge M
  zusammen mit Relationen, Funktionen, und Konstanten auf M
- häufig unterliegen diese weiteren Einschränkungen

Kurzeinführung:

- algebraische Struktur ist eine Menge M
  zusammen mit Relationen, Funktionen, und Konstanten auf M
- häufig unterliegen diese weiteren Einschränkungen

Beispiele

- $(\mathbb{N}, \mathrm{nachfolger}, 0)$ ist eine algebraische Struktur mit
  - einer Funktion $\mathrm{nachfolger} \colon \mathbb{N} \to \mathbb{N}$ und
  - einer Konstante $0 \in \mathbb{N}$

Algebraische Strukturen — Grundlagen

Kurzeinführung:

- algebraische Struktur ist eine Menge M
  zusammen mit Relationen, Funktionen, und Konstanten auf M
- häufig unterliegen diese weiteren Einschränkungen

Beispiele

- $(\mathbb{N}, \text{nachfolger}, 0)$ ist eine algebraische Struktur mit
  - einer Funktion $\text{nachfolger} \colon \mathbb{N} \to \mathbb{N}$ und
  - einer Konstante $0 \in \mathbb{N}$
- Peano-Axiome beschreiben algebraische Strukturen (N, s, z) mit
  (siehe §6.6)
  - einer Funktion $s \colon N \to N$ und (speziell: injektiver Funktion)
  - einer Konstante $z \in N$ (mit weiteren Eigenschaften)

Algebraische Strukturen — Grundlagen

Kurzeinführung:

- algebraische Struktur ist eine Menge M zusammen mit Relationen, Funktionen, und Konstanten auf M
- häufig unterliegen diese weiteren Einschränkungen

Beispiele

- $(\mathbb{N}, \text{nachfolger}, 0)$ ist eine algebraische Struktur mit
  - einer Funktion $\text{nachfolger} \colon \mathbb{N} \to \mathbb{N}$ und
  - einer Konstante $0 \in \mathbb{N}$
- Peano-Axiome beschreiben algebraische Strukturen (N, s, z) mit (siehe §6.6)
  - einer Funktion $s \colon N \to N$ und (speziell: injektiver Funktion)
  - einer Konstante $z \in N$ (mit weiteren Eigenschaften)
- jede teilweise geordnete Menge $(M, \preceq)$ ist eine algebraische Struktur mit
  - einer Relation $\preceq \subseteq M \times M$ (speziell: einer Ordnungsrelation)

§9.2 Definition (Algebraische Struktur)

Sei U eine Grundmenge und seien

- $R_1, \ldots, R_k \subseteq U \times U$ Relationen auf U

§9.2 Definition (Algebraische Struktur)

Sei U eine Grundmenge und seien

- $R_1, \ldots, R_k \subseteq U \times U$ Relationen auf U
- $f_1, \ldots, f_\ell \colon U \times U \to U$ binäre (zweistellige) Funktionen auf U

§9.2 Definition (Algebraische Struktur)

Sei U eine Grundmenge und seien

- $R_1, \ldots, R_k \subseteq U \times U$ Relationen auf U
- $f_1, \ldots, f_\ell \colon U \times U \to U$ binäre (zweistellige) Funktionen auf U
- $g_1, \ldots, g_m \colon U \to U$ unäre (einstellige) Funktionen auf U und

§9.2 Definition (Algebraische Struktur)

Sei U eine Grundmenge und seien

- $R_1, \ldots, R_k \subseteq U \times U$ Relationen auf U
- $f_1, \ldots, f_\ell \colon U \times U \to U$ binäre (zweistellige) Funktionen auf U
- $g_1, \ldots, g_m \colon U \to U$ unäre (einstellige) Funktionen auf U und
- $c_1, \ldots, c_n \in U$ Elemente (auch: Konstanten) von U.

§9.2 Definition (Algebraische Struktur)

Sei U eine Grundmenge und seien

- $R_1, \ldots, R_k \subseteq U \times U$ Relationen auf U
- $f_1, \ldots, f_\ell \colon U \times U \to U$ binäre (zweistellige) Funktionen auf U
- $g_1, \ldots, g_m \colon U \to U$ unäre (einstellige) Funktionen auf U und
- $c_1, \ldots, c_n \in U$ Elemente (auch: Konstanten) von U.

Dann ist $\big(U, \langle R_1, \ldots, R_k\rangle, \langle f_1, \ldots, f_\ell\rangle, \langle g_1, \ldots, g_m\rangle, \langle c_1, \ldots, c_n\rangle\big)$ eine algebraische Struktur des Typs $(k,\ \ell,\ m,\ n)$.

§9.2 Definition (Algebraische Struktur)

Sei U eine Grundmenge und seien

- $R_1, \dots, R_k \subseteq U \times U$ Relationen auf U
- $f_1, \dots, f_\ell \colon U \times U \to U$ binäre (zweistellige) Funktionen auf U
- $g_1, \dots, g_m \colon U \to U$ unäre (einstellige) Funktionen auf U und
- $c_1, \dots, c_n \in U$ Elemente (auch: Konstanten) von U.

Dann ist $\big(U, \langle R_1, \dots, R_k\rangle, \langle f_1, \dots, f_\ell\rangle, \langle g_1, \dots, g_m\rangle, \langle c_1, \dots, c_n\rangle\big)$ eine algebraische Struktur des Typs $(k,\ \ell,\ m,\ n)$.

Beispiele

- jede Äquivalenzrelation $\equiv\ \subseteq M \times M$ liefert eine algebraische Struktur $(M, \langle\equiv\rangle, \langle\rangle, \langle\rangle, \langle\rangle)$ des Typs $(1,\ 0,\ 0,\ 0)$
- die Wahrheitswerte $\{0, 1\}$ bilden eine algebraische Struktur $(\{0,\ 1\}, \langle\rangle, \langle\vee,\ \wedge\rangle, \langle\neg\rangle, \langle 0,\ 1\rangle)$ des Typs $(0,\ 2,\ 1,\ 2)$

Notizen

- algebraische Struktur
  = Grundmenge mit Relationen, Funktionen und Konstanten
- wir betrachten nur binäre und unäre Funktionen
  und (2-stellige) Relationen

Notizen

- algebraische Struktur
  = Grundmenge mit Relationen, Funktionen und Konstanten
- wir betrachten nur binäre und unäre Funktionen
  und (2-stellige) Relationen
- Reihenfolge im Typ:
  1. Anzahl Relationen
  2. Anzahl binärer Funktionen
  3. Anzahl unärer Funktionen
  4. Anzahl Konstanten
- wir lassen leere Blöcke am Ende weg
  und lassen die Gruppierung weg, falls offensichtlich
  z.B. $(M, \langle \preceq \rangle)$ oder $(M, \preceq)$ statt $(M, \langle \preceq \rangle, \langle \rangle, \langle \rangle, \langle \rangle)$

weitere Beispiele

- jede teilweise geordnete Menge $(M, \preceq)$ <u>ist</u> eine algebraische Struktur des Typs $(1, 0, 0, 0)$

weitere Beispiele

- jede teilweise geordnete Menge $(M, \preceq)$ <u>ist</u> eine algebraische Struktur des Typs $(1, 0, 0, 0)$
- die Peano-Axiome spezifizieren eine algebraische Struktur (N, s, z) des Typs $(0, 0, 1, 1)$

(Beschreibung der natürlichen Zahlen)

weitere Beispiele

- jede teilweise geordnete Menge $(M, \preceq)$ <u>ist</u> eine algebraische Struktur des Typs $(1, 0, 0, 0)$
- die Peano-Axiome spezifizieren eine algebraische Struktur (N, s, z) des Typs $(0, 0, 1, 1)$

  (Beschreibung der natürlichen Zahlen)
- jede Potenzmenge $\mathcal{P}(M)$ liefert eine algebraische Struktur $(\mathcal{P}(M), \subseteq, \cup, \cap, \cdot^c, \emptyset, M)$ des Typs $(1, 2, 1, 2)$

§9.2 Definition (Isomorphismus)

Seien $\mathcal{U} = (U, \langle R_1, \ldots, R_k\rangle, \langle f_1, \ldots, f_\ell\rangle, \langle g_1, \ldots, g_m\rangle, \langle c_1, \ldots, c_n\rangle)$ und $\mathcal{U}' = (U', \langle R'_1, \ldots, R'_k\rangle, \langle f'_1, \ldots, f'_\ell\rangle, \langle g'_1, \ldots, g'_m\rangle, \langle c'_1, \ldots, c'_n\rangle)$ zwei algebraische Strukturen gleichen Typs.
Eine Funktion $\varphi\colon U \to U'$ heißt Isomorphismus von $\mathcal{U}$ nach $\mathcal{U}'$, gdw.

