Kapitel 3

Verbände und Boolesche Algebren

3.1 Halbgeordnete Mengen

In den Abschnitten 1.5 und 1.6 haben wir uns schon einführend mit Halbordnungen beschäftigt. Jetzt werden wir uns eingehender mit diesen Strukturen auseinandersetzen und wiederholen ein paar grundlegende Definitionen.
Sei M eine Menge und R eine zweistellige Relation auf M mit

1) $\forall x \in M : xRx$ (Reflexivität),

2) $\forall x, y \in M : xRy$ und $yRx \Rightarrow x = y$ (Antisymmetrie),

3) $\forall x, y, z \in M : xRy$ und $yRz \Rightarrow xRz$ (Transitivität),

dann heißt R eine *Halbordnung* auf M. Weiters heißt (M, R) eine *halbgeordnete* Menge. Gilt zusätzlich

4) $\forall x, y \in M : xRy$ oder yRx (Vergleichbarkeit),

dann heißt (M, R) eine *Kette* oder *linear geordnete* Menge oder *Totalordnung*.

3.1.1 Anmerkung. Statt „Halbordnung“ sagt man oft auch „partielle Ordnung“, abgekürzt po oder p.o., manchmal auch nur „Ordnung“.[1] Diese Ausdrücke werden sowohl für die Relation R selbst wie auch für die gesamte Struktur (M, R) verwendet.
Gelegentlich ist mit „Ordnung“ auch eine *Totalordnung* (=*lineare Ordnung*, *Kette*[2]) gemeint.

Bezeichnungen. Statt R wird meist „$\leq$“ geschrieben. Weiters sei:

$$\begin{aligned} x \geq y &:\Leftrightarrow y \leq x, \\ x < y &:\Leftrightarrow x \leq y,\ x \neq y, \\ x > y &:\Leftrightarrow x \geq y,\ x \neq y. \end{aligned}$$

3.1.2 Anmerkung. Für $A, B \subseteq M$ schreiben wir $A \leq B$ für $\forall x \in A\, \forall y \in B\ (x \leq y)$. Statt „$a \leq x$ und $b \leq x$“ schreiben wir also $\{a, b\} \leq x$ oder meist weiter abgekürzt „$a, b \leq x$“; analog ist $x \leq a, b$ zu verstehen.
Statt „$a \leq b$ und $b \leq c$“ schreiben wir oft $a \leq b \leq c$.

Eine *strikte Halbordnung* auf einer Menge M ist eine zweistellige Relation S, die

1) irreflexiv ($\forall x \in M$: $(x, x) \notin R$) und

[1] englisch: *order oder partial order*
[2] englisch: *: total order, linear order, chain*

2) transitiv

ist. Wenn S eine strikte Halbordnung ist, dann ist $S \cup \{(x,x) \mid x \in M\}$ eine Halbordnung; wenn R eine Halbordnung ist, dann ist $R \setminus \{(x,x) \mid x \in M\}$ eine strikte Halbordnung. Jeder Satz über Ordnungen lässt sich also in einen Satz über strikte Ordnungen übersetzen, und umgekehrt.
Gelegentlich ist mit dem Wort „Ordnung“ oder „Halbordnung“ auch eine strikte Halbordnung gemeint. Ob es sich tatsächlich um eine Halbordnung in unserem Sinn oder um eine strikte Halbordnung handelt, lässt sich meist aus dem Kontext oder aus der Notation erschließen: Für Halbordnungen werden meist Symbole wie $\leq$, $\leqq$, $\subseteq$, $\preceq$, $\sqsubseteq$ etc verwendet, für strikte Halbordnungen $<$, $\subset$, $\prec$, $\sqsubset$, etc. Um die Areflexivität einer Relation zu betonen, verwendet man auch gerne Symbole wie $\subsetneqq$.

3.1.3 Beispiele. 1) $(\mathbb{R}, \leq)$ ist Kette.

2) $(\mathbb{N}_0, |)$ ist halbgeordnete Menge, aber keine Kette.

3) $(\mathfrak{P}(M), \subseteq)$ ist halbgeordnete Menge, aber für $|M| \geq 2$ keine Kette.

3.1.4 Definition. Sei $(M, \leq)$ halbgeordnete Menge. Dann heißt $k \in M$ *kleinstes* (bzw. *größtes*) Element von $M :\Leftrightarrow \forall x \in M : k \leq x$ (bzw. $k \geq x$). (Vgl. auch 1.6.2.)

3.1.5 Beispiele. 1) $(\mathbb{R}, \leq)$ hat kein kleinstes bzw. größtes Element.

2) $(\mathbb{N}_0, |)$ hat 1 als kleinstes und 0 als größtes Element.

3) $(\mathfrak{P}(M), \subseteq)$ hat $\emptyset$ als kleinstes und M als größtes Element.

3.1.6 Anmerkung. Es gibt stets höchstens ein kleinstes bzw. größtes Element, denn: sind k_1, k_2 kleinste Elemente, dann gilt $k_1 \leq k_2$ und $k_2 \leq k_1$, somit $k_1 = k_2$. Analog für größte Elemente.

3.1.7 Definition. Sei $(M, \leq)$ halbgeordnete Menge. Dann heißt $m \in M$ *minimales* (bzw. *maximales*) Element von $M :\Leftrightarrow (\forall x \in M : x \leq m$ (bzw. $x \geq m$) $\Rightarrow x = m)$.

Jedes kleinste Element ist auch minimal, jedes größte auch maximal.

3.1.8 Satz. a) *Sei $(M, \leq)$ halbgeordnete Menge und $N \subseteq M$. Dann ist $(N, \leq)$ ebenfalls eine halbgeordnete Menge. Ist $(M, \leq)$ eine Kette, dann auch $(N, \leq)$. Dabei steht $(N, \leq)$ abkürzend für $(N, \leq \cap (N \times N))$.*

b) *Ist $(M, \leq)$ halbgeordnete Menge, dann auch $(M, \geq)$. („Dualitätsprinzip für halbgeordnete Mengen“)* □

Duale Begriffe:

$\leq$	$\geq$
kleinstes Element	größtes Element
maximales Element	minimales Element

So gilt etwa: m ist maximal in $(M, \leq) \Leftrightarrow m$ ist minimal in $(M, \geq)$.

3.1.9 Definition. Sei $(M, \leq)$ halbgeordnete Menge und $N \subseteq M$. Dann heißt $u \in M$ eine *untere Schranke* von $N :\Leftrightarrow \forall x \in N : u \leq x$. Ein größtes Element der Menge aller unteren Schranken heißt ein *Infimum* von N, in Zeichen: $\inf N$ oder $\bigwedge N$. Ein Element $v \in M$ heißt eine *obere Schranke* von $N :\Leftrightarrow \forall x \in N : x \leq v$, und eine kleinste obere Schranke heißt ein *Supremum* von N, in Zeichen: $\sup N$ oder $\bigvee N$. (Vgl. auch 1.6.2.)

3.1.10 Beispiele. 1) In $(\mathbb{R}, \leq)$ entsprechen die eben definierten Begriffe den in der Analysis üblichen.

2) In $(\mathbb{N}_0, |)$ gilt für $T \subseteq \mathbb{N}_0$ mit $T \neq \emptyset$: $\inf T = \mathrm{ggT}(T)$ und $\sup T = \mathrm{kgV}(T)$. Weiters ist $\inf \emptyset = 0$ und $\sup \emptyset = 1$.

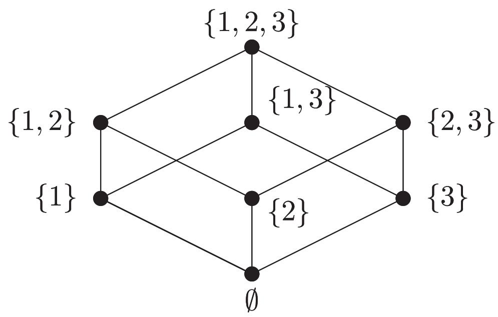
3) In $(\mathfrak{P}(M), \subseteq)$ gilt für $\mathcal{S} \subseteq \mathfrak{P}(M)$: $\inf \mathcal{S} = \bigcap \mathcal{S}$ und $\sup \mathcal{S} = \bigcup \mathcal{S}$.

