3. Algebra und Begriffsverbände

Algebraische Strukturen

Def.: Eine n-stellige (n-äre) [algebraische] *Operation* [auch: *Verknüpfung*] auf einer Menge A ist eine Abbildung $f: A^n \to A$.

Der Spezialfall $n = 0$: $A^0 = \{ \emptyset \}$, $f() = f(\emptyset) = \text{const.}$

Zweistelliges f wird oft in Infixnotation geschrieben:
$f(a, b) = a \circ b$ oder $= a \cdot b$ oder $= a + b$.

Def.: $\mathbf{A} = (A, F) = (A, (f_i)_{i\in I})$ heißt (universelle) *Algebra*, wenn A eine beliebige Menge ist und $F = (f_i)_{i\in I}$ eine Familie n_i-stelliger Operationen f_i auf A, d.h. jedem f_i ist $a(f_i) = n_i \in \mathrm{N}_0$ zugeordnet und $f_i: A^{n_i} \to A$.

A heißt die *Trägermenge* von $\mathbf{A}$,
$T = (n_i)_{i\in I}$ heißt *Typ* von $\mathbf{A}$,
$|A|$ (Kardinalzahl) heißt die *Ordnung* von $\mathbf{A}$.

Beispiele:
(a) Jede Algebra vom Typ (2) heißt *Gruppoid* (auch: *Magma*).

(b) Eine (2)-Algebra $(A, \circ)$ heißt *Halbgruppe*, wenn für alle $a, b, c \in A$ gilt: $(a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativgesetz).

(c) Eine (2, 0)-Algebra (A, °, e) heißt *Gruppoid mit neutralem Element*, wenn für alle $a \in A$ gilt:
$a \circ e = e \circ a = a$.

(d) Eine Halbgruppe mit neutralem Element heißt *Monoid*.

(e) Eine *Quasigruppe* ist ein Gruppoid, für das gilt:
$\forall a \in A\ \forall b \in A\ \exists x \in A\ \exists y \in A : a \circ x = b\ \wedge\ y \circ a = b$.

(f) Eine *Loop* ist eine Quasigruppe mit neutralem Element.

Satz: Sei (A, °) Halbgruppe. Dann sind folgende Aussagen gleichwertig:
(a) A ist Quasigruppe.
(b) (A, °) hat ein linksneutrales Element e_l, d.h.:
$\forall a \in A : e_l \circ a = a$,
und es gilt:
$\forall a \in A\ \exists a' \in A : a' \circ a = e_l$.
(c) (A, °) hat ein neutrales Element e, und zu jedem $a \in A$ existiert ein Inverses a^{-1}:
$a \circ a^{-1} = e\ \wedge\ a^{-1} \circ a = e$.

Beweis: siehe Weinert (1984).

Def.: Eine solche Halbgruppe heißt *Gruppe*.

Darstellung eines endlichen Gruppoids durch eine Verknüpfungstafel (Strukturtafel):
linke Spalte: 1. Operand a, oberste Zeile: 2. Operand b, zugehöriger Eintrag im Inneren: a ° b.

Beispiel:

°	a	b	c	d
a	a	b	c	d
b	b	c	c	c
c	c	d	a	b
d	d	b	b	a

(Gruppoid mit neutralem Element)

Beispiel einer Gruppe:

°	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(die Kleinsche Vierergruppe)

Beispiel einer Loop, die keine Gruppe ist:

°	a	b	c	d	e
a	a	b	c	d	e
b	b	d	e	a	c
c	c	a	b	e	d
d	d	e	a	c	b
e	e	c	d	b	a

Def.: Sei (A, F) eine Algebra, $F = (f_i)_{i \in I}$. Eine Algebra (B, F') mit $F' = (f_i')_{i \in I}$ (vom selben Typ wie (A, F)) heißt <u>Unteralgebra</u> von (A, F) genau dann, wenn gilt:

(1) $B \subseteq A$

(2) $\forall i \in I: \; f_i' = f_i \big|_{B^{n_i}}$ (= Einschränkung von f_i auf B^{n_i})

(3) $\forall i \in I: \; \forall b_1, b_2, \ldots, b_{n_i} \in B \; : \; f_i(b_1, b_2, \ldots, b_{n_i}) \in B$

Mit anderen Worten: Genau die $B \subseteq A$, die bzgl. aller f_i abgeschlossen sind, sind Trägermengen von Unteralgebren.