- φ bijektiv ist,

§9.2 Definition (Isomorphismus)

Seien $\mathcal{U} = (U, \langle R_1, \ldots, R_k\rangle, \langle f_1, \ldots, f_\ell\rangle, \langle g_1, \ldots, g_m\rangle, \langle c_1, \ldots, c_n\rangle)$ und $\mathcal{U}' = (U', \langle R'_1, \ldots, R'_k\rangle, \langle f'_1, \ldots, f'_\ell\rangle, \langle g'_1, \ldots, g'_m\rangle, \langle c'_1, \ldots, c'_n\rangle)$ zwei algebraische Strukturen gleichen Typs.
Eine Funktion $\varphi\colon U \to U'$ heißt Isomorphismus von $\mathcal{U}$ nach $\mathcal{U}'$, gdw.

- φ bijektiv ist,
- für alle $1 \leq i \leq k$ und $u_1, u_2 \in U$ gilt

$$(u_1, u_2) \in R_i \qquad \text{gdw.} \qquad (\varphi(u_1), \varphi(u_2)) \in R'_i$$

§9.2 Definition (Isomorphismus)

Seien $\mathcal{U} = (U, \langle R_1, \dots, R_k\rangle, \langle f_1, \dots, f_\ell\rangle, \langle g_1, \dots, g_m\rangle, \langle c_1, \dots, c_n\rangle)$ und $\mathcal{U}' = (U', \langle R'_1, \dots, R'_k\rangle, \langle f'_1, \dots, f'_\ell\rangle, \langle g'_1, \dots, g'_m\rangle, \langle c'_1, \dots, c'_n\rangle)$ zwei algebraische Strukturen gleichen Typs.

Eine Funktion $\varphi\colon U \to U'$ heißt Isomorphismus von $\mathcal{U}$ nach $\mathcal{U}'$, gdw.

- φ bijektiv ist,
- für alle $1 \leq i \leq k$ und $u_1, u_2 \in U$ gilt

$$(u_1, u_2) \in R_i \qquad \text{gdw.} \qquad \big(\varphi(u_1), \varphi(u_2)\big) \in R'_i$$

- für alle $1 \leq i \leq \ell$ und $u_1, u_2 \in U$ gilt

$$\varphi\big(f_i(u_1, u_2)\big) = f'_i\big(\varphi(u_1), \varphi(u_2)\big)$$

- $\varphi\big(g_i(u)\big) = g'_i\big(\varphi(u)\big)$ für alle $1 \leq i \leq m$ und $u \in U$, und
- $\varphi(c_i) = c'_i$ für alle $1 \leq i \leq n$.

§9.2 Definition (Isomorphismus)

Seien $\mathcal{U} = (U, \langle R_1, \ldots, R_k\rangle, \langle f_1, \ldots, f_\ell\rangle, \langle g_1, \ldots, g_m\rangle, \langle c_1, \ldots, c_n\rangle)$ und $\mathcal{U}' = (U', \langle R'_1, \ldots, R'_k\rangle, \langle f'_1, \ldots, f'_\ell\rangle, \langle g'_1, \ldots, g'_m\rangle, \langle c'_1, \ldots, c'_n\rangle)$ zwei algebraische Strukturen gleichen Typs.
Eine Funktion $\varphi\colon U \to U'$ heißt Isomorphismus von $\mathcal{U}$ nach $\mathcal{U}'$, gdw.

- φ bijektiv ist,
- für alle $1 \leq i \leq k$ und $u_1, u_2 \in U$ gilt

$$(u_1, u_2) \in R_i \qquad \text{gdw.} \qquad \big(\varphi(u_1), \varphi(u_2)\big) \in R'_i$$

- für alle $1 \leq i \leq \ell$ und $u_1, u_2 \in U$ gilt

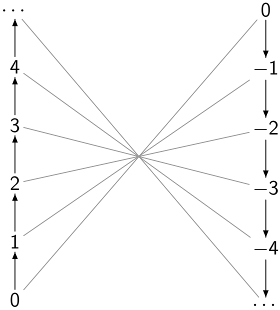
$$\varphi\big(f_i(u_1, u_2)\big) = f'_i\big(\varphi(u_1), \varphi(u_2)\big)$$

- $\varphi\big(g_i(u)\big) = g'_i\big(\varphi(u)\big)$ für alle $1 \leq i \leq m$ und $u \in U$, und
- $\varphi(c_i) = c'_i$ für alle $1 \leq i \leq n$.

$\mathcal{U}$ und $\mathcal{U}'$ heißen isomorph, gdw. ein solcher Isomorphismus existiert.

Beispiel

$(\mathbb{N}, \text{nachfolger}, 0)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, g, 0)$ mit $g(z) = z - 1$ für alle $z \leq 0$ sind isomorph vermittels

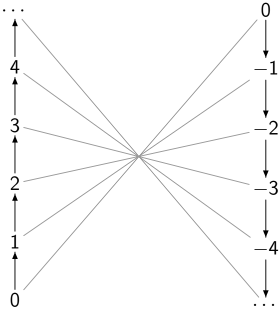


Algebraische Strukturen — Isomorphie

Beispiel

$(\mathbb{N}, \text{nachfolger}, 0)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, g, 0)$ mit $g(z) = z - 1$ für alle $z \leq 0$ sind isomorph vermittels Isomorphismus $\varphi(n) = -n$ für alle $n \in \mathbb{N}$

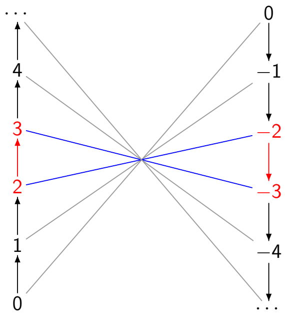
- φ bijektiv (leicht nachweisbar)
- $\varphi(\text{nachfolger}(n)) = \varphi(n+1) = -n-1 = g(-n) = g(\varphi(n))$



Beispiel

$(\mathbb{N}, \mathrm{nachfolger}, 0)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, g, 0)$ mit $g(z) = z - 1$ für alle $z \leq 0$ sind isomorph vermittels Isomorphismus $\varphi(n) = -n$ für alle $n \in \mathbb{N}$

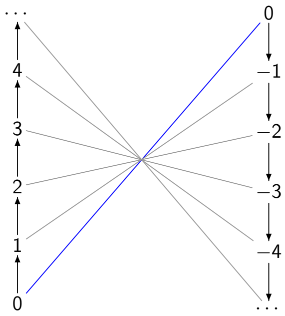
- φ bijektiv (leicht nachweisbar)
- $\varphi(\mathrm{nachfolger}(n)) = \varphi(n+1) = -n-1 = g(-n) = g(\varphi(n))$



Beispiel

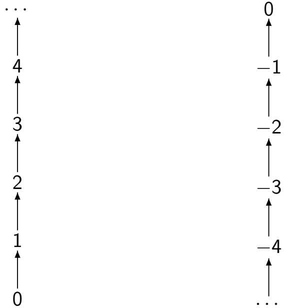
$(\mathbb{N}, \text{nachfolger}, 0)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, g, 0)$ mit $g(z) = z - 1$ für alle $z \leq 0$ sind isomorph vermittels Isomorphismus $\varphi(n) = -n$ für alle $n \in \mathbb{N}$