Hassediagramm. Sei $(M, \leq)$ eine endliche halbgeordnete Menge und die Relation „benachbart" definiert durch:

$$a, b \textit{ benachbart } :\Leftrightarrow \begin{cases} 1)\ a < b \text{ oder } b < a, \\ 2)\ \text{es gibt kein } c \text{ mit } a < c < b \text{ oder } b < c < a. \end{cases}$$

Dann ist das Hassediagramm von $(M, \leq)$ gegeben durch den Graphen der Relation „benachbart". (Knotenmenge M; ist $a < b$, zeichnet man den Knoten a „tiefer" als den Knoten b und verbindet a und b mit einer Kante, falls sie benachbart sind.)

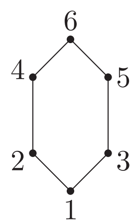
3.1.11 Beispiel. Das Hassediagramm für $(\mathfrak{P}(\{1, 2, 3\}), \subseteq)$ sieht so aus:

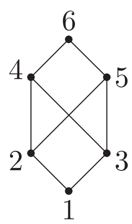


3.2 Halbordnungen und Verbände

3.2.1 Definition. Sei $(V, \leq)$ eine halbgeordnete Menge. $(V, \leq)$ heißt *verbandsgeordnete Menge* $:\Leftrightarrow$ $\sup\{a, b\}$ und $\inf\{a, b\}$ existieren für alle $a, b \in V$. (Vgl. auch 1.6.4.)

3.2.2 Beispiel. Auf $M = \{1, 2, 3, 4, 5, 6\}$ seien zwei Halbordnungsrelationen $\leq$ und $\leq'$ definiert.

$(M, \leq)$: 

$(M, \leq')$: 

$(M, \leq)$ ist verbandsgeordnet (z.B. ist $\inf\{2, 3\} = 1$ und $\sup\{2, 3\} = 6$). Dagegen ist $(M, \leq')$ *nicht* verbandsgeordnet: $\sup\{2, 3\}$ existiert nicht, da die Menge $\{2, 3\}$ die oberen Schranken 4, 5 und 6, also keine kleinste obere Schranke besitzt.

Statt „verbandsgeordnete Menge" kann man auch *Verband im ordnungstheoretischen Sinn* sagen. Wir werden jetzt sehen, dass man sich dem Konzept der verbandsgeordneten Mengen auch von algebraischer Seite nähern kann.

3.2.3 Definition. Eine Algebra $(V, \wedge, \vee)$ vom Typ $(2, 2)$ heißt ein *Verband*[3] $:\Leftrightarrow$ für alle $a, b, c \in V$ gilt:

[3] englisch: *lattice*

1) $a \wedge b = b \wedge a$, $a \vee b = b \vee a$,

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

3) $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$.

Nach 1) und 2) sind $\wedge$ und $\vee$ kommutativ und assoziativ, d.h., $(V, \wedge)$ und $(V, \vee)$ sind kommutative Halbgruppen. Die beiden unter 3) genannten Gesetze nennt man *Verschmelzungsgesetze*.

3.2.4 Beispiel. $(\mathfrak{P}(M), \cap, \cup)$ ist ein Verband.

3.2.5 Lemma. *Sei* $(V, \wedge, \vee)$ *ein Verband, dann gilt:*

a) $\forall a \in V : a \wedge a = a = a \vee a$,

b) $\forall a, b \in V : a \wedge b = a \Leftrightarrow a \vee b = b$.

Beweis. a) Auf Grund der Verschmelzungsgesetze gilt: $a \wedge a = a \wedge (a \vee (a \wedge a)) = a$ und $a \vee a = a \vee (a \wedge (a \vee a)) = a$.

b) $\Rightarrow$: $a \vee b = (a \wedge b) \vee b = b$, $\Leftarrow$: $a \wedge b = a \wedge (a \vee b) = a$, ebenfalls nach den Verschmelzungsgesetzen. □

Der folgende Satz stellt den Zusammenhang zwischen Verbänden und verbandsgeordneten Mengen her.

3.2.6 Satz. (a) *Sei* $(V, \wedge, \vee)$ *ein Verband. Definiert man eine Relation* $\leq$ *auf* V *durch*

$$\forall a, b \in V : \quad a \leq b :\Leftrightarrow a \wedge b = a,$$

dann ist $(V, \leq)$ *eine verbandsgeordnete Menge, wobei* $a \wedge b = \inf\{a, b\}$, $a \vee b = \sup\{a, b\}$.

(b) *Sei* $(V, \leq)$ *eine verbandsgeordnete Menge. Definiert man auf* V *zweistellige Operationen* $\wedge, \vee$ *durch*

$$\forall a, b \in V : \qquad a \wedge b := \inf\{a, b\}, \ a \vee b := \sup\{a, b\},$$

dann ist $(V, \wedge, \vee)$ *ein Verband.*

(c) *Die in* (a) *und* (b) *definierten Zuordnungen sind zueinander invers.*

Beweis. (a) Die Relation $\leq$ ist reflexiv ($a \leq a$ wegen $a \wedge a = a$), antisymmetrisch ($a \leq b \leq a \Rightarrow a \wedge b = a$ und $a \wedge b = b$, also $a = b$) und transitiv ($a \leq b \leq c \Rightarrow a \wedge b = a$, $b \wedge c = b$, daher $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$).

Wir zeigen nun, dass $a \wedge b = \inf\{a, b\}$ gilt: $a \wedge b \leq a, b$ gilt wegen $a \wedge b \wedge a = a \wedge b \wedge b = a \wedge b$; aus $x \leq a, b$ folgt $a \wedge x = b \wedge x = x$, also $(a \wedge b) \wedge x = a \wedge (b \wedge x) = a \wedge x = x$, daher $x \leq a \wedge b$.
Die Beziehung $a \vee b = \sup\{a, b\}$ zeigt man ganz ähnlich.

(b) Wir müssen zeigen, dass die Verbandsgesetze gelten:

$a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a$.

Wir überlegen zunächst, dass jede untere Schranke s von $\{a, b, c\}$ auch untere Schranke von $\{a, b \wedge c\}$ ist, und umgekehrt:

$s \leq a, b, c \Rightarrow s \leq a$ und $s \leq b \wedge c = \inf\{b, c\}$;
wenn umgekehrt $s \leq a$ und $s \leq b \wedge c$, dann ist $s \leq a, b, c$.

Daher ist die größte untere Schranke von a, b, c auch gleich der größten unteren Schranke von a und $b \wedge c$:

$$a \wedge (b \wedge c) = \inf\{a, b, c\}.$$

Analog ist auch $(a \wedge b) \wedge c = \inf\{a, b, c\}$, also $(a \wedge b) \wedge c = \inf\{a, b, c\} = a \wedge (b \wedge c)$.

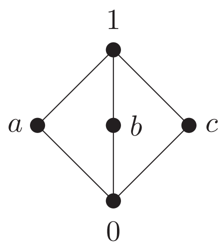
Analog zeigt man die dualen Gesetze.

(c) $(V, \wedge, \vee) \overset{(a)}{\longmapsto} (V, \leq) \overset{(b)}{\longmapsto} (V, \wedge^*, \vee^*)$, wobei $a \wedge^* b = \inf\{a, b\} = a \wedge b$ und $a \vee^* b = \sup\{a, b\} = a \vee b$.