Beachte: Falls f_i mit $a(f_i) = n_i = 0$ auftreten, besagt (3): $f_i' = f_i \in B$, d.h. die durch 0-stellige Operationen in A ausgezeichneten Konstanten von (A, F) liegen in B. Insbesondere gilt dann $B \neq \emptyset$.

Andernfalls wird $B = \emptyset$ als Trägermenge einer Unteralgebra zugelassen.

Beispiele: $(2\mathbb{N}, \cdot)$ und $(\emptyset, \cdot)$ sind Unteralgebren (Unterhalbgruppen) der Halbgruppe $(\mathbb{N}, \cdot)$

$(\{+1; -1\}, \cdot)$ ist eine Untergruppe von $(\mathbb{Q} \setminus \{0\}, \cdot)$

Satz: Sei $M \neq \emptyset$, $\mathrm{T}_M := \{ f \mid f : M \to M \text{ Abbildung} \}$.

(a) $(\mathrm{T}_M, \circ, id)$ mit $\circ$ als Komposition (Nacheinanderausführung) von Abbildungen ist ein Monoid, das *Transformationsmonoid* von *M*. $(\mathrm{T}_M, \circ)$ heißt auch *symmetrische Halbgruppe*.

(b) Für $|M| = n < \infty$ gilt $|\mathrm{T}_M| = n^n$, und für $n \geq 2$ ist $(\mathrm{T}_M, \circ)$ nichtkommutativ.

(c) Genau die bijektiven Abbildungen sind die in $(\mathrm{T}_M, \circ, id)$ invertierbaren Elemente. Sie bilden eine Untergruppe $(\mathrm{S}_M, \circ, id, (\cdot)^{-1})$, die *symmetrische Gruppe* von *M*. (Für $|M| = n$ auch: S_n). Die Elemente sind sämtliche Permutationen von *M*. Für $|M| = n < \infty$ gilt $|\mathrm{S}_M| = n!$.

Satz: Der Schnitt $\bigcap_{j \in J} B_j$ eines beliebigen Systems $(B_j)_{j \in J}$ von Unteralgebren von (A, F) ist stets wieder eine Unteralgebra von (A, F).

Def.: Sei (A, F) Algebra, $X \subseteq A$. Dann ist $(\langle X \rangle, F)$ mit $\langle X \rangle = \bigcap_{\substack{B \text{ Unteralgebra von } A \\ X \subseteq B}} B$ die kleinste Unteralgebra von (A, F), die X enthält. Sie heißt die <u>von X erzeugte</u> Unteralgebra.

X heißt <u>Erzeugendensystem</u> einer Algebra (C, F), falls $\langle X \rangle = C$.

Bemerkung: Die Funktion $\langle\cdot\rangle : X \mapsto \langle X\rangle$ erfüllt $\forall X, Y \subseteq A$:

(1) $X \subseteq Y \Rightarrow \langle X\rangle \subseteq \langle Y\rangle$ (Monotonie)

(2) $X \subseteq \langle X\rangle$ (Extensivität)

(3) $\langle\langle X\rangle\rangle = \langle X\rangle$ (Idempotenz)

Eine solche Funktion nennt man einen <u>Hüllenoperator</u>.

Schrittweise Erzeugung von $\langle X\rangle$:

Der <u>Baire-Operator</u> auf der Potenzmenge von A wird def. durch

$$B(Y) = Y \cup \{ f_i(b_1, \dots, b_{n_i}) \mid i \in I,\ n_i = a(f_i),\ b_1, \dots, b_{n_i} \in Y \}.$$

Dann gilt $\langle X\rangle = \bigcup_{n\in\mathbb{N}} B^n(X)$.

(Beweis: Weinert 1983.)

Satz:

Es sei $(A, \circ)$ Halbgruppe, $X \subseteq A$. Dann ist

$$\langle X\rangle = \left\{ \prod_{i=1}^{n} x_i \;\middle|\; n\in\mathbb{N},\ x_i \in X \right\}.$$

Es sei $(A, \circ, e, (\cdot)^{-1})$ Gruppe, $X \subseteq A$. Dann ist

$$\langle X\rangle = \left\{ \prod_{i=1}^{n} x_i^{\varepsilon_i} \;\middle|\; n\in\mathbb{N},\ x_i \in X,\ \varepsilon_i \in \{1; -1\} \right\}.$$

Man nennt $\langle X\rangle$ die von X erzeugte Unter(halb)gruppe und X ein <u>Erzeugendensystem</u> von $\langle X\rangle$.