- φ bijektiv (leicht nachweisbar)
- $\varphi(\text{nachfolger}(n)) = \varphi(n+1) = -n-1 = g(-n) = g(\varphi(n))$
- $\varphi(0) = 0$



weiteres Beispiel

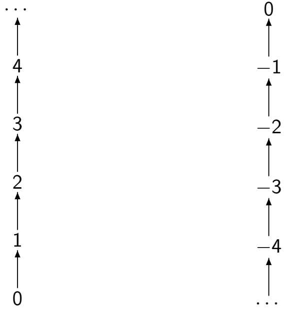
$(\mathbb{N}, \leq)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, \leq)$ sind nicht isomorph



weiteres Beispiel

$(\mathbb{N}, \leq)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, \leq)$ sind nicht isomorph

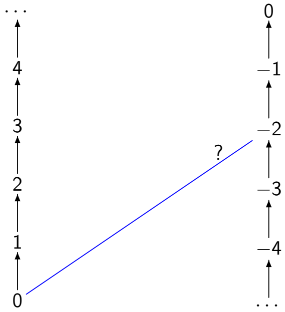
Beweis: Sei φ Isomorphismus und $z = \varphi(0)$.



weiteres Beispiel

$(\mathbb{N}, \leq)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, \leq)$ sind nicht isomorph

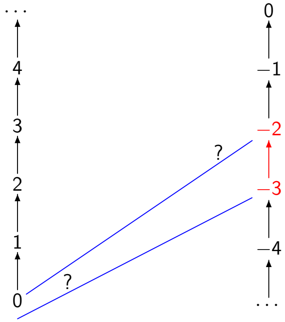
Beweis: Sei φ Isomorphismus und $z = \varphi(0)$. Da $z - 1 \leq 0$ und φ bijektiv, existiert $n \in \mathbb{N} \setminus \{0\}$, so dass $\varphi(n) = z - 1$. Es gilt $0 \leq n$, aber $\varphi(0) = z \not\leq z - 1 = \varphi(n)$ im Widerspruch zur Isomorphismus-Eigenschaft. Also existiert kein Isomorphismus und die Strukturen sind nicht isomorph.



weiteres Beispiel

$(\mathbb{N}, \leq)$ und $(\{z \in \mathbb{Z} \mid z \leq 0\}, \leq)$ sind nicht isomorph

Beweis: Sei φ Isomorphismus und $z = \varphi(0)$. Da $z - 1 \leq 0$ und φ bijektiv, existiert $n \in \mathbb{N} \setminus \{0\}$, so dass $\varphi(n) = z - 1$. Es gilt $0 \leq n$, aber $\varphi(0) = z \not\leq z - 1 = \varphi(n)$ im Widerspruch zur Isomorphismus-Eigenschaft. Also existiert kein Isomorphismus und die Strukturen sind nicht isomorph.



§9.3 Theorem

Isomorphie ist eine Äquivalenzrelation
auf algebraischen Strukturen eines bestimmten Typs.

Beweis.

leichte Übung $\square$

§9.4 Theorem

$\mathrm{id}_{\mathbb{Q}}$ ist der einzige Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$

§9.4 Theorem

$\mathrm{id}_{\mathbb{Q}}$ ist der einzige Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$

Beweis (direkt; 1/2).

Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.
Wir zeigen zunächst $\varphi(0) = 0$, $\varphi(1) = 1$ und $\varphi(-1) = -1$.

- $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$. Es gibt nur eine Zahl $n \in \mathbb{Q}$, so dass $n = n + n$. Also $\varphi(0) = 0$.

§9.4 Theorem

$\mathrm{id}_{\mathbb{Q}}$ ist der einzige Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$

Beweis (direkt; 1/2).

Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.
Wir zeigen zunächst $\varphi(0) = 0$, $\varphi(1) = 1$ und $\varphi(-1) = -1$.

- $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$. Es gibt nur eine Zahl $n \in \mathbb{Q}$, so dass $n = n + n$. Also $\varphi(0) = 0$.
- $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$. Es gibt nur zwei Zahlen $n \in \mathbb{Q}$, so dass $n = n \cdot n$. Da $\varphi(0) = 0$ und φ injektiv ist, gilt also $\varphi(1) = 1$.

§9.4 Theorem

$\mathrm{id}_{\mathbb{Q}}$ ist der einzige Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$

Beweis (direkt; 1/2).

Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.
Wir zeigen zunächst $\varphi(0) = 0$, $\varphi(1) = 1$ und $\varphi(-1) = -1$.

- $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$. Es gibt nur eine Zahl $n \in \mathbb{Q}$, so dass $n = n + n$. Also $\varphi(0) = 0$.
- $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$. Es gibt nur zwei Zahlen $n \in \mathbb{Q}$, so dass $n = n \cdot n$. Da $\varphi(0) = 0$ und φ injektiv ist, gilt also $\varphi(1) = 1$.
- $\varphi(1) = \varphi((-1) \cdot (-1)) = \varphi(-1) \cdot \varphi(-1)$. Es gibt nur zwei Zahlen $n \in \mathbb{Q}$, so dass $\varphi(1) = 1 = n \cdot n$. Da $\varphi(1) = 1$ und φ injektiv ist, gilt also $\varphi(-1) = -1$.

Beweis (direkt; 2/2).

Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.

- Für jedes $n \in \mathbb{N}$ gilt

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ mal}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ mal}} = \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n$$

Beweis (direkt; 2/2).

Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.

- Für jedes $n \in \mathbb{N}$ gilt

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ mal}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ mal}} = \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n$$

- Analog für $z \in \mathbb{Z}$ mit $z \leq 0$ unter Nutzung von -1

Beweis (direkt; 2/2).

Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.

- Für jedes $n \in \mathbb{N}$ gilt

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ mal}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ mal}} = \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n$$

- Analog für $z \in \mathbb{Z}$ mit $z \leq 0$ unter Nutzung von -1
- Seien $m, n \in \mathbb{Z}$ mit $n > 0$. Z.zg. $\varphi(\frac{m}{n}) = \frac{m}{n}$. Es gilt

$$m = \varphi(m) = \varphi(\frac{m}{n} \cdot n) = \varphi(\frac{m}{n}) \cdot \varphi(n) = \varphi(\frac{m}{n}) \cdot n$$

Diese Gleichung läßt sich eindeutig lösen und wir erhalten $\varphi(\frac{m}{n}) = \frac{m}{n}$.

Beweis (direkt; 2/2).

Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.

- Für jedes $n \in \mathbb{N}$ gilt

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ mal}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ mal}} = \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n$$

- Analog für $z \in \mathbb{Z}$ mit $z \leq 0$ unter Nutzung von -1
- Seien $m, n \in \mathbb{Z}$ mit $n > 0$. Z.zg. $\varphi(\frac{m}{n}) = \frac{m}{n}$. Es gilt

$$m = \varphi(m) = \varphi(\frac{m}{n} \cdot n) = \varphi(\frac{m}{n}) \cdot \varphi(n) = \varphi(\frac{m}{n}) \cdot n$$

  Diese Gleichung läßt sich eindeutig lösen und wir erhalten $\varphi(\frac{m}{n}) = \frac{m}{n}$.

Also gilt $\varphi = \mathrm{id}_{\mathbb{Q}}$. $\square$

Verbände — Charakterisierung

Theorem (§8.16)

Für jeden Verband $(M, \preceq)$ und alle $x, y, z \in M$ gelten

- $x \vee y = y \vee x$ und $x \wedge y = y \wedge x$ Kommutativität
- $x \vee (y \vee z) = (x \vee y) \vee z$ und $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ Assoziativität
- $x \vee (x \wedge y) = x$ und $x \wedge (x \vee y) = x$ Absorption

Notizen:

- für jeden Verband $(M, \preceq)$ (selbst eine algebraische Struktur) existiert also eine algebraische Struktur $(M, \vee, \wedge)$ mit den obigen Beschränkungen an die Funktionen $\vee, \wedge \colon M \times M \to M$

§9.5 Theorem

Sei $(M, \sqcup, \sqcap)$ eine algebraische Struktur des Typs $(0, 2, 0, 0)$, so dass für alle $x, y, z \in M$

- $x \sqcup y = y \sqcup x$ und $x \sqcap y = y \sqcap x$ Kommutativität
- $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$ und $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$ Assoziativität
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$ Absorption

§9.5 Theorem

Sei $(M, \sqcup, \sqcap)$ eine algebraische Struktur des Typs $(0, 2, 0, 0)$, so dass für alle $x, y, z \in M$

- $x \sqcup y = y \sqcup x$ und $x \sqcap y = y \sqcap x$ — Kommutativität
- $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$ und $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$ — Assoziativität
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$ — Absorption

Dann ist $(M, \preceq)$ ein Verband, wobei

$$\preceq \; = \{(x, y) \in M \times M \mid x = x \sqcap y\}$$

Beweis (direkt; 1/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen zunächst die Eigenschaften einer Ordnungsrelation nach:

Beweis (direkt; 1/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen zunächst die Eigenschaften einer Ordnungsrelation nach:

- reflexiv: Für jedes $x \in M$ gilt $x = x \sqcap (x \sqcup (x \sqcap x)) = x \sqcap x$ (Absorption zweifach) also auch $x \preceq x$.