$(V, \leq) \overset{(b)}{\longmapsto} (V, \wedge, \vee) \overset{(a)}{\longmapsto} (V, \leq^*)$, wobei $a \leq^* b \Leftrightarrow a \wedge b = a \Leftrightarrow \inf\{a, b\} = a \Leftrightarrow a \leq b$. $\square$

Jeder endliche Verband kann somit durch ein Hassediagramm beschrieben werden.

3.2.7 Beispiele. 1)



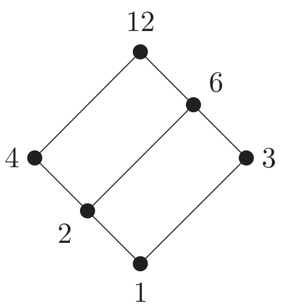
$\wedge$	0	a	b	c	1
0	0	0	0	0	0
a	0	a	0	0	a
b	0	0	b	0	b
c	0	0	0	c	c
1	0	a	b	c	1

$\vee$	0	a	b	c	1
0	0	a	b	c	1
a	a	a	1	1	1
b	b	1	b	1	1
c	c	1	1	c	1
1	1	1	1	1	1

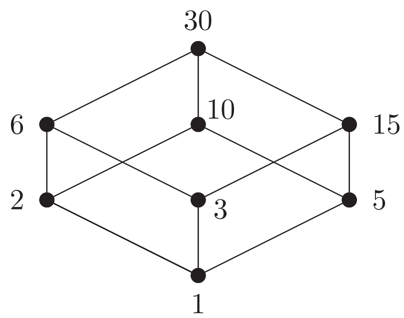
0 ist kleinstes Element und zugleich neutrales Element bei $\vee$. 1 ist größtes Element und zugleich neutrales Element bei $\wedge$.

2) Teilerverbände $(T_n, \mathrm{ggT}, \mathrm{kgV})$ mit $T_n := \{t \in \mathbb{N} \mid t \text{ teilt } n\}$, $n \in \mathbb{N}$. Hassediagramm von

T_{12} :



T_{30} :



3) Sei A eine Algebra (z.B. eine Gruppe). Dann wird die Menge $\mathrm{Sub}(A)$ aller Unteralgebren von A durch die Mengeninklusion $\subseteq$ zu einer verbandsgeordneten Menge: Für $X, Y \in \mathrm{Sub}(A)$ ist nämlich $X \cap Y$ wieder eine Unteralgebra von A und daher die größte untere Schranke von X und Y, d.h. $X \wedge Y = X \cap Y$. Die kleinste obere Schranke ist

$$(*) \qquad X \vee Y = \langle X \cup Y \rangle = \bigcap \{Z \in \mathrm{Sub}(A) \mid X \cup Y \subseteq Z \subseteq A\}$$

die von $X \cup Y$ erzeugte Unteralgebra. (Vgl. 2.1.10 und 2.1.11.)

3.2.8 Anmerkung. Die Operationen $\wedge$ und $\vee$ nennt man oft (in Analogie zu den Operationen $\cap$ und $\cup$ in $\mathfrak{P}(X)$) „Schnitt“ und „Vereinigung“[4].

[4] englisch: *meet, join*

Diese Bezeichnungen können aber gelegentlich missverstanden werden: Wenn wir etwa den Verband $\mathrm{Sub}(A)$ aller Unteralgebren einer Algebra A betrachten, ist der verbandstheoretische Schnitt (d.h. das Infimum im Verband) zweier Unteralgebren zwar gleich dem mengentheoretischen Durchschnitt. Die verbandstheoretische Vereinigung (d.h. das Supremum im Verband) ist, wie in $(*)$ angegeben, die von $X \cup Y$ erzeugte Unteralgebra $\langle X \cup Y \rangle$, welche in der Regel eine echte Obermenge der mengentheoretischen Vereinigung $X \cup Y$ darstellt.

Dualitätsprinzip für Verbände:

$$\begin{aligned} (V, \wedge, \vee) \text{ Verband} &\Leftrightarrow (V, \vee, \wedge) \text{ Verband}, \\ (V, \leq) \text{ verbandsgeordnet} &\Leftrightarrow (V, \geq) \text{ verbandsgeordnet}. \end{aligned}$$

Wenn wir den Verband $(V, \wedge, \vee)$ mit V bezeichnen, nennen wir den Verband $(V, \vee, \wedge)$ den zu V dualen Verband und bezeichnen ihn mit V^d.
Zu jeder Aussage φ über Verbände (im ordnungstheoretischen oder auch im algebraischen Sinn) definieren wir eine Aussage φ^d, die „duale" Aussage so: Wir ersetzen in φ das Symbol $\wedge$ durch $\vee$, $\vee$ durch $\wedge$, $\leq$ durch $\geq$. (Alle weiteren verbandstheoretischen Konzepte müssen natürlich ebenfalls durch die dualen ersetzt werden — „minimal" durch „maximal", inf durch sup, etc.)
Wenn nun die Aussage φ für den Verband V zutrifft (z.B.: „V hat ein größtes Element"), dann trifft die Aussage φ^d auf den Verband V^d zu (z.B.: „V^d hat ein kleinstes Element").
Wenn eine Aussage φ auf alle Verbände zutrifft, dann trifft auch φ^d auf alle Verbände zu.

3.2.9 Satz (Rechenregeln für Verbände). 1) *Die Operationen $\vee$ und $\wedge$ sind monoton. Das heißt, aus $a_1 \leq a_2$ und $b_1 \leq b_2$ folgt $a_1 \wedge b_1 \leq a_2 \wedge b_2$ und $a_1 \vee b_1 \leq a_2 \vee b_2$.*

2) *$a \leq b \wedge c \Leftrightarrow a \leq b$ und $a \leq c$.*

3) *$a \geq b \vee c \Leftrightarrow a \geq b$ und $a \geq c$.*

Beweis. (1) ist Übungsbeispiel 60. (2) gilt, weil $b \wedge c$ die *größte* untere Schranke für b und c ist. (3) ist zu (2) dual. □

3.2.A Unterverbände

Sei $(V, \wedge, \vee)$ ein Verband. Ein *Unterverband* ist eine Teilmenge von V, die unter $\wedge$ und $\vee$ abgeschlossen ist.

3.2.10 Beispiel. Sei $(V, \wedge, \vee)$ ein Verband, und sei $\leq$ die zugehörige Ordnung. Wenn $K \subseteq V$ eine Kette in $(V, \leq)$ ist, dann ist K Unterverband von V. Insbesondere ist jede einelementige Teilmenge ein Unterverband, ebenso die leere Menge.

3.2.11 Anmerkung. Sei V Verband mit den Operationen $\wedge$ und $\vee$ und der Ordnung $\leq$. Sei W ein Unterverband; die Operationen von W sind dann die Einschränkungen von $\wedge$ und $\vee$ auf die Menge $V \times V$; wir schreiben aber meist $\wedge$ und $\vee$ (oder gelegentlich $\wedge_W$ und $\vee_W$) für diese Operationen, statt genauer $\wedge\restriction(V \times V)$ und $\vee\restriction(V \times V)$ zu schreiben.

Die partielle Ordnung von W ist die Einschränkung von $\leq$ auf die Menge W, d.h. formal: die Menge $\{(x, y) \in W \times W \mid x \leq y\}$, oder kürzer $\leq \cap (W \times W)$; wir schreiben $\leq$ oder $\leq_W$ für diese Relation.
Die Struktur $(W, \leq)$ ist ein verbandsgeordnete Menge.

3.2.12 Beispiel. Sei V die Potenzmenge der Menge $\{0, 1, 2\}$, und sei $W_1 := \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$, $W_2 := \{\emptyset, \{0\}, \{1\}, \{0, 1, 2\}\}$.

Dann ist V ein Verband mit Operationen $\cup$ und $\cap$ und der Relation $\subseteq$. Die Halbordnungen $(W_1, \subseteq)$ und $(W_2, \subseteq)$ sind zueinander isomorph; beide sind verbandsgeordnete Mengen. Aber W_1 ist Unterverband von V, W_2 nicht.