Def.: Seien (A, F), (B, F) Algebren vom selben Typ.

Eine Abb. $\varphi : A \to B$ heißt <u>kompatibel</u> mit $f_i \in F$ $:\Longleftrightarrow$

$$\forall a_1, \dots, a_{n_i} \in A : \varphi(f_i(a_1, \dots, a_{n_i})) = f_i(\varphi(a_1), \dots, \varphi(a_{n_i})).$$

φ heißt <u>Homomorphismus</u> von (A, F) in (B, F) $:\Longleftrightarrow$

φ ist kompatibel mit allen f_i, $i \in I$.

Ein Homomorphismus φ heißt
- *Epimorphismus*, falls φ surjektiv
- *Monomorphismus*, falls φ injektiv
- *Isomorphismus*, falls φ bijektiv.

Ein Homomorphismus φ: (*A*, *F*) → (*A*, *F*) heißt *Endomorphismus*; wenn φ zusätzlich bijektiv: *Automorphismus*.

Def.: Seien (A, F), (B, F) Algebren vom selben Typ.

Dann liefert $(A \times B, F)$ mit

$$f_i((a_1, b_1), \dots, (a_{n_i}, b_{n_i})) = (f_i(a_1, \dots, a_{n_i}), f_i(b_1, \dots, b_{n_i}))$$

wieder eine Algebra vom selben Typ wie (A, F) und (B, F), das <u>direkte Produkt</u> von (A, F) und (B, F).

Verallg. auf endlich viele Algebren klar; auch möglich für beliebige Familien von Algebren.

Def.:
Sei $A \neq \emptyset$. $(A, +, \cdot)$ heißt *Halbring*, wenn die folgenden Bedingungen erfüllt sind:
(1) $(A, +)$ ist kommutative Halbgruppe,
(2) $(A, \cdot)$ ist Halbgruppe,
(3) es gelten die Distributivgesetze:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und}$$
$$(b + c) \cdot a = b \cdot a + c \cdot a \qquad \text{für alle } a, b, c \in A.$$

Ein Halbring $(A, +, \cdot)$ heißt *Ring*, wenn $(A, +)$ Gruppe ist.

Es sei $(A, +, \cdot)$ ein Halbring.
Falls die Halbgruppe $(A, +)$ ein (dann eindeutig bestimmtes) neutrales Element hat, nennt man dieses das *Nullelement* des Halbrings und bezeichnet es mit 0.
Es sei $A' = A - \{0\}$, falls $(A, +, \cdot)$ ein Nullelement 0 hat, und $A' = A$ sonst.
Def.:
Sei $|A| \geq 2$. Ein Halbring $(A, +, \cdot)$ heißt *Halbkörper*, wenn $(A', \cdot)$ eine Untergruppe von $(A, \cdot)$ ist.
Ist $(A, +, \cdot)$ sowohl Halbkörper als auch Ring, so heißt diese Struktur ein *Körper* (engl.: *field*).

Beispiele:
$(\mathbb{N}, +, \cdot)$ Halbring, kein Ring
$(\mathbb{Z}, +, \cdot)$ Ring, kein Körper
$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ Körper

Def.: Sei $(A, \circ)$ Gruppoid, $<$ Relation auf A.
$<$ heißt *linkskompatibel* auf $(A, \circ)$ (bzgl. $\circ$), wenn gilt:

$$\forall a, b, c \in A: \quad a < b \Rightarrow c \circ a < c \circ b.$$

Analog: rechtskompatibel.
$<$ *kompatibel* auf $(A, \circ)$ $:\Leftrightarrow$ $<$ rechts- und linkskompatibel.

Ist $\sim$ Äquivalenzrelation auf A und (links)kompatibel, so heißt $\sim$ *Linkskongruenz* bzw. *Kongruenz* auf $(A, \circ)$.
(Verallgemeinerung auf beliebige Algebren klar.)