Beweis (direkt; 1/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen zunächst die Eigenschaften einer Ordnungsrelation nach:

- reflexiv: Für jedes $x \in M$ gilt $x = x \sqcap (x \sqcup (x \sqcap x)) = x \sqcap x$ (Absorption zweifach) also auch $x \preceq x$.
- antisymmetrisch: Seien $x \preceq y$ und $y \preceq x$. D.h. $x = x \sqcap y$ und $y = y \sqcap x$. Mit Hilfe der Kommutativität gilt dann

$$x = x \sqcap y = y \sqcap x = y$$

Beweis (direkt; 1/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen zunächst die Eigenschaften einer Ordnungsrelation nach:

- reflexiv: Für jedes $x \in M$ gilt $x = x \sqcap (x \sqcup (x \sqcap x)) = x \sqcap x$ (Absorption zweifach) also auch $x \preceq x$.
- antisymmetrisch: Seien $x \preceq y$ und $y \preceq x$. D.h. $x = x \sqcap y$ und $y = y \sqcap x$. Mit Hilfe der Kommutativität gilt dann
$$x = x \sqcap y = y \sqcap x = y$$
- transitiv: Seien $x \preceq y$ und $y \preceq z$. D.h. $x = x \sqcap y$ und $y = y \sqcap z$. Unter Nutzung der Assoziativität erhalten wir
$$x = x \sqcap y = x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z = x \sqcap z$$
und damit $x \preceq z$.

Beweis (direkt; 2/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen nun noch die Suprema (Infima analog) nach:

- Supremum: Seien $x, y \in M$. Wir behaupten, dass $x \sqcup y$ das Supremum von $\{x, y\}$ ist.

Beweis (direkt; 2/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen nun noch die Suprema (Infima analog) nach:

- Supremum: Seien $x, y \in M$. Wir behaupten, dass $x \sqcup y$ das Supremum von $\{x, y\}$ ist.
  - obere Schranke: Es gilt $x = x \sqcap (x \sqcup y)$ (Absorption) und damit $x \preceq x \sqcup y$. Ebenso gilt $y = y \sqcap (y \sqcup x)$ und damit $y \preceq x \sqcup y$, da $y \sqcup x = x \sqcup y$ (Kommutativität).

Beweis (direkt; 2/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen nun noch die Suprema (Infima analog) nach:

- Supremum: Seien $x, y \in M$. Wir behaupten, dass $x \sqcup y$ das Supremum von $\{x, y\}$ ist.
  - obere Schranke: Es gilt $x = x \sqcap (x \sqcup y)$ (Absorption) und damit $x \preceq x \sqcup y$. Ebenso gilt $y = y \sqcap (y \sqcup x)$ und damit $y \preceq x \sqcup y$, da $y \sqcup x = x \sqcup y$ (Kommutativität).
  - kleinste obere Schranke: Sei $z \in M$, so dass $x \preceq z$ und $y \preceq z$. D.h. $x = x \sqcap z$ und $y = y \sqcap z$. Wir folgern zunächst mit Absorption und Kommutativität $x \sqcup z = (x \sqcap z) \sqcup z = z$ und $y \sqcup z = (y \sqcap z) \sqcup z = z$.

Beweis (direkt; 2/2).

Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen nun noch die Suprema (Infima analog) nach:

- Supremum: Seien $x, y \in M$. Wir behaupten, dass $x \sqcup y$ das Supremum von $\{x,\ y\}$ ist.
  - obere Schranke: Es gilt $x = x \sqcap (x \sqcup y)$ (Absorption) und damit $x \preceq x \sqcup y$. Ebenso gilt $y = y \sqcap (y \sqcup x)$ und damit $y \preceq x \sqcup y$, da $y \sqcup x = x \sqcup y$ (Kommutativität).
  - kleinste obere Schranke: Sei $z \in M$, so dass $x \preceq z$ und $y \preceq z$. D.h. $x = x \sqcap z$ und $y = y \sqcap z$. Wir folgern zunächst mit Absorption und Kommutativität $x \sqcup z = (x \sqcap z) \sqcup z = z$ und $y \sqcup z = (y \sqcap z) \sqcup z = z$. Damit ergibt sich nun

$$\begin{aligned}(x \sqcup y) \sqcap z &= (x \sqcup y) \sqcap (x \sqcup z)\\ &= (x \sqcup y) \sqcap (x \sqcup (y \sqcup z))\\ &= (x \sqcup y) \sqcap ((x \sqcup y) \sqcup z) = (x \sqcup y)\end{aligned}$$

    und damit $(x \sqcup y) \preceq z$. □

Verbände — Charakterisierung

Notizen:

- §8.16 liefert algebraische Struktur à la §9.5 für jeden Verband
- §9.5 liefert Verband für jede derartige algebraische Struktur

$\rightarrow$ starke Korrespondenz (wir verwenden beide Sichtweisen)

Notizen:

- §8.16 liefert algebraische Struktur à la §9.5 für jeden Verband
- §9.5 liefert Verband für jede derartige algebraische Struktur

$\longrightarrow$ starke Korrespondenz (wir verwenden beide Sichtweisen)

§9.6 Korollar

Die Funktion f mit $f((M, \preceq)) = (M, \vee, \wedge)$ für alle Verbände $(M, \preceq)$ ist bijektiv zwischen Verbänden und algebraischen Strukturen à la §9.5.

Notizen:

- §8.16 liefert algebraische Struktur à la §9.5 für jeden Verband
- §9.5 liefert Verband für jede derartige algebraische Struktur

$\rightarrow$ starke Korrespondenz (wir verwenden beide Sichtweisen)

§9.6 Korollar

Die Funktion f mit $f((M, \preceq)) = (M, \vee, \wedge)$ für alle Verbände $(M, \preceq)$ ist bijektiv zwischen Verbänden und algebraischen Strukturen à la §9.5.

Beweis.

Hier ohne Beweis. Es wäre noch zu zeigen, dass die Umwandlungen aus §8.16 und §9.5 unter Komposition die Identitäten liefern. $\square$

§9.7 Definition (Unterstruktur)

Seien $\mathcal{U} = (U, \langle R_1, \dots, R_k\rangle, \langle f_1, \dots, f_\ell\rangle, \langle g_1, \dots, g_m\rangle, \langle c_1, \dots, c_n\rangle)$ und $\mathcal{V} = (V, \langle R'_1, \dots, R'_k\rangle, \langle f'_1, \dots, f'_\ell\rangle, \langle g'_1, \dots, g'_m\rangle, \langle c'_1, \dots, c'_n\rangle)$ zwei algebraische Strukturen gleichen Typs.
Dann ist $\mathcal{V}$ eine Unterstruktur von $\mathcal{U}$, gdw.

- $V \subseteq U$

§9.7 Definition (Unterstruktur)

Seien $\mathcal{U} = (U, \langle R_1, \ldots, R_k\rangle, \langle f_1, \ldots, f_\ell\rangle, \langle g_1, \ldots, g_m\rangle, \langle c_1, \ldots, c_n\rangle)$ und $\mathcal{V} = (V, \langle R'_1, \ldots, R'_k\rangle, \langle f'_1, \ldots, f'_\ell\rangle, \langle g'_1, \ldots, g'_m\rangle, \langle c'_1, \ldots, c'_n\rangle)$ zwei algebraische Strukturen gleichen Typs.
Dann ist $\mathcal{V}$ eine Unterstruktur von $\mathcal{U}$, gdw.