3.2.B Kongruenzrelationen

3.2.13 Lemma. *Seien $(V_i, \wedge_i, \vee_i)$ für $i = 1, 2$ Verbände mit den zugehörigen Ordnungen $\leq_i$, und sei $f : V_1 \to V_2$ ein Verbandshomomorphismus.*
Dann erhält f die Ordnung, d.h.: $x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$ für alle $x, y \in V_1$.

Beweis. Wenn $x \leq_1 y$, dann $x \wedge_1 y = x$. Daher $f(x) \wedge_2 f(y) = f(x \wedge_1 y) = f(x)$, also $f(x) \leq_2 f(y)$. □

Eine Kongruenzrelation ist eine Äquivalenzrelation $\theta \subseteq V \times V$, die mit den Operationen $\wedge$ und $\vee$ verträglich ist:

$$a_1 \theta a_2, b_1 \theta b_2 \;\Rightarrow (a_1 \vee b_1) \theta (a_2 \vee b_2),\ (a_1 \wedge b_1) \theta (a_2 \wedge b_2).$$

Aus dem allgemeinen Homomorphiesatz folgt, dass für jeden surjektiven Verbandshomomorphismus $f : V \to W$ die Relation $\{(x, y) \mid f(x) = f(y)\}$ eine Kongruenzrelation ist, und dass alle Kongruenzrelationen diese Form haben.
Es ist nicht immer leicht festzustellen, ob eine vorliegende Partition tatsächlich von einer Kongruenzrelation kommt. Das folgende Konzept kann manchmal hilfreich sein:

3.2.14 Definition. Sei $(L, \leq)$ eine partielle Ordnung. Eine Teilmenge $A \subseteq L$ heißt *konvex*, wenn $\forall a, b \in A\ \forall x \in L :\ a \leq x \leq b \Rightarrow x \in A$ gilt. Das heißt, mit allen Elementen $a, b \in A$ muss schon das ganze Intervall $[a, b] := \{x \in L \mid a \leq x \leq b\}$ eine Teilmenge von A sein.

3.2.15 Lemma. *Sei θ eine Kongruenzrelation auf einem Verband $(V, \wedge, \vee)$. Dann ist jede Kongruenzklasse eine konvexe Menge, und jede Kongruenzklasse ist Unterverband von V.*

Beweis. Sei $f : (V, \wedge, \vee) \to (W, \wedge, \vee)$ ein Homomorphismus, mit Kern θ. Jede Klasse $[v]_\theta$ ist von der Form $f^{-1}(w)$ für ein $w \in W$ (nämlich $w := f(v)$).

- Konvexität: Sei $a \leq x \leq b$ mit $f(a) = f(b)$. Zu zeigen ist $f(a) = f(x)$.
  Aus dem vorigen Lemma wissen wir $f(a) \leq f(x) \leq f(b) = f(a)$. Daher $f(a) = f(x)$.
- Unterverband: Seien v_1, v_2 in der selben Äquivalenzklasse, d.h. $f(v_1) = f(v_2) =: w$. Dann ist $f(v_1 \vee v_2) = w \vee w = w$, also ist $v_1 \vee v_2$ in derselben Klasse. Daher ist jede Klasse unter $\vee$ abgeschlossen; analog auch unter $\wedge$.

□

3.2.16 Anmerkung. Nicht jede Äquivalenzrelation, deren Klassen konvexe Unterverbände sind, ist eine Kongruenzrelation.

3.2.C Vollständige Verbände

3.2.17 Definition. Eine partielle Ordnung $(P, \leq)$ heißt *vollständig*, wenn jede Teilmenge $S \subseteq P$ ein Supremum und ein Infimum hat. (Statt $\sup S$ und $\inf S$ schreibt man manchmal auch $\bigvee S$ und $\bigwedge S$.) Wir nennen einen Verband $(L, \wedge, \vee)$ vollständig, wenn L mit der Verbandsordnung vollständig ist. (Vgl. auch 1.6.4.)

Insbesondere ist jede vollständige partielle Ordnung eine verbandsgeordnete Menge, kann also als vollständiger Verband aufgefasst werden.

3.2.18 Anmerkung. Die reellen Zahlen $\mathbb{R}$ mit der üblichen Ordnung sind im Sinne dieser Definition also nicht vollständig, die erweiterten reellen Zahlen $\mathbb{R} \cup \{-\infty, \infty\}$ schon. Wir[5] nennen eine partielle Ordnung „bedingt vollständig“[6], wenn jede nichtleere nach oben beschränkte Menge ein Supremum und jede nach unten beschränkte nichtleere Menge ein Infimum hat. Eine bedingt vollständige Halbordnung wird durch Adjunktion von zwei neuen Elementen ∞ und $-\infty$ zu einer vollständigen Halbordnung, daher kann man alle Sätze über vollständige Halbordnungen in Sätze über bedingt vollständige Halbordnungen übersetzen. Eine bedingt vollständige Halbordnung ist im Allgemeinen kein Verband. Die Familie aller endlichen Teilmengen von $\mathbb{N}$ ist ein Beispiel eines bedingt vollständigen Verbandes, der nicht vollständig ist.

3.2.19 Satz. *Sei $(P, \leq)$ eine Halbordnung, in der jede Teilmenge ein Infimum hat. Dann hat auch jede Teilmenge von P ein Supremum.* (*Vgl. auch* 1.6.5.)

Beweis. Übungsaufgabe 64. □

3.2.20 Beispiele.

1) Sei A eine Algebra. Die Menge aller Unteralgebren bildet einen vollständigen Verband. Das Infimum einer Familie von Unteralgebren ist einfach der Durchschnitt dieser Unteralgebren. (Übungsaufgabe 65)

2) Sei A eine Algebra. Die Menge aller Kongruenzrelationen $\theta \subseteq A \times A$ bildet einen vollständigen Verband. Das Infimum einer Familie von Kongruenzrelationen ist einfach der mengentheoretische Durchschnitt dieser Relationen. (Übungsaufgabe 68)

3.3 Boolesche Algebren

Bevor wir uns Booleschen Algebren widmen können, müssen ein paar weitere Begriffe für Verbände eingeführt werden.

3.3.1 Definition. Ein Verband $(V, \wedge, \vee)$ heißt *distributiv* :⇔ für alle $a, b, c \in V$ gilt:

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

wenn also $\wedge$ distributiv über $\vee$ und $\vee$ distributiv über $\wedge$ ist.

3.3.2 Anmerkung. $(V, \wedge, \vee)$ distributiver Verband ⇔ $(V, \vee, \wedge)$ distributiver Verband (Dualitätsprinzip).

3.3.3 Lemma. *Sei $(V, \wedge, \vee)$ ein Verband. Dann gilt:*

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

Beweis. $\Rightarrow$: $(a \vee b) \wedge (a \vee c) = \underbrace{[(a \vee b) \wedge a]}_{a} \vee [(a \vee b) \wedge c] = \underbrace{a \vee (a \wedge c)}_{a} \vee (b \wedge c) = a \vee (b \wedge c)$.

$\Leftarrow$: analog. □

Das bedeutet: Um zu überprüfen, ob ein Verband distributiv ist, muss man nur eines der beiden Distributivgesetze nachrechnen. Das andere gilt dann auch (allerdings nicht auf Grund des Dualitätsprinzips!).

3.3.4 Beispiel. $(\mathfrak{P}(M), \cap, \cup)$ ist ein distributiver Verband.

[5] Achtung! Manche Autoren verwenden den Namen „vollständig“ für die Eigenschaft, die wir hier „bedingt vollständig“ nennen.

[6] englisch: *conditionally complete*

3.3.5 Definition. Sei $(V, \wedge, \vee)$ ein Verband. Ein Element $0 \in V$ heißt ein *Nullelement* von $V :\Leftrightarrow \forall a \in V : a \vee 0 = a$ (d.h., 0 ist neutral bzgl. $\vee$). Ein Element $1 \in V$ heißt ein *Einselement* von $V :\Leftrightarrow \forall a \in V : 1 \wedge a = a$ (d.h., 1 ist neutral bzgl. $\wedge$).