Charakterisierung von Kongruenzrelationen:

Satz:
Sei $(A, \circ)$ Gruppoid und $\sim$ Äquivalenzrelation auf A. Zu $a \in A$ sei $[a]$ die Äquivalenzklasse von a, also $[a] = \{ b \in A \mid b \sim a \}$.
Es sei $A / \sim \; = \{ [a] \mid a \in A \}$ die Menge der Äquivalenzklassen von A unter $\sim$. Dann gilt:

$$\sim \text{ Kongruenz auf } (A, \circ)$$
$$\Leftrightarrow \forall a, a', b, b' \in A : (a \sim a' \wedge b \sim b' \Rightarrow a \circ b \sim a' \circ b').$$

Dies ist wiederum gleichwertig damit, dass für $A / \sim$ die Def.

$$\forall a, b \in A: \; [a] \circ [b] := [a \circ b]$$

unabhängig von der Wahl der Repräsentanten a, a', a''... $\in [a]$ bzw. b, b', ... $\in [b]$ ist.

In diesem Fall ist $\sim^{\#}: \begin{array}{l} A \to A/\sim \\ a \mapsto [a] \end{array}$

ein Epimorphismus von $(A, \circ)$ auf $(A/\sim, \circ)$,
und $(A/\sim, \circ)$ ist Gruppoid bzw. Halbgruppe bzw. Gruppe, wenn dies für $(A, \circ)$ gilt.

$(A/\sim, \circ)$ heißt <u>Faktorgruppoid</u> oder <u>Quotientengruppoid</u> oder <u>Kongruenzklassengruppoid</u>.

Beispiel: Gruppe $(\mathbb{Z}, +)$, Kongruenz $a \equiv_n b :\Leftrightarrow$ n teilt $(a-b)$, $(\mathbb{Z}/\equiv_n, +)$ Restklassengruppe modulo n (= zyklische Gruppe der Ordnung n).

Freie Halbgruppen und freie Monoide

Def.:

Sei $X \neq \emptyset$ und $X^+ := \bigcup\limits_{n \in \mathbb{N}} X^n = \bigcup\limits_{n \in \mathbb{N}} \{ (x_1, \dots, x_n) \mid x_\nu \in X \}$.

Dann entsteht eine Halbgruppe $(X^+, \cdot)$ durch die Verknüpfung

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_m) := (x_1, \dots, x_n, y_1, \dots, y_m).$$

Die Klammern werden hier meist weggelassen: Konkatenation von Wörtern. $x_1 \dots x_n \cdot y_1 \cdots y_m = x_1 \cdots x_n y_1 \cdots y_m$

$(X^+, \cdot)$ heißt die <u>freie Halbgruppe</u> über X.

Man nennt oft X Alphabet, X^+ die Menge der (freien) Worte über X.

Das durch Hinzufügen eines Einselements 1 entstehende Monoid $(X^*, \cdot, 1)$ mit $X^* := X^+ \cup \{1\}$ heißt das <u>freie Monoid</u> über X.

"Kern" einer Abbildung:
Def.: Sei $f: A \to B$ Abbildung.
$\sim$ = Kern f ist Äquivalenzrelation auf A, def. gemäß
$a_1 \sim a_2 \;:\Leftrightarrow f(a_1) = f(a_2)$ (d.h. gleiches Bild unter f).

Darstellung mit definierenden Relationen

Def. und Satz:
Es sei $(A, \circ)$ Halbgruppe. Eine <u>Darstellung</u> von $(A, \circ)$ <u>durch erzeugende Elemente und definierende Relationen</u> ist gegeben durch

- eine Menge $X \neq \emptyset$ von erzeugenden Symbolen $x_1, x_2, \ldots \in X$,
- eine Abbildung $f: X \to A$ mit $\langle f(X) \rangle = A$ (oft $f = id$),
- eine Relation ρ auf X^+, d.h. eine Menge von Paaren von Wörtern $(w_i, w_i') \in X^+ \times X^+$,

so dass für die von ρ <u>erzeugte</u> Kongruenz $\sim$ auf $(X^+, \cdot)$
(d.h.: $\sim = \bigcap\limits_{\substack{\rho \subseteq \mu \\ \mu \text{ Kongruenz}}} \mu$) gilt: $\sim = \text{Kern } \bar{f}$

für den eindeutig bestimmten Homomorphismus
$$\bar{f}: (X^+, \cdot) \to (A, \circ) \quad \text{mit } \bar{f}|_X = f .$$

Man nennt diese Darstellung <u>endlich</u> und dann A <u>endlich darstellbar</u>, wenn $|X| < \infty$ und $|\rho| < \infty$.