- $V \subseteq U$
- für alle $1 \leq i \leq k$ und $v_1, v_2 \in V$ gilt $(R'_i = R_i \cap (V \times V))$

$$(v_1, v_2) \in R'_i \qquad \text{gdw.} \qquad (v_1, v_2) \in R_i$$

§9.7 Definition (Unterstruktur)

Seien $\mathcal{U} = (U, \langle R_1, \dots, R_k\rangle, \langle f_1, \dots, f_\ell\rangle, \langle g_1, \dots, g_m\rangle, \langle c_1, \dots, c_n\rangle)$ und $\mathcal{V} = (V, \langle R'_1, \dots, R'_k\rangle, \langle f'_1, \dots, f'_\ell\rangle, \langle g'_1, \dots, g'_m\rangle, \langle c'_1, \dots, c'_n\rangle)$ zwei algebraische Strukturen gleichen Typs.
Dann ist $\mathcal{V}$ eine Unterstruktur von $\mathcal{U}$, gdw.

- $V \subseteq U$
- für alle $1 \leq i \leq k$ und $v_1, v_2 \in V$ gilt $(R'_i = R_i \cap (V \times V))$

$$(v_1, v_2) \in R'_i \qquad \text{gdw.} \qquad (v_1, v_2) \in R_i$$

- $f'_i(v_1, v_2) = f_i(v_1, v_2)$ für alle $1 \leq i \leq \ell$ und $v_1, v_2 \in V$
- $g'_i(v) = g_i(v)$ für alle $1 \leq i \leq m$ und $v \in V$, und
- $c'_i = c_i$ für alle $1 \leq i \leq n$.

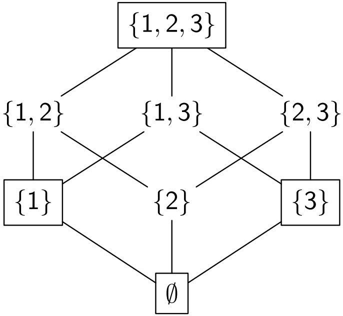
Notizen:

- Relationen, Funktionen und Konstanten der Oberstruktur übertragen sich eingeschränkt auf V auf die Unterstruktur
- wir sagen daher $V \subseteq U$ bildet eine Unterstruktur, falls

$$(V, \langle R'_1, \ldots, R'_k \rangle, \langle f'_1, \ldots, f'_\ell \rangle, \langle g'_1, \ldots, g'_m \rangle, \langle c_1, \ldots, c_n \rangle)$$

  eine algebraische Struktur ist, wobei
  - $R'_i = R_i \cap V^2$ für alle $1 \leq i \leq k$
  - $f'_i = f_i \cap V^3$ für alle $1 \leq i \leq \ell$
  - $g'_i = g_i \cap V^2$ für alle $1 \leq i \leq m$

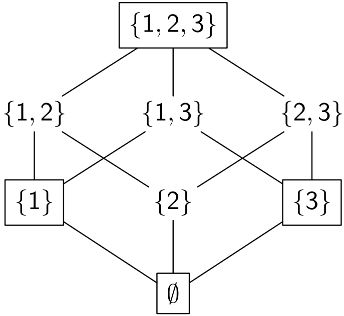
Beispiel: Wir betrachten den Verband $\mathcal{U} = (\mathcal{P}(\{1,\ 2,\ 3\}, \cup, \cap)$



und die Teilmenge $V = \{\emptyset,\ \{1\},\ \{3\},\ \{1,\ 2,\ 3\}\}$.

Verbände — Charakterisierung

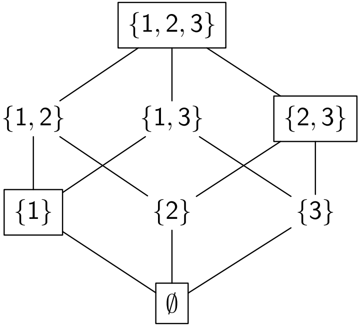
Beispiel: Wir betrachten den Verband $\mathcal{U} = (\mathcal{P}(\{1, 2, 3\}, \cup, \cap)$



und die Teilmenge $V = \{\emptyset, \{1\}, \{3\}, \{1, 2, 3\}\}$.

V bildet keine Unterstruktur von $\mathcal{U}$

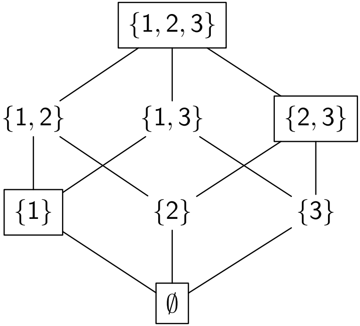
Beispiel: Wir betrachten den Verband $\mathcal{U} = (\mathcal{P}(\{1, 2, 3\}, \cup, \cap)$



und die Teilmenge $V' = \{\emptyset, \{1\}, \{2, 3\}, \{1, 2, 3\}\}$.

Verbände — Charakterisierung

Beispiel: Wir betrachten den Verband $\mathcal{U} = (\mathcal{P}(\{1,\ 2,\ 3\}, \cup, \cap)$

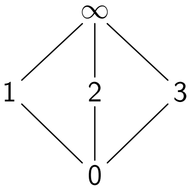


und die Teilmenge $V' = \{\emptyset,\ \{1\},\ \{2,\ 3\},\ \{1,\ 2,\ 3\}\}$.

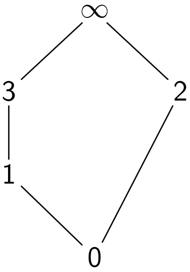
V' bildet <u>eine</u> Unterstruktur von $\mathcal{U}$

§9.8 Theorem (Charakterisierung Distributivität)

Sei $\mathcal{V} = (V, \vee, \wedge)$ eine algebraische Struktur mit den Eigenschaften aus §9.5 (d.h. ein Verband $(V, \preceq)$ mit Supremum $\vee$ und Infimum $\wedge$). Dann ist $\mathcal{V}$ distributiv gdw. keine Unterstruktur von $\mathcal{V}$ isomorph zu M_3 oder N_5 ist.



M_3



N_5

Beweisskizze (1/3).

Sei $U \subseteq V$ eine Teilmenge, die eine Unterstruktur $(U, \vee', \wedge')$ bildet, die isomorph zu $M_3 = (\{0, 1, 2, 3, \infty\}, \vee_3, \wedge_3)$ ist.
Sei $\varphi\colon U \to \{0, 1, 2, 3, \infty\}$ ein Isomorphismus.
Also existieren $u_1, u_2, u_3 \in U$ mit

$$\varphi(u_1) = 1 \qquad \varphi(u_2) = 2 \qquad \text{und} \qquad \varphi(u_3) = 3$$

Beweisskizze (1/3).

Sei $U \subseteq V$ eine Teilmenge, die eine Unterstruktur $(U, \vee', \wedge')$ bildet, die isomorph zu $M_3 = (\{0, 1, 2, 3, \infty\}, \vee_3, \wedge_3)$ ist.
Sei $\varphi\colon U \to \{0, 1, 2, 3, \infty\}$ ein Isomorphismus.
Also existieren $u_1, u_2, u_3 \in U$ mit

$$\varphi(u_1) = 1 \qquad \varphi(u_2) = 2 \qquad \text{und} \qquad \varphi(u_3) = 3$$

Dann gilt

$$\begin{aligned}
\varphi\big(u_1 \vee (u_2 \wedge u_3)\big) &= \varphi\big(u_1 \vee' (u_2 \wedge' u_3)\big) \\
&= \varphi(u_1) \vee_3 (\varphi(u_2) \wedge_3 \varphi(u_3)) = 1 \vee_3 (2 \wedge_3 3) = 1 \\
\varphi\big((u_1 \vee u_2) \wedge (u_1 \vee u_3)\big) &= \varphi\big((u_1 \vee' u_2) \wedge' (u_1 \vee' u_3)\big) \\
&= (\varphi(u_1) \vee_3 \varphi(u_2)) \wedge_3 (\varphi(u_1) \vee_3 \varphi(u_3)) \\
&= (1 \vee_3 2) \wedge_3 (1 \vee_3 3) = \infty
\end{aligned}$$

Beweisskizze (1/3).