3.3.6 Definition. Sei $(V, \wedge, \vee)$ ein Verband. Der Verband V heißt beschränkt, wenn es sowohl ein Nullelement als auch ein Einselement gibt.

3.3.7 Anmerkung. $\forall a \in V : a \vee 0 = a \Leftrightarrow \forall a \in V : a \wedge 0 = 0$, $\forall a \in V : 1 \wedge a = a \Leftrightarrow \forall a \in V : 1 \vee a = 1$.

3.3.8 Definition. Eine Algebra $(V, \wedge, \vee, 0, 1)$ vom Typ $(2, 2, 0, 0)$ heißt ein *Verband mit Null- und Einselement* (oder kurz $\{0,1\}$-*Verband*) $:\Leftrightarrow$

1) $(V, \wedge, \vee)$ ist ein Verband,

2) 0 ist Nullelement von V,

3) 1 ist Einselement von V.

3.3.9 Beispiel. $(\mathfrak{P}(M), \cap, \cup, \emptyset, M)$ ist ein Verband mit Null- und Einselement.

3.3.10 Definition. Ein Verband mit Null- und Einselement $(V, \wedge, \vee, 0, 1)$ heißt *komplementär* $:\Leftrightarrow \forall a \in V \; \exists a' \in V : a \wedge a' = 0$ und $a \vee a' = 1$. Jedes solche Element a' heißt ein *Komplement* von a.

3.3.11 Beispiel. $(\mathfrak{P}(M), \cap, \cup, \emptyset, M)$ ist ein komplementärer Verband, wobei für $A \subseteq M$ das Komplement durch $A' = M \setminus A$ gegeben ist.

3.3.12 Definition. Ein distributiver und komplementärer Verband $(V, \wedge, \vee, 0, 1)$ heißt ein *Boolescher Verband*.

3.3.13 Beispiel. $(\mathfrak{P}(M), \cap, \cup, \emptyset, M)$ ist ein Boolescher Verband.

3.3.14 Satz. *Ist* $(V, \wedge, \vee, 0, 1)$ *ein Boolescher Verband, so gibt es zu jedem* $a \in V$ *genau ein Komplement* a'.

Beweis. Seien a' und a^* Komplemente von a. Dann gilt $a \vee a' = 1 = a \vee a^*$, $a \wedge a' = 0 = a \wedge a^*$ und damit $a' = a' \vee 0 = a' \vee (a \wedge a^*) = (a' \vee a) \wedge (a' \vee a^*) = 1 \wedge (a' \vee a^*) = a' \vee a^*$. Also gilt $a^* \leq a'$, und aus Symmetriegründen erhält man auch $a' \leq a^*$, also $a^* = a'$. □

3.3.15 Definition. Eine Algebra $(B, \wedge, \vee, 0, 1, ')$ vom Typ $(2, 2, 0, 0, 1)$ heißt *Boolesche Algebra*[7] $:\Leftrightarrow$

1) $(B, \wedge, \vee, 0, 1)$ ist ein distributiver Verband mit Null- und Einselement,

2) $\forall a \in B : a \wedge a' = 0$ und $a \vee a' = 1$.

3.3.16 Anmerkung. $(B, \wedge, \vee, 0, 1, ')$ Boolesche Algebra $\Rightarrow$ $(B, \wedge, \vee, 0, 1)$ Boolescher Verband. Ist umgekehrt $(B, \wedge, \vee, 0, 1)$ Boolescher Verband und a' das (eindeutig bestimmte) Komplement von a, so ist $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra.
Manche Autoren verwenden für die Operationen $\vee$, $\wedge$ der Booleschen Algebra die Symbole $+$ und $\cdot$. Wir tun dies nicht, um Verwechslungen mit Booleschen Ringen (siehe nächster Abschnitt) zu vermeiden, und um die Verwandtschaft zu Verbänden zu betonen.

[7] englisch: *Boolean algebra*

Für das Komplement x' werden auch oft andere Symbole verwendet, wie x^c, $-x$, $\neg x$, $\sim x$, $\bar{x}$. Statt $a \wedge b'$ schreibt man manchmal in Analogie zu Mengenalgebren $a \setminus b$.

Dualitätsprinzip:

$$(B, \wedge, \vee, 0, 1, ') \text{ Boolesche Algebra} \Leftrightarrow (B, \vee, \wedge, 1, 0, ') \text{ Boolesche Algebra.}$$

3.3.17 Beispiel. $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ mit $A' = M \setminus A$ ist eine Boolesche Algebra.

3.3.18 Satz (Satz über Komplemente). *Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra. Dann gilt:*

a) $(a')' = a$ *für alle* $a \in B$.

b) $0' = 1$ *und* $1' = 0$.

c) $(a \vee b)' = a' \wedge b'$ *und* $(a \wedge b)' = a' \vee b'$ *für alle* $a, b \in B$ (de Morgan'sche Gesetze).

Beweis. a) $a \vee a' = 1$, $a \wedge a' = 0 \Longrightarrow a$ ist Komplement von a', aus der Eindeutigkeit des Komplements folgt $(a')' = a$.

b) $0 \vee 1 = 1$, $0 \wedge 1 = 0 \Longrightarrow 0' = 1$, $1' = 0$.

c) $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = 1 \wedge 1 = 1$, $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = 0 \vee 0 = 0 \Longrightarrow (a \vee b)' = a' \wedge b'$. Analog: $(a \wedge b)' = a' \vee b'$. □

3.3.19 Satz (Rechenregeln für Boolesche Algebren). *Sei B eine Boolesche Algebra. Dann gilt für alle $a, b \in B$:*

a) $a \leq b \;\Leftrightarrow\; b' \leq a'$. (*Man sagt auch, dass die Abbildung $a \mapsto a'$ antiton ist.*)

b) $a \leq b \;\Leftrightarrow\; a' \vee b = 1 \;\Leftrightarrow\; a \wedge b' = 0$.
In Analogie zur Logik wird der Ausdruck $a' \vee b$ manchmal auch mit $a \to b$ abgekürzt, d.h. $\to$ wird als Name einer 2-stelligen Operation verstanden.

c) $a \leq b' \;\Leftrightarrow\; a \wedge b = 0 \;\Leftrightarrow\; b \leq a'$.
Die Gleichung $a \wedge b = 0$ kürzt man (in Analogie zur linearen Algebra) auch mit $a \perp b$ ab. Die Elemente a und b heißen in so einem Fall „disjunkt“.

Beweis. a) Wir verwenden die Regel von de Morgan, sowie die Tatsache, dass man $x \leq y$ in äquivalenter Weise sowohl durch $x \wedge y = x$ als auch durch $x \vee y = y$ definieren kann: $a \leq b \;\Leftrightarrow\; a \wedge b = a \;\Leftrightarrow\; (a \wedge b)' = a' \;\Leftrightarrow\; a' \vee b' = a' \;\Leftrightarrow\; b' \leq a'$.

b) Wenn $a \leq b$, dann ist $a' \vee b = a' \vee (a \vee b) = 1$. Wenn umgekehrt $a' \vee b = 1$ ist, dann gilt:

$$a = a \wedge 1 = a \wedge (a' \vee b) = (a \wedge a') \vee (a \wedge b) = a \wedge b,$$

also $a \leq b$. Die zweite Äquivalenz folgt dann aus dem Gesetz von de Morgan.
c) folgt aus b). □