Entsprechend für Monoide und Gruppen.

Beachte: Die von ρ erzeugte Kongruenz ist die kleinste (d.h. als Klasseneinteilung feinste) Kongruenz auf $(X^+, \cdot)$, die ρ enthält, in der also $w_i \sim w_i'$ für alle i.
Man schreibt oft $=$ statt $\sim$ und nimmt $f = id$ an, identifiziert also die Elemente von A mit Wortdarstellungen aus Symbolen aus X.

Der Cayley-Graph

Def.: Sei die Halbgruppe (das Monoid, die Gruppe) $(A, \circ)$ endlich erzeugt durch das Erzeugendensystem X.
Der <u>Cayley-Graph</u> von $(A, \circ)$ bzgl. X ist ein gerichteter Graph mit Knotenmenge A und mit X als Menge von Kantenlabels, für den gilt:

$$a \xrightarrow[x_i]{} b \quad :\Longleftrightarrow \quad a \circ x_i = b$$

(präziser: $a \circ f(x_i) = b$)

Im Falle eines selbstinversen Erzeugenden x_j (d.h. $x_j^{-1} = x_j$) fasst man je zwei gegenläufige Kanten mit Label x_j zu je einer ungerichteten Kante zusammen:

$$\begin{tikzcd} a \arrow[r, bend left, "x_j"] & b \arrow[l, bend left, "x_j"] \end{tikzcd} \quad \equiv \quad \begin{tikzcd} a \arrow[r, dash, "x_j"'] & b \end{tikzcd}$$

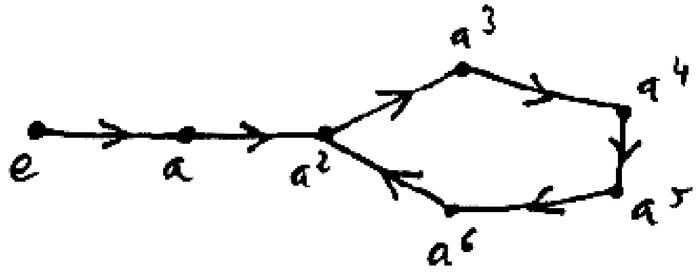
Beispiel 1:

Erzeugendensystem $X = \{ a \}$,
definierende Relation $\rho = \{ (a^7; a^2) \}$
oder kurz " $a^7 = a^2$ "

def. als Monoid das *zyklische Monoid* mit Vorperiode 2 und Periodenlänge 5:

$a^7 = a^2 \;\Rightarrow\; a^8 = a^3,\; a^9 = a^4, ..., a^{12} = a^7 = a^2, ...$
$A = \{ e; a; a^2; a^3; a^4; a^5; a^6 \},\; |A| = 7$
(e ist das neutrale Element)

mit Cayley-Graph:



(Der Cayley-Graph enthält dieselbe Information wie die Verknüpfungstafel!)

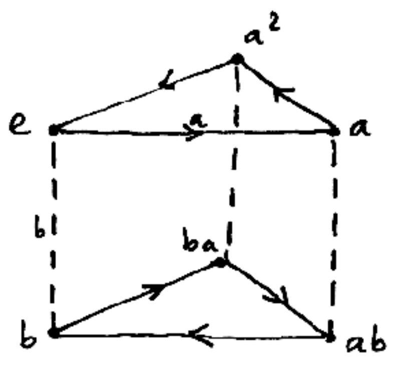
Beispiel 2:
Gruppe, erzeugt von $X = \{ a; b \}$
mit den definierenden Relationen

$$a^3 = e$$
$$b^2 = e$$
$$(ab)^2 = e.$$

Behauptung: $|A| = 6$, $A = \{ e; a; b; a^2; ab; ba \}$.
Denn: Multiplikation von rechts mit den Erzeugenden führt nicht aus dieser Menge heraus:

$$b^2 = e$$
$$a^3 = e$$
$$aab = a^{-1}b = a^{-1}(abab)b = babb = ba$$
$$aba = b^{-1} = b$$
$$baa = ba^{-1} = ba^{-1}abab = bbab = ab$$
$$bab = a^{-1}abab = a^{-1} = a^2$$

Cayley-Graph:



Anmerkung: diese Gruppe ist isomorph zur symmetrischen Gruppe S_3 aller Permutationen von 3 Elementen vermittels

$$a \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Def.:

Es sei $Z \neq \emptyset$ eine Menge und $(S, \circ)$ eine Halbgruppe.