Sei $U \subseteq V$ eine Teilmenge, die eine Unterstruktur $(U, \vee', \wedge')$ bildet, die isomorph zu $M_3 = (\{0, 1, 2, 3, \infty\}, \vee_3, \wedge_3)$ ist.
Sei $\varphi \colon U \to \{0, 1, 2, 3, \infty\}$ ein Isomorphismus.
Also existieren $u_1, u_2, u_3 \in U$ mit

$$\varphi(u_1) = 1 \qquad \varphi(u_2) = 2 \qquad \text{und} \qquad \varphi(u_3) = 3$$

Dann gilt

$$\begin{aligned}
\varphi\big(u_1 \vee (u_2 \wedge u_3)\big) &= \varphi\big(u_1 \vee' (u_2 \wedge' u_3)\big) \\
&= \varphi(u_1) \vee_3 (\varphi(u_2) \wedge_3 \varphi(u_3)) = 1 \vee_3 (2 \wedge_3 3) = 1 \\
\varphi\big((u_1 \vee u_2) \wedge (u_1 \vee u_3)\big) &= \varphi\big((u_1 \vee' u_2) \wedge' (u_1 \vee' u_3)\big) \\
&= (\varphi(u_1) \vee_3 \varphi(u_2)) \wedge_3 (\varphi(u_1) \vee_3 \varphi(u_3)) \\
&= (1 \vee_3 2) \wedge_3 (1 \vee_3 3) = \infty
\end{aligned}$$

Da $1 \neq \infty$, gilt auch $\varphi^{-1}(1) \neq \varphi^{-1}(\infty)$, womit $\mathcal{V}$ nicht distributiv ist.

Beweisskizze (2/3).

(isomorph zu N_5 analog) Umgekehrt sei $\mathcal{V}$ nicht distributiv.

Beweisskizze (2/3).

(isomorph zu N_5 analog) Umgekehrt sei $\mathcal{V}$ nicht distributiv.

Fall 1: Es existieren $a, b, c \in V$ mit $a \preceq b$ und

$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c) = b \wedge (a \vee c)$$

Verbände — Charakterisierung

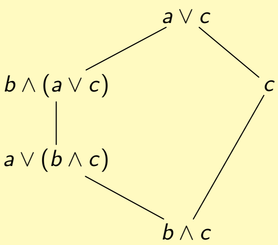
Beweisskizze (2/3).

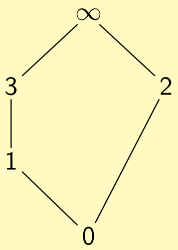
(isomorph zu N_5 analog) Umgekehrt sei $\mathcal{V}$ nicht distributiv.

Fall 1: Es existieren $a, b, c \in V$ mit $a \preceq b$ und

$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c) = b \wedge (a \vee c)$$

Es folgt, dass das linke Hasse-Diagramm





eine Unterstruktur von $\mathcal{V}$ ist (viel Nachrechnen). Der Isomorphismus zu N_5 (rechtes Hasse-Diagramm) ist offensichtlich.

Beispiele vom Nachrechnen:

- partielle Ordnung: z.zg. $a \vee (b \wedge c) \preceq b \wedge (a \vee c)$
  Wir zeigen dazu $a \vee (b \wedge c) \preceq b$ und $a \vee (b \wedge c) \preceq a \vee c$.

Beispiele vom Nachrechnen:

- partielle Ordnung: z.zg. $a \vee (b \wedge c) \preceq b \wedge (a \vee c)$
  Wir zeigen dazu $a \vee (b \wedge c) \preceq b$ und $a \vee (b \wedge c) \preceq a \vee c$. Dies wiederum zeigen wir durch $a \preceq b$ und $b \wedge c \preceq b$ sowie $a \preceq a \vee c$ und $b \wedge c \preceq c \preceq a \vee c$.

Beispiele vom Nachrechnen:

- partielle Ordnung: z.zg. $a \vee (b \wedge c) \preceq b \wedge (a \vee c)$
  Wir zeigen dazu $a \vee (b \wedge c) \preceq b$ und $a \vee (b \wedge c) \preceq a \vee c$. Dies wiederum zeigen wir durch $a \preceq b$ und $b \wedge c \preceq b$ sowie $a \preceq a \vee c$ und $b \wedge c \preceq c \preceq a \vee c$.

- Suprema und Infima: z.zg. $(b \wedge (a \vee c)) \vee c = a \vee c$. Wir zeigen dazu $(b \wedge (a \vee c)) \vee c \preceq a \vee c \vee c = a \vee c$ und $a \preceq b \wedge (a \vee c)$.

Beispiele vom Nachrechnen:

- partielle Ordnung: z.zg. $a \vee (b \wedge c) \preceq b \wedge (a \vee c)$
  Wir zeigen dazu $a \vee (b \wedge c) \preceq b$ und $a \vee (b \wedge c) \preceq a \vee c$. Dies wiederum zeigen wir durch $a \preceq b$ und $b \wedge c \preceq b$ sowie $a \preceq a \vee c$ und $b \wedge c \preceq c \preceq a \vee c$.

- Suprema und Infima: z.zg. $(b \wedge (a \vee c)) \vee c = a \vee c$. Wir zeigen dazu $(b \wedge (a \vee c)) \vee c \preceq a \vee c \vee c = a \vee c$ und $a \preceq b \wedge (a \vee c)$. Dies wiederum zeigen wir durch $a \preceq b$ und $a \preceq a \vee c$.

Beispiele vom Nachrechnen:

- partielle Ordnung: z.zg. $a \vee (b \wedge c) \preceq b \wedge (a \vee c)$
  Wir zeigen dazu $a \vee (b \wedge c) \preceq b$ und $a \vee (b \wedge c) \preceq a \vee c$. Dies wiederum zeigen wir durch $a \preceq b$ und $b \wedge c \preceq b$ sowie $a \preceq a \vee c$ und $b \wedge c \preceq c \preceq a \vee c$.

- Suprema und Infima: z.zg. $(b \wedge (a \vee c)) \vee c = a \vee c$. Wir zeigen dazu $(b \wedge (a \vee c)) \vee c \preceq a \vee c \vee c = a \vee c$ und $a \preceq b \wedge (a \vee c)$. Dies wiederum zeigen wir durch $a \preceq b$ und $a \preceq a \vee c$.

- Ungleichheit: z.zg. $a \vee (b \wedge c) \neq b \wedge c$. Sei $a \vee (b \wedge c) = b \wedge c$. Also $a \preceq b \wedge c \preceq c$, womit

$$a \vee (b \wedge c) = b \wedge c = b \wedge (a \vee c)$$

  im Widerspruch zur Annahme.

Beweisskizze (3/3).

Fall 2: Für alle $x, y, z \in V$ mit $x \preceq y$ gilt $x \vee (y \wedge z) = y \wedge (x \vee z)$.

Beweisskizze (3/3).

Fall 2: Für alle $x, y, z \in V$ mit $x \preceq y$ gilt $x \vee (y \wedge z) = y \wedge (x \vee z)$. Trotzdem existieren $a, b, c \in V$, so dass

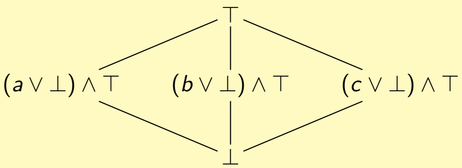
$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$$

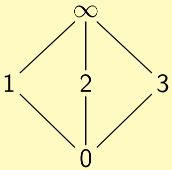
Beweisskizze (3/3).