3.3.20 Satz (Satz über Homomorphismen). *Seien $(B, \wedge, \vee, 0, 1, ')$ und $(C, \wedge, \vee, 0, 1, ')$ Boolesche Algebren, $\varphi : B \to C$ surjektiv. Dann gilt: φ ist Homomorphismus von $(B, \wedge, \vee, 0, 1, ')$ nach $(C, \wedge, \vee, 0, 1, ')$ $\Leftrightarrow$ φ ist Homomorphismus von $(B, \wedge, \vee)$ nach $(C, \wedge, \vee)$. (D.h., es genügt, dass φ mit den Verbandsoperationen verträglich ist.)*

Beweis. $\Rightarrow$: trivial.
$\Leftarrow$: Wegen $0 \vee a = a$ gilt $\varphi(0) \vee \varphi(a) = \varphi(a)$ für alle $a \in B$. Da φ surjektiv ist, gilt $\varphi(0) \vee c = c$ für alle $c \in C$. Also ist $\varphi(0)$ neutral bezüglich $\vee$ in C und daher $\varphi(0) = 0$. Analog zeigt man $\varphi(1) = 1$.
φ ist verträglich mit $'$: $a \vee a' = 1$, $a \wedge a' = 0 \Rightarrow \varphi(a) \vee \varphi(a') = \varphi(1) = 1$, $\varphi(a) \wedge \varphi(a') = \varphi(0) = 0$ $\Rightarrow \varphi(a') = \varphi(a)'$. □

3.3.A Boolesche Ringe und Kongruenzen

3.3.21 Definition. Ein Ring $(R, +, 0, -, \cdot, 1)$ mit Einselement heißt *Boolescher Ring*, wenn $\forall x \in R: \; x \cdot x = x$ gilt.

3.3.22 Lemma. *In jedem Booleschen Ring gilt:*

1) $x + x = 0$ *für alle* $x \in R$, *d.h.,* $-x = x$,

2) $x \cdot y = y \cdot x$ *für alle* $x, y \in R$, *d.h.,* R *ist ein kommutativer Ring.*

Beweis. Ad 1. $x + 1 = (x + 1)(x + 1) = xx + x + x + 1 = (x + x) + (x + 1)$, nach Kürzen von $x + 1$ erhält man $x + x = 0$.
Ad 2. $x + y = (x + y)(x + y) = xx + xy + yx + yy = (x + y) + xy + yx$, nach Kürzen von $x + y$ erhält man $xy + yx = 0$ und durch Addieren von yx folgt mit 1. $xy = yx$. □

3.3.23 Satz.

(a) *Sei* $(R, +, 0, -, \cdot, 1)$ *ein Boolescher Ring. Mit den Operationen*

$$x \wedge y := xy, \qquad x \vee y := x + y + xy, \qquad x' := 1 + x \ (= 1 - x)$$

ist die Algebra $(R, \wedge, \vee, 0, 1, ')$ *eine Boolesche Algebra,*
und es gilt $x + y = (x \wedge y') \vee (x' \wedge y)$.

(b) *Sei* $(B, \wedge, \vee, 0, 1,')$ *eine Boolesche Algebra. Mit den Operationen*

$$x \cdot y := x \wedge y, \qquad x + y := (x \wedge y') \vee (x' \wedge y), \qquad -x := x$$

ist $(B, +, 0, -, \cdot, 1)$ *ein Boolescher Ring,*
und es gilt $x \vee y = x + y + xy = 1 + (1 + x)(1 + y)$.

(c) *Die in* (a) *und* (b) *beschriebenen Abbildungen zwischen Booleschen Algebren und Booleschen Ringen sind invers zueinander.*

Weiters gilt: Seien $(R_i, +, 0, -, \cdot, 1)$ *(für* $i = 1, 2$*) Boolesche Ringe, mit zugehörigen Booleschen Algebren* $(R_i, \wedge, \vee, 0, 1, ')$. *Eine Abbildung* $f : R_1 \to R_2$ *ist genau dann Ringhomomorphismus, wenn sie ein Homomorphismus von Booleschen Algebren ist.*

Beweis. Übungsbeispiele 70 – 72. □

3.3.24 Anmerkung. Die Operation $x + y = (x \wedge y') \vee (y \wedge x')$ heißt auch „symmetrische Differenz"; sie wird manchmal $x \,\Delta\, y$ geschrieben.

Jede Kongruenzrelation $\sim$ auf einem Ring, erst recht also auf jedem Booleschen Ring, ist durch ein Ideal charakterisiert, nämlich die Äquivalenzklasse von 0. Da die Ringoperationen durch die Operationen der Booleschen Algebra beschrieben werden (und umgekehrt), sind die Kongruenzrelationen eines Booleschen Rings genau die Kongruenzrelationen der entsprechenden Booleschen Algebra. Die Ringkongruenzen kann man durch Ringideale beschreiben; wir wollen diese Ideale nun auch ordnungstheoretisch charakterisieren.

3.3.25 Definition. Sei B Boolesche Algebra. Eine nichtleere Teilmenge $I \subseteq B$ heißt Ideal, wenn gilt

(i) $i \in I$ und $x \leq i \Rightarrow x \in I$,

(ii) $i_1, i_2 \in I \Rightarrow i_1 \vee i_2 \in I$.

3.3.26 Satz. *Sei* $\mathfrak{B}_{\mathrm{BA}} = (B, \wedge, \vee, 0, 1, ')$ *eine Boolesche Algebra und* $\mathfrak{B}_{\mathrm{R}} = (B, +, 0, -, \cdot, 1)$ *der assoziierte Boolesche Ring.*

(a) *Eine Teilmenge* $I \subseteq B$ *ist genau dann ein Ideal (im gerade definierten Sinn) in der Booleschen Algebra* $\mathfrak{B}_{\mathrm{BA}}$, *wenn* I *ein Ideal (im ringtheoretischen Sinn) des assoziierten Booleschen Rings* $\mathfrak{B}_{\mathrm{R}}$ *ist.*

(b) *Ist* I *ein Ideal in* $\mathfrak{B}_{\mathrm{BA}}$ *(bzw.* $\mathfrak{B}_{\mathrm{R}}$*), dann gilt für die zugehörige Kongruenz* θ*:*

$$x\theta y \overset{\text{(I)}}{\Leftrightarrow} x + y \in I \overset{\text{(II)}}{\Leftrightarrow} \exists i \in I : \ x \vee i = y \vee i$$

Beweis. (a) $\Rightarrow$: Weil $I \neq \emptyset$ und $0 \leq i$ für $i \in I$ folgt $0 \in I$. Für $i_1, i_2 \in I$ gilt $i_1 \wedge i_2' \leq i_1 \in I$, also ist $i_1 \wedge i_2' \in I$ wegen der Idealeigenschaft (i); analog folgt $i_1' \wedge i_2 \in I$, und daraus erhält man mit der Idealeigenschaft (ii)

$$i_1 - i_2 = i_1 + i_2 = (i_1 \wedge i_2') \vee (i_1' \wedge i_2) \in I.$$

Für $i \in I$ und $x \in B$ gilt $x \cdot i = x \wedge i \leq i \in I$, also folgt wieder mit (i) $x \cdot i \in I$. Das zeigt insgesamt, dass I ein Ideal im Ring $\mathfrak{B}_{\mathrm{R}}$ ist.
$\Leftarrow$: (i) $i \in I$ und $x \leq i \Rightarrow x = x \wedge i = x \cdot i \in I$. (ii) $i_1, i_2 \in I \Rightarrow i_1 + i_2, i_1 \cdot i_2 \in I \Rightarrow i_1 \vee i_2 = (i_1 + i_2) + i_1 \cdot i_2 \in I$.

(b) Die Äquivalenz (I) gilt für jede Kongruenz in einem Ring, also auch im Booleschen Ring $\mathfrak{B}_{\mathrm{R}}$ (man beachte $x + y = x - y$).
(II) $\Rightarrow$: Für $i = x + y \in I$ gilt:

$$x \vee i = x \vee (x + y) = x \vee ((x \wedge y') \vee (x' \wedge y)) = x \vee (x' \wedge y) = x \vee y,$$

analog rechnet man $y \vee i = x \vee y$ nach, also erhält man $x \vee i = y \vee i$.