Es sei weiterhin
$$\delta^*: Z \times S \to Z$$
$$(z; s) \mapsto \delta^*(z; s) = zs$$

eine Rechtsoperatorenanwendung von S auf Z mit

(1) $\forall z \in Z \; \forall s_1, s_2 \in S: \quad (zs_1)s_2 = z(s_1 \circ s_2)$ und

(2) falls $(S, \circ)$ ein Einselement 1 hat: $\forall z \in Z: \quad z1 = z$.

Dann heißt $Z_S = (Z; (S, \circ); \delta^*)$, aufgefasst als Algebra mit sovielen einstelligen Operationen, wie S Elemente hat, eine <u>S-(Rechts-) Menge</u>.

Nach (1) genügt es wegen $z(s_1 \circ \ldots \circ s_n) = (\ldots((zs_1)s_2)\ldots)s_n$, ein Erzeugendensystem X von S und $\delta := \delta^*|_X$, also $(Z; X; \delta)$ anzugeben.

Für $S = X^*$ über einem (meist endlichen) Alphabet X ist dann der Spezialfall

$$A = (Z; X; \delta) = (Z; X^*; \delta^*)$$

ein <u>Moore-Automat</u> (auch: Halbautomat) mit Zustandsmenge Z, Eingabealphabet X, Transitionsfunktion δ.

Satz: Jeder Moore-Automat $A = (Z; X; \delta)$ ist selbst eine X^*-Rechtsmenge Z_{X^*}. Man ordnet ihm „sein Monoid"

$$S^1 = (X^*/\sim\, ; \circ ; 1)$$

mit der S^1-Rechtsmenge $Z_{S^1} = (Z; S^1; \delta^*_{S^1})$ zu gemäß

$$w \sim w' :\Leftrightarrow \forall z \in Z: zw = zw'$$

$$(z; [w]_\sim) \longmapsto \delta^*_{S^1}(z; [w]_\sim) := zw$$

mit beliebigem $w \in [w]_\sim$.

Satz: Jedem Monoid $(S^1; \circ; 1)$ mit $S^1 \neq \{1\}$ kann ein Moore-Automat $A = (Z; X; \delta)$ zugeordnet werden gemäß

$$Z = S^1, \quad |X| = |S| \text{ mit } S = S^1 \setminus \{1\}, \quad \varphi: X \to S \text{ Bijektion}$$

$$\text{und } \delta(z; x) := z \circ \varphi(x) \quad (\text{Produkt in } (S^1; \circ)),$$

dessen Monoid i. Sinne des vorherigen Satzes genau das Ausgangsmonoid S^1 ist.

(Weinert 1984)

Halbverbände, Verbände und boolesche Algebren

Def.:

Ein algebraischer $\wedge$-*Halbverband* ist eine kommutative, idempotente Halbgruppe $(S; \wedge)$

(d.h. $\forall a, b \in S: a \wedge b = b \wedge a$

und $\forall a \in S: a \wedge a = a$).

Def.:
Eine partiell geordnete Menge $(M; \leq)$ heißt ordnungstheoretischer $\wedge$-Halbverband, wenn gilt:
$\forall a, b \in M$ existiert $a \wedge b := \inf\{a; b\}$.

Satz:
Jeder ordnungstheoretische $\wedge$-Halbverband $(M; \leq)$ ist ein algebraischer $\wedge$-Halbverband gemäß
$a \wedge b := \inf\{a; b\}$, und umgekehrt gemäß
$a \leq b \;:\Leftrightarrow\; a \wedge b = a$;
und diese Korrespondenz ist bijektiv.

(aus Weinert 1984)

Def.:
Ein algebraischer *Verband* ist eine Algebra $(S; \wedge; \vee)$, für die gilt: $(S; \wedge)$ und $(S; \vee)$ sind kommutative Halbgruppen, und es gelten die Absorptionsgesetze:
$\forall a, b \in S: \; a \wedge (a \vee b) = a$ und $a \vee (a \wedge b) = a$.