Fall 2: Für alle $x, y, z \in V$ mit $x \preceq y$ gilt $x \vee (y \wedge z) = y \wedge (x \vee z)$. Trotzdem existieren $a, b, c \in V$, so dass

$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$$

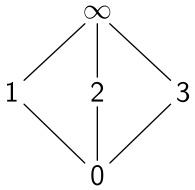
Es folgt, dass das linke Hasse-Diagramm mit
$\bot = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c)$ und $\top = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$





eine Unterstruktur von $\mathcal{V}$ ist (noch mehr Nachrechnen). Der Isomorphismus zu M_3 (rechtes Hasse-Diagramm) ist offensichtlich. □

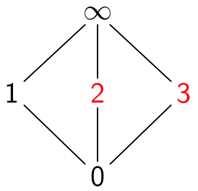
Nicht-distributiver Verband M_3:



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge \infty = \infty$

Verbände — Charakterisierung

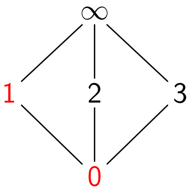
<u>Nicht-distributiver Verband M_3:</u>



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge \infty = \infty$

Verbände — Charakterisierung

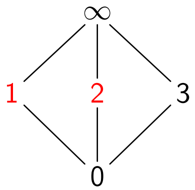
Nicht-distributiver Verband M_3:



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge \infty = \infty$

Verbände — Charakterisierung

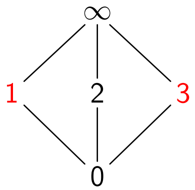
<u>Nicht-distributiver Verband M_3:</u>



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge \infty = \infty$

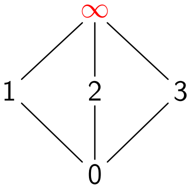
Verbände — Charakterisierung

<u>Nicht-distributiver Verband M_3:</u>



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge \infty = \infty$

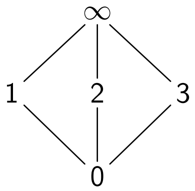
Nicht-distributiver Verband M_3:



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge \infty = \infty$

Verbände — Charakterisierung

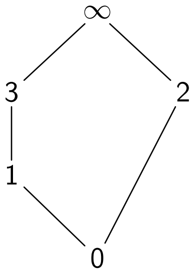
Nicht-distributiver Verband M_3:



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge \infty = \infty$

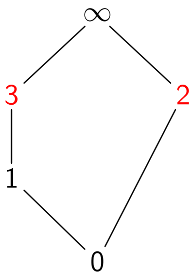
Verbände — Charakterisierung

Nicht-distributiver Verband N_5:



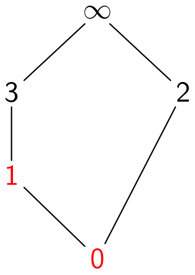
denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge 3 = 3$

Nicht-distributiver Verband N_5:



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge 3 = 3$

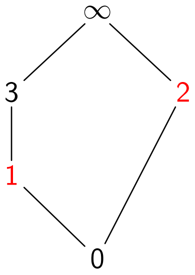
Nicht-distributiver Verband N_5:



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge 3 = 3$

Verbände — Charakterisierung

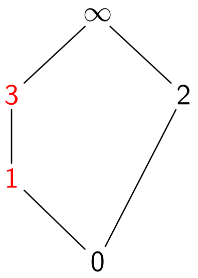
Nicht-distributiver Verband N_5:



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge 3 = 3$

Verbände — Charakterisierung

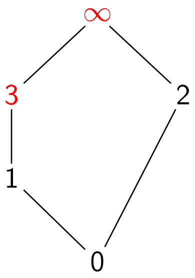
<u>Nicht-distributiver Verband N_5:</u>



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge 3 = 3$

Verbände — Charakterisierung

<u>Nicht-distributiver Verband N_5:</u>



denn $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$
aber $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge 3 = 3$

§9.9 Definition (Komplement und Boolesche Algebra)

Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\bot$ (von M) und größtem Element $\top$ (von M).

- Sei $x \in M$. Ein Element $y \in M$ heißt Komplement von x gdw. $x \wedge y = \bot$ und $x \vee y = \top$.

§9.9 Definition (Komplement und Boolesche Algebra)

Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\bot$ (von M) und größtem Element $\top$ (von M).

- Sei $x \in M$. Ein Element $y \in M$ heißt Komplement von x gdw. $x \wedge y = \bot$ und $x \vee y = \top$.
- Der Verband $(M, \preceq)$ heißt komplementiert gdw. für jedes $x \in M$ ein Komplement $y \in M$ von x existiert.

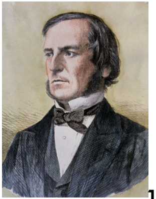
§9.9 Definition (Komplement und Boolesche Algebra)

Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\bot$ (von M) und größtem Element $\top$ (von M).

- Sei $x \in M$. Ein Element $y \in M$ heißt Komplement von x gdw. $x \wedge y = \bot$ und $x \vee y = \top$.
- Der Verband $(M, \preceq)$ heißt komplementiert gdw. für jedes $x \in M$ ein Komplement $y \in M$ von x existiert.
- Der Verband $(M, \preceq)$ heißt Boolesche Algebra gdw. er komplementiert und distributiv ist und $\bot \neq \top$ gilt.

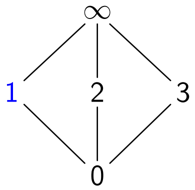
George Boole (* 1815; † 1864)

- engl. Philosoph und Mathematiker
- symbolische Aussagenlogik
- nur Grundschulausbildung



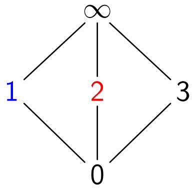
Notizen:

- Komplemente sind in allgemeinen Verbänden nicht eindeutig



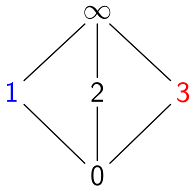
Notizen:

- Komplemente sind in allgemeinen Verbänden nicht eindeutig
- 2 ist Komplement von 1



Notizen:

- Komplemente sind in allgemeinen Verbänden nicht eindeutig
- 2 ist Komplement von 1
- 3 ist auch Komplement von 1



§9.10 Theorem

Sei $(M, \preceq)$ ein distributiver Verband mit kleinstem Element $\bot$ und größtem Element $\top$. Für jedes $x \in M$ existiert höchstens ein Komplement von x.

§9.10 Theorem

Sei $(M, \preceq)$ ein distributiver Verband mit kleinstem Element $\bot$ und größtem Element $\top$. Für jedes $x \in M$ existiert höchstens ein Komplement von x.

Beweis (direkt).

Sei $x \in M$ und seien $y, z \in M$ Komplemente von x.

- Wir zeigen $y = y \wedge z$

$$\begin{aligned} y &= \top \wedge y = (x \vee z) \wedge y = (x \wedge y) \vee (z \wedge y) \\ &= \bot \vee (z \wedge y) = y \wedge z \end{aligned}$$

§9.10 Theorem

Sei $(M, \preceq)$ ein distributiver Verband mit kleinstem Element $\bot$ und größtem Element $\top$. Für jedes $x \in M$ existiert höchstens ein Komplement von x.

Beweis (direkt).

Sei $x \in M$ und seien $y, z \in M$ Komplemente von x.

- Wir zeigen $y = y \wedge z$

$$\begin{aligned} y &= \top \wedge y = (x \vee z) \wedge y = (x \wedge y) \vee (z \wedge y) \\ &= \bot \vee (z \wedge y) = y \wedge z \end{aligned}$$

- Wir zeigen $z = y \wedge z$

$$\begin{aligned} z &= \top \wedge z = (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) \\ &= \bot \vee (y \wedge z) = y \wedge z \end{aligned}$$

§9.10 Theorem

Sei $(M, \preceq)$ ein distributiver Verband mit kleinstem Element $\bot$ und größtem Element $\top$. Für jedes $x \in M$ existiert höchstens ein Komplement von x.

Beweis (direkt).

Sei $x \in M$ und seien $y, z \in M$ Komplemente von x.

- Wir zeigen $y = y \wedge z$

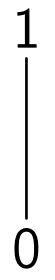
$$\begin{aligned} y &= \top \wedge y = (x \vee z) \wedge y = (x \wedge y) \vee (z \wedge y) \\ &= \bot \vee (z \wedge y) = y \wedge z \end{aligned}$$

- Wir zeigen $z = y \wedge z$

$$\begin{aligned} z &= \top \wedge z = (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) \\ &= \bot \vee (y \wedge z) = y \wedge z \end{aligned}$$

Also $y = y \wedge z = z$ □

Algebraische Strukturen — Boolesche Algebren



Beispiel

$(\{0, 1\}, \{(0,0), (0,1), (1,1)\})$ Verband der Wahrheitswerte mit

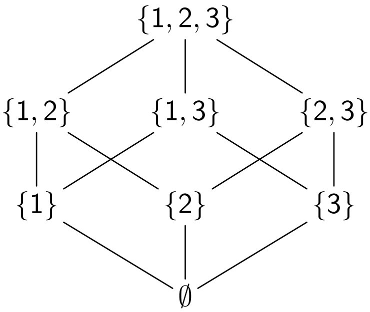
- kleinstem Element 0 und größtem Element 1
- Supremum $\vee$ und Infimum $\wedge$

Ist distributiv, da total geordnet.