$\Leftarrow$: Wir zeigen $x + y \leq i$, woraus dann $x + y \in I$ aus Idealeigenschaft (ii) folgt: $x = x \wedge (x \vee i) = x \wedge (y \vee i) = (x \wedge y) \vee (x \wedge i)$; durch Schneiden mit y' erhalten wir $x \wedge y' = x \wedge y' \wedge i$, also $x \wedge y' \leq i$; analog erhält man $x' \wedge y = x' \wedge y \wedge i$, also $x' \wedge y \leq i$; aus diesen beiden Eigenschaften folgt $x + y = (x \wedge y') \vee (x' \wedge y) \leq i$. $\square$

3.3.27 Beispiel. Sei $B = \mathfrak{P}(\mathbb{N})$ die Potenzmenge der natürlichen Zahlen. Mit den Operationen $\cup$, $\cap$ wird B zu einer Booleschen Algebra ($1 = \mathbb{N}$, etc.).

Man prüft leicht nach, dass die Famile aller endlichen Teilmengen von $\mathbb{N}$ ein Ideal in B bildet. Die zugehörige Kongruenzrelation θ sieht so aus: für $X, Y \subseteq \mathbb{N}$ gilt $X\theta Y$ genau dann, wenn $\exists n \in \mathbb{N} : X \cap [n, \infty) = Y \cap [n, \infty)$, d.h., wenn X und Y bis auf endlich viele Elemente übereinstimmen.

3.3.28 Beispiel. Sei B die Famile aller Borelmengen $X \subseteq [0, 1]$. B ist Boolesche Algebra (mit den üblichen Operationen $\cup, \cap, \ldots$). Sei λ das Lebesguemaß.

Sei $I := \{X \in B \mid \lambda(X) = 0\}$, die Familie der Nullmengen. Dann gilt in der zugehörigen Kongruenz $X\theta Y$ genau dann, wenn X und Y „bis auf eine Lebesgue-Nullmenge“ übereinstimmen.

3.3.B Endliche Boolesche Algebren

3.3.29 Definition. Sei $(V, \wedge, \vee, 0, 1)$ ein Verband mit 0- und 1-Element. Dann heißt $a \in V$ ein *Atom* $:\Leftrightarrow$

1) $0 < a$ und

2) $0 \leq b \leq a \Rightarrow b = 0 \vee b = a$

(d.h., a ist ein oberer Nachbar von 0).

3.3.30 Lemma (Rechenregeln für Atome). *Sei B Boolesche Algebra, $a \in B$ ein Atom. Dann gilt für alle $b, c \in B$:*

(A1) *$a \leq b$ genau dann, wenn $a \wedge b \neq 0$. Anders gesagt: $a \not\leq b \;\Leftrightarrow\; a \wedge b = 0$.*

(A2) *$a \leq b'$ genau dann, wenn $a \not\leq b$.*

(A3) *$a \leq b \wedge c$ genau dann, wenn $a \leq b$ und $a \leq c$.*

(A4) *$a \leq b \vee c$ genau dann, wenn $a \leq b$ oder $a \leq c$.*

Beweis.

(A1) $a \wedge b \leq a$, daher kann $a \wedge b$ nur die Werte 0 und a annehmen. Daher $a \wedge b \neq 0 \Leftrightarrow a \wedge b = a \Leftrightarrow a \leq b$.

(A2) $a \leq b' \Leftrightarrow a \wedge b = 0$ gilt für beliebige a, b. Wenn aber a Atom ist, gilt mit (A1):

$$a \leq b' \quad \Leftrightarrow \quad a \wedge b = 0 \quad \Leftrightarrow \quad a \not\leq b.$$

(A3) Dies gilt sogar für beliebige $a, b, c \in B$ (und sogar in jedem Verband).

(A4) Wir zeigen statt dessen $a \not\leq b \vee c \;\Leftrightarrow\; a \not\leq b$ und $a \not\leq c$. Wir verwenden das Distributivgesetz $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ sowie Rechenregel (A1):

$$a \not\leq b \vee c \;\Leftrightarrow\; (a \wedge b) \vee (a \wedge c) = 0 \;\Leftrightarrow\; a \wedge b = 0 \text{ und } a \wedge c = 0 \;\Leftrightarrow\; a \not\leq b \text{ und } a \not\leq c.$$

□

3.3.31 Anmerkung. Die Regeln (A2), (A3), (A4) geben eine Korrespondenz zwischen den algebraischen Operationen $'$, $\wedge$, $\vee$ und den logischen Junktoren „nicht", „und", „oder". Im nächsten Satz übersetzen wir diese logischen Junktoren in die mengentheoretischen Operationen $'$, $\cap$ und $\cup$.

3.3.32 Lemma. *Sei $(B, \wedge, \vee, 0, 1, ')$ eine endliche Boolesche Algebra. Dann gibt es zu jedem Element $b \in B \setminus \{0\}$ ein Atom $a \in B$ mit $a \leq b$. (Dies gilt sogar für beliebige endliche Verbände.)*

Beweis. Sei $b \in B \setminus \{0\}$. Ist b Atom, so kann man $a = b$ setzen. Ist b kein Atom, so gibt es ein $b_1 \in B$ mit $0 < b_1 < b$. Ist b_1 Atom, so kann man $a = b_1$ setzen. Andernfalls setzt man das Verfahren fort und erhält eine Kette $b > b_1 > b_2 > \ldots$, die, da B endlich ist, bei einem b_i abbrechen muss. Dann setzt man $a = b_i$. □

3.3.33 Satz (Satz von Stone für endliche Boolesche Algebren). *Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra und $M := \{a \in B \mid a \text{ Atom von } B\}$.*
Sei $\varphi : B \to \mathfrak{P}(M)$ gegeben durch $\varphi(b) := \{a \in M \mid a \leq b\}$.
Dann gilt:

- *φ ist Homomorphismus von Booleschen Algebren.*
- *Wenn B endlich ist, dann ist φ Isomorphismus der Booleschen Algebren B und $\mathfrak{P}(M)$.*

Beweis. Da $\varphi(b) \subseteq M$, ist φ wohldefiniert.

- $\varphi(b') = M \setminus \varphi(b)$:

$$\begin{aligned} a \in \varphi(b') &\Leftrightarrow a \leq b' \\ &\Leftrightarrow a \not\leq b \quad \text{wegen Rechenregel A2} \\ &\Leftrightarrow a \notin \varphi(b) \\ &\Leftrightarrow a \in M \setminus \varphi(b) \end{aligned}$$

- $\varphi(b \vee c) = \varphi(b) \cup \varphi(c)$:

$$\begin{aligned} a \in \varphi(b \vee c) &\Leftrightarrow a \leq b \vee c \\ &\Leftrightarrow a \leq b \text{ oder } a \leq c \quad \text{wegen Rechenregel A4} \\ &\Leftrightarrow a \in \varphi(b) \text{ oder } a \in \varphi(c) \\ &\Leftrightarrow a \in \varphi(b) \cup \varphi(c) \end{aligned}$$

- $\varphi(b \wedge c) = \varphi(b) \cap \varphi(c)$: Analog, mit Hilfe der Rechenregel A3.
- Wenn B endlich ist, dann ist φ surjektiv:

  Sei $U \in \mathfrak{P}(M)$, d.h., $U \subseteq M$. Weil U endlich ist, können wir das Supremum von U bilden: Sei $U = \{a_1, \ldots, a_r\}$ und $b := a_1 \vee \cdots \vee a_r = \sup U$. Dann gilt $\varphi(b) = \varphi(a_1 \vee \cdots \vee a_r) = \varphi(a_1) \cup \cdots \cup \varphi(a_r) \overset{a_i \text{ Atome}}{=} \{a_1\} \cup \cdots \cup \{a_r\} = U$.
- φ ist injektiv (d.h., $b \neq c \Rightarrow \varphi(b) \neq \varphi(c)$). Da φ auch ein Ringhomomorphismus ist, genügt es, $\ker(\varphi) = \{0\}$ zu zeigen: Wenn $b \in \ker(\varphi)$, dann ist $\varphi(b) = \emptyset$, d.h. es gibt kein Atom $a \leq b$. Nach dem gerade bewiesenen Lemma muss $b = 0$ sein.