Satz: Jeder ordnungstheoretische Verband $(M; \leq)$ ist ein algebraischer Verband gemäß
$a \wedge b := \inf\{a; b\}$ und $a \vee b := \sup\{a; b\}$,
und umgekehrt gemäß $a \leq b \;:\Leftrightarrow\; a \wedge b = a$;
und diese Korrespondenz ist bijektiv.

Def.:
Ein Verband heißt *distributiv*, falls beide Distributivgesetze gelten:

$$
\begin{aligned}
a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \\
a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c)
\end{aligned}
$$

Elemente $0, 1 \in V$ eines Verbandes hießen *Null– und Einselement*, falls gelten

$$\forall a \in V \; : \; 0 \wedge a = 0, \quad 0 \vee a = a$$
$$\forall a \in V \; : \; 1 \wedge a = a, \quad 1 \vee a = 1.$$

Ein Verband heißt komplementär, falls er Null- und Einselement enthält und es zu jedem Element *a* ein komplementäres Element
$\overline{a} \in V$ gibt mit

$$a \wedge \overline{a} = 0, \quad a \vee \overline{a} = 1$$

Ein distributiver und komplementärer Verband wird nach George Boole (1815–1864) *Boolescher Verband* oder *Boolesche Algebra* genannt.

Beispiele:

a) Es sei *M* eine Menge. Nach den Gesetzen der Mengenalgebra ist dann $(\mathcal{P}(M), \cap, \cup)$ ein distributiver Verband.
Es gibt ferner ein Nullelement $\emptyset$ und ein Einselement M. Der Verband ist auch komplementär mit $\overline{A} = M \setminus A$, also ist $(\mathcal{P}(M), \cap, \cup)$ eine Boolesche Algebra.

b) $(\mathbb{N}, \mathrm{ggT}, \mathrm{kgV})$ ist ein distributiver Verband. Ein Nullelement ist die $1 \in \mathbb{N}$, der Verband besitzt jedoch kein Einselement und ist somit auch keine Boolesche Algebra!

c) Wir setzen $\mathbb{B} := \{0,1\}$ mit den Verknüpfungen

$$i \wedge j := \min(i,j), \quad i \vee j := \max(i,j).$$

Analog definieren wir für $\mathbb{B}^n := \{(i_1,\ldots,i_n) \mid i_k \in \mathbb{B}\}, \quad n \in \mathbb{N}$,

$$\begin{aligned}(i_1,\ldots,i_n) \wedge (j_1,\ldots,j_n) &:= (\min(i_1,j_1),\ldots,\min(i_n,j_n))\\ (i_1,\ldots,i_n) \vee (j_1,\ldots,j_n) &:= (\max(i_1,j_1),\ldots,\max(i_n,j_n))\end{aligned}$$

Damit ist $(\mathbb{B}^n, \wedge, \vee)$ ein distributiver Verband mit Nullelement $\mathbf{0} := (0,\ldots,0)$ und Einselement $\mathbf{1} := (1,\ldots,1)$. Weiterhin ist $\mathbb{B}^n$ auch komplementär mit

$$\overline{(i_1,\ldots,i_n)} := (\overline{i_1},\ldots,\overline{i_n}), \qquad \overline{i_k} := \begin{cases} 0, & i_k = 1 \\ 1, & i_k = 0 \end{cases}$$

Damit ist $(\mathbb{B}^n, \wedge, \vee)$ eine Boolesche Algebra.

Satz (Eindeutigkeit von 0, 1 und Komplement):

a) Besitzt ein Verband ein Null– bzw. ein Einselement, so ist dieses eindeutig bestimmt.

b) In einem distributiven Verband V gilt die folgende *Kürzungsregel*

$$\forall a,b,c \in V : \ (a \wedge b = a \wedge c) \ \wedge \ (a \vee b = a \vee c) \ \Rightarrow \ b = c.$$

c) In einer Booleschen Algebra sind die Komplemente eindeutig bestimmt und es gelten $\overline{\overline{a}} = a$, $\overline{a \wedge b} = \overline{a} \vee \overline{b}$ sowie $\overline{a \vee b} = \overline{a} \wedge \overline{b}$.