Für jedes $b \in \{0, 1\}$ gilt $b \wedge \underbrace{(1 - b)}_{\neg b} = 0$ und $b \vee \underbrace{(1 - b)}_{\neg b} = 1$.

Also komplementiert und damit Boolesche Algebra

Algebraische Strukturen — Boolesche Algebren



weiteres Beispiel

- für jede Menge M ist $(\mathcal{P}(M), \subseteq)$ ein distributiver Verband
  - mit kleinstem Element $\emptyset$ und größtem Element M
  - Supremum $\cup$ und Infimum $\cap$
- $M' \cap (M')^c = \emptyset$ und $M' \cup (M')^c = M$ für jedes $M' \in \mathcal{P}(M)$

$\rightarrow$ komplementiert und sogar Boolesche Algebra falls $M \neq \emptyset$

noch ein Beispiel

- sei $M \neq \emptyset$ eine unendliche Menge und

$$\mathcal{M} = \{X \in \mathcal{P}(M) \mid X \text{ endlich}\} \cup \{X \in \mathcal{P}(M) \mid M \setminus X \text{ endlich}\}$$

- distributiver, unvollständiger Verband
  - mit kleinstem Element $\emptyset$ und größtem Element M
  - Supremum $\cup$ und Infimum $\cap$
- $M' \cap (M')^c = \emptyset$ und $M' \cup (M')^c = M$ für jedes $M' \in \mathcal{P}(M)$

$\rightarrow$ komplementiert und damit Boolesche Algebra

§9.11 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit kleinstem Element $\perp$ und größtem Element $\top$ und sei $\cdot^c \colon M \to M$, so dass für alle $x \in M$ das Element x^c das Komplement von x ist. Dann gelten

1. $(x^c)^c = x$ für alle $x \in M$ und
2. $(x \wedge y)^c = x^c \vee y^c$ und $(x \vee y)^c = x^c \wedge y^c$ für alle $x, y \in M$

§9.11 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit kleinstem Element $\bot$ und größtem Element $\top$ und sei $\cdot^c \colon M \to M$, so dass für alle $x \in M$ das Element x^c das Komplement von x ist. Dann gelten

1. $(x^c)^c = x$ für alle $x \in M$ und
2. $(x \wedge y)^c = x^c \vee y^c$ und $(x \vee y)^c = x^c \wedge y^c$ für alle $x, y \in M$

Beweis (direkt; 1/2).

1. Per Definition ist $(x^c)^c$ das Komplement von x^c. Aufgrund der Kommutativität von $\wedge$ und $\vee$ (§8.16) ist x auch Komplement von x^c. Da das Komplement eindeutig ist (§9.10), gilt $x = (x^c)^c$.

Beweis (direkt; 2/2).

2. Wir zeigen, dass $(x \vee y) \wedge (x^c \wedge y^c) = \bot$ und $(x \vee y) \vee (x^c \wedge y^c) = \top$. Aufgrund der Eindeutigkeit des Komplements ist dann $(x \vee y)^c = x^c \wedge y^c$.

Beweis (direkt; 2/2).

2. Wir zeigen, dass $(x \vee y) \wedge (x^c \wedge y^c) = \perp$ und $(x \vee y) \vee (x^c \wedge y^c) = \top$. Aufgrund der Eindeutigkeit des Komplements ist dann $(x \vee y)^c = x^c \wedge y^c$.

$$
\begin{aligned}
&(x \vee y) \wedge (x^c \wedge y^c) \\
&= (x \wedge x^c \wedge y^c) \vee (y \wedge x^c \wedge y^c) \\
&= (\perp \wedge y^c) \vee (\perp \wedge x^c) = \perp \vee \perp = \perp
\end{aligned}
$$

Beweis (direkt; 2/2).

2. Wir zeigen, dass $(x \vee y) \wedge (x^c \wedge y^c) = \bot$ und $(x \vee y) \vee (x^c \wedge y^c) = \top$. Aufgrund der Eindeutigkeit des Komplements ist dann $(x \vee y)^c = x^c \wedge y^c$.

$$\begin{aligned} & (x \vee y) \wedge (x^c \wedge y^c) \\ = {} & (x \wedge x^c \wedge y^c) \vee (y \wedge x^c \wedge y^c) \\ = {} & (\bot \wedge y^c) \vee (\bot \wedge x^c) = \bot \vee \bot = \bot \end{aligned}$$

Analog rechnen wir die zweite Gleichheit

$$\begin{aligned} & (x \vee y) \vee (x^c \wedge y^c) \\ = {} & (x \vee y \vee x^c) \wedge (x \vee y \vee y^c) \\ = {} & (\top \vee y) \vee (\top \vee x) = \top \vee \top = \top \end{aligned}$$

Beweis (direkt; 2/2).

2. Wir zeigen, dass $(x \vee y) \wedge (x^c \wedge y^c) = \bot$ und $(x \vee y) \vee (x^c \wedge y^c) = \top$. Aufgrund der Eindeutigkeit des Komplements ist dann $(x \vee y)^c = x^c \wedge y^c$.

$$\begin{aligned} & (x \vee y) \wedge (x^c \wedge y^c) \\ = & (x \wedge x^c \wedge y^c) \vee (y \wedge x^c \wedge y^c) \\ = & (\bot \wedge y^c) \vee (\bot \wedge x^c) = \bot \vee \bot = \bot \end{aligned}$$

Analog rechnen wir die zweite Gleichheit

$$\begin{aligned} & (x \vee y) \vee (x^c \wedge y^c) \\ = & (x \vee y \vee x^c) \wedge (x \vee y \vee y^c) \\ = & (\top \vee y) \vee (\top \vee x) = \top \vee \top = \top \end{aligned}$$

Ebenso für das zweite deMorgan-Gesetz. $\square$

Notizen:

- wir nutzen m^c für das Komplement von m in Booleschen Algebren

Notizen:

- wir nutzen m^c für das Komplement von m in Booleschen Algebren

§9.12 Theorem (vgl. §9.5)

Sei $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass für alle $x, y \in M$

- $\sqcap$ und $\sqcup$ kommutativ, distributiv und assoziativ sind,
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$, Absorption
- und $x \sqcap x^* = \bot$ und $x \sqcup x^* = \top$. Komplemente

Notizen:

- wir nutzen m^c für das Komplement von m in Booleschen Algebren

§9.12 Theorem (vgl. §9.5)

Sei $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass für alle $x, y \in M$

- $\sqcap$ und $\sqcup$ kommutativ, distributiv und assoziativ sind,
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$, — Absorption
- und $x \sqcap x^* = \bot$ und $x \sqcup x^* = \top$. — Komplemente

Dann ist $(M, \preceq)$ mit $x \preceq y$ gdw. $x = x \sqcap y$ eine Boolesche Algebra.

Notizen:

- wir nutzen m^c für das Komplement von m in Booleschen Algebren

§9.12 Theorem (vgl. §9.5)

Sei $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass für alle $x, y \in M$

- $\sqcap$ und $\sqcup$ kommutativ, distributiv und assoziativ sind,
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$, Absorption
- und $x \sqcap x^* = \bot$ und $x \sqcup x^* = \top$. Komplemente

Dann ist $(M, \preceq)$ mit $x \preceq y$ gdw. $x = x \sqcap y$ eine Boolesche Algebra.

Beweis (direkt).

Unter Nutzung von §9.5 leicht nachzurechnen. □

Zusammenfassung

- Algebraische Strukturen
- Isomorphismen und Unterstrukturen
- Charakterisierung Distributivität
- Boolesche Algebren

Fünfte Aufgabenserie bereits im AlmaWeb verfügbar