□

3.3.34 Anmerkungen. 1) $|M| = |M_1| \Rightarrow (\mathfrak{P}(M), \cap, \cup, \emptyset, M, ') \cong (\mathfrak{P}(M_1), \cap, \cup, \emptyset, M_1, ')$.

2) $|M| = n \in \mathbb{N}_0 \Rightarrow |\mathfrak{P}(M)| = 2^n$.

3.3.35 Folgerung. Ist B endliche Boolesche Algebra, dann gilt $|B| = 2^n$ für ein $n \in \mathbb{N}_0$. Zu jedem $n \in \mathbb{N}_0$ gibt es somit — bis auf Isomorphie — genau eine Boolesche Algebra mit 2^n Elementen, nämlich $\mathfrak{P}(\{0, 1, \ldots, n-1\})$.

Dieser Satz kann — geeignet modifiziert — auf beliebige Boolesche Algebren verallgemeinert werden. Man kann dabei nicht erwarten, dass jede Boolesche Algebra zu einer Potenzmengenalgebra isomorph ist; es gibt nämlich abzählbar unendliche Boolesche Algeben, während die Potenzmenge einer Menge nicht abzählbar unendlich sein kann: die Potenzmenge jeder endlichen Menge ist endlich, und die Potenzmenge jeder unendlichen Menge ist überabzählbar.

3.3.36 Definition. Sei M Menge. Eine Menge $\mathfrak{K} \subseteq \mathfrak{P}(M)$ heißt *Mengenkörper*[8] $:\Leftrightarrow$ für alle $A, B \in \mathfrak{K}$ gilt

[8] englisch: *field of sets*

1) $A \cup B \in \mathfrak{K}$,

2) $A \cap B \in \mathfrak{K}$,

3) $A' \in \mathfrak{K}$,

4) $A \cap B' = A \setminus B \in \mathfrak{K}$,

5) $M \in \mathfrak{K}$.

3.3.37 Beispiel. $\mathfrak{P}(M)$ ist Mengenkörper. Auch $\{M, \emptyset\}$ ist Mengenkörper.

3.3.38 Anmerkung. Die Liste 1) – 5) ist redundant. Aus 4) und 5) folgen bereits die Bedingungen 1), 2), 3). Ebenso folgen, wenn man $\mathfrak{K} \neq \emptyset$ voraussetzt, aus 3) und 4) die übrigen Bedingungen, oder aus 1) und 3), oder auch aus 2) und 3).

3.3.39 Definition. Sei $\mathfrak{K} \subseteq \mathfrak{P}(M)$ ein Mengenkörper. Dann heißt die Boolesche Algebra $(\mathfrak{K}, \cap, \cup, \emptyset, M, ')$ eine *Mengenkörperalgebra*.

(Oft wird in der Notation nicht zwischen der Menge $\mathfrak{K}$ und der Booleschen Algebra $(\mathfrak{K}, \cap, \cup, \emptyset, M, ')$ unterschieden, und beide werden mit „Mengenkörper“ bezeichnet.)

Eine Mengenkörperalgebra ist also eine Unteralgebra von $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$.
Die folgenden Beispiele zeigen, dass eine Mengenkörperalgebra Atome haben kann, aber nicht haben muss.

3.3.40 Beispiele. 1) Sei $(0, 1]$ das halboffene Intervall der reellen Zahlengeraden und $\mathfrak{K} \subseteq \mathfrak{P}((0, 1])$ gegeben durch $\mathfrak{K} := \{\emptyset\} \cup \{\bigcup_{1 \leq i \leq n}(a_i, b_i] \mid 0 \leq a_i < b_i \leq 1,\ n \in \mathbb{N}\}$. Dann ist $\mathfrak{K}$ Unteralgebra von $(\mathfrak{P}((0, 1]), \cap, \cup, \emptyset, (0, 1], ')$. $\mathfrak{K}$ enthält keine Atome.

2) Sei X eine beliebige unendliche Menge; sei I die Menge aller endlichen Teilmengen von X, und sei $F := I^* = \{X \setminus A \mid A \in I\}$ die Menge der „ko-endlichen“ Teilmengen von X. Dann ist $I \cup F$ eine Unteralgebra von $(\mathfrak{P}(X), \cap, \cup, \emptyset, X, ')$. I ist nämlich unter Schnitten und Vereinigungen abgeschlossen, daher auch F: wenn nämlich $x, y \in F$, dann $x', y' \in I$, also $x' \cup y' \in I$, daher $x \cap y = (x' \cup y')' \in F$. Das Komplement jedes Elements von I liegt in F, und umgekehrt.
Die Atome von $I \cup F$ sind genau die einelementigen Teilmengen von X.

Es gilt der folgende Darstellungssatz[9]:

3.3.41 Satz (von Stone). *Jede Boolesche Algebra ist isomorph zu einer Mengenkörperalgebra.*

[9] Ein Darstellungssatz ist ein Satz, der aussagt, dass jede abstrakte Struktur mit gewissen Eigenschaften isomorph zu einer „konkreten“ (mehr oder weniger bekannten) Struktur ist. Der Cayley'sche Satz für Gruppen besagt, dass jede „abstrakte“ Gruppe zu einer Gruppe von Bijektionen einer Menge isomorph ist; diese Gruppe ist insofern „konkret“, als die Gruppenoperation auf dieser Menge einfach die Verknüpfung von Abbildungen ist.

Der Darstellungssatz von Stone identifiziert jede Boolesche Algebra mit einer Unteralgebra der Potenzmengenalgebra; die Potenzmengenalgebra ist insofern konkret, als die Verbandsoperationen die mengentheoretischen Operationen $\cup$ und $\cap$ sind.

In der linearen Algebra haben Sie einen Darstellungssatz für Vektorräume kennengelernt. Zum Beispiel ist jeder n-dimensionale Vektorraum über dem Körper K zum Vektorraum K^n isomorph, in welchem die Operationen (Addition, Skalarmultiplikation) konkret durch die Körperoperationen in den einzelnen Komponenten gegeben werden.

3.3.42 Anmerkung. $\mathfrak{P}(M) \cong \{0,1\}^M$ (direkte Potenz). (Jeder Teilmenge wird ihre charakteristische Funktion zugeordnet.) Aus dem Satz von Stone folgt daher: Jede Boolesche Algebra B ist isomorph zu einer Unteralgebra einer Potenz $\{0,1\}^M$. Jedes Gesetz, welches in der Booleschen Algebra $\{0,1\}$ mit den Operationen

$$\begin{array}{c|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \qquad \begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad \begin{array}{c|c} ' & \\ \hline 0 & 1 \\ 1 & 0 \end{array}$$

gilt, muss daher in allen Booleschen Algebren gelten!

3.3.43 Anmerkung. Ein analoger Sachverhalt gilt auch für distributive Verbände. Dazu definieren wir: $\mathfrak{V} \subseteq \mathfrak{P}(M)$ heißt *Mengenverband* $:\Leftrightarrow$ für alle $A, B \in \mathfrak{V}$ gilt $A \cap B, A \cup B \in \mathfrak{V}$. Es gilt dann (ohne Beweis): Jeder distributive Verband ist isomorph zu einem Mengenverband. Daraus folgt wieder: Jedes Gesetz, welches im distributiven Verband $\{0,1\}$ mit den obigen Operationen $\wedge, \vee$ gilt, muss in allen distributiven Verbänden gelten.