Beweis: s. Oberle (2007).

Satz (Dualitätsprinzip für Verbände):

Jede korrekte Formel in einem Verband, in dem nur die Verknüpfungen $\wedge$ und $\vee$ verwendet werden, bleibt richtig, wenn überall $\wedge$ und $\vee$ vertauscht werden. Die Formel mit vertauschten Verknüpfungen heisst *duale Aussage*. Liegt eine Beweis für eine Formel vor und vertauscht man darin die Verknüpfungen $\wedge$ und $\vee$, so erhält man einen Beweis für die duale Aussage.

Satz:

Besitzt ein Verband V ein Null– und Einselement, so gilt: $0 = \min V$ und $1 = \max V$.
Jeder *endliche* Verband besitzt ein Null– und ein Einselement.

Beweis: s. Oberle (2007).

Def.:

Sei V ein Verband mit Nullelement 0. Ein Element $y \neq 0$ heißt *Atom*, falls für alle $x \in V$ gilt: $x \geq y$ oder $x \wedge y = 0$.

V heißt *atomar*, falls jedes Element $x \neq 0$ eine Basisdarstellung $x = y_1 \vee y_2 \vee \ldots \vee y_m$ mit Atomen $y_1, \ldots, y_m$ besitzt.

Beispiele:

a) $(\mathcal{P}(M), \cup, \cap)$ hat die Atome $\{a\}$, $a \in M$. Ist M endlich, so ist $(\mathcal{P}(M), \cup, \cap)$ atomar.

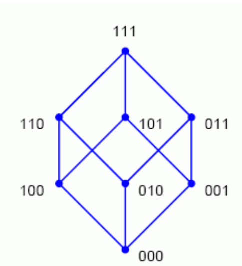
b) Im distributiven Verband $(\mathbb{N}, \text{ggT}, \text{kgV})$ ist $p \in \mathbb{N}$ genau dann ein Atom, wenn p prim ist. Ein Element $n \in \mathbb{N}$ besitzt jedoch nur dann eine Basisdarstellung durch Atome, wenn jeder Primfaktor von n einfach ist.

c) Die Boolesche Algebra $(\mathbb{B}^n, \wedge, \vee)$ ist atomar. Die Atome sind die kanonischen Einheitsvektoren $\mathrm{e}_i := (0, \ldots, 0, 1, 0, \ldots, 0)$, $i = 1, \ldots, n$, wobei die 1 an der i-ten Stelle steht. Die Basisdarstellung eines Elements $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ lautet

$$\mathbf{x} = \bigvee_{\{i:\, x_i = 1\}} \mathrm{e}_i .$$

Betrachten wir konkret $(\mathbb{B}^3, \wedge, \vee)$, so hat man die Atome $\mathrm{e}_1 = 100$, $\mathrm{e}_2 = 010$ und $\mathrm{e}_3 = 001$ und für $\mathbf{x} = 101$ ergibt sich die Basisdarstellung $101 = 100 \vee 001$.

Liniendiagramm von $\mathbf{B}^3$:



Der folgende *Kennzeichnungssatz für endliche Boolesche Algebren* zeigt, dass diese stets atomar sind, und bereits durch ihre Elementzahl bis auf Isomorphie eindeutig bestimmt sind.

Stonescher Darstellungssatz:

Es sei $(V, \wedge, \vee)$ eine endliche Boolesche Algebra.

a) Sind $y_1 \neq y_2$ zwei verschiedene Atome so gilt $y_1 \wedge y_2 = 0$.

b) Zu jedem $x \in V \setminus \{0\}$ gibt es ein Atom $y \in V$ mit $y \leq x$.

c) V ist atomar.

d) Die Basisdarstellung eines Elementes $x \in V$ durch Atome $x = y_1 \vee y_2 \vee \cdots \vee y_m$ ist bis auf die Reihenfolge eindeutig.

e) Hat V genau m Atome, so hat V genau 2^m Elemente.

f) Gleichmächtige (endliche) Boolesche Algebren sind isomorph.

Ausschnitte entnommen aus
Hebisch & Weinert (1993), Oberle (2007),
Weinert (1983), Weinert (1984)
(genaue Quellenangaben siehe http://www.uni-forst.gwdg.de/~wkurth/fs10_lit.htm)