4. Algebraische Strukturen

Definition (4.1) Sei M eine Menge. Eine Abbildung $\circ : M \times M \to M$ heißt eine *(zweistellige) Verknüpfung* in M. Man schreibt für die Bilder einer Verknüpfung $a \circ b := \circ(a, b)$ mit $a, b \in M$.

Eine Verknüpfung $\circ$ heißt

kommutativ $:\Leftrightarrow$ $\forall\, a, b \in M\, :\, a \circ b = b \circ a$

assoziativ $:\Leftrightarrow$ $\forall\, a, b, c \in M\, :\, a \circ (b \circ c) = (a \circ b) \circ c.$

Eine Menge M zusammen mit k Verknüpfungen $\circ_1, \dots, \circ_k$ nennt man eine *algebraische Struktur* und schreibt dafür $(M, \circ_1, \dots, \circ_k)$.

Beispiele (4.2)

a) $(\mathbb{N},+,\cdot)$, $(\mathbb{R},+,\cdot)$

b) $F := M^M := \{f|\, f : M \to M \text{ Abbildung}\}$ zusammen mit der Komposition $\circ$ von Abbildungen als Verknüpfung: $(F,\circ)$.

c) Die Menge der reellen (n,n)-Matrizen zusammen mit Addition und Matrizenmultiplikation $(\mathbb{R}^{(n,n)},+,\cdot)$.

d) Sei Π die Menge der reellen Polynome. An Verknüpfungen hat man Addition, Multiplikation und die Hintereinanderausführung: $(\Pi,+,\cdot,\circ)$.

e) Zu einer Menge M ist $(\mathcal{P}(M),\cup,\cap,\setminus)$ eine algebraische Struktur.

Definition (4.3)

Eine algebraische Struktur $(G, \circ)$ mit einer assoziativen Verknüpfung $\circ$ heißt eine *Halbgruppe*. Gilt darüber hinaus

$$
\begin{array}{lll}
\exists\, e \in G\ \forall\, a \in G & : & e \circ a = a \circ e = a \qquad \textit{(neutrales Element)}, \\
\forall\, a \in G\ \exists\, a^{-1} \in G & : & a \circ a^{-1} = a^{-1} \circ a = e \quad \textit{(inverses Element)},
\end{array}
$$

so nennt man $(G, \circ)$ eine *Gruppe*. Eine Gruppe heißt *abelsch*, falls die Verknüpfung $\circ$ kommutativ ist.

Beispiele (4.4)

a) Es bezeichne $S(M)$ die Menge aller bijektiven Abbildungen $M \to M$. $(S(M), \circ)$, ist dann eine Gruppe (die *symmetrische Gruppe*) mit neutralem Element id_M. I.Allg. ist diese Gruppe nichtkommutativ.

b) $(\mathbb{R}, +)$ ist abelsche Gruppe mit neutralem Element 0.

c) $(\mathbb{N}, +)$, $(\mathbb{R}, \cdot)$ sind Halbguppen, aber keine Gruppen.

Definition (4.5) (Homomorphismen)

Seien $(M, \circ_1, \ldots, \circ_k)$ und $(N, \star_1, \ldots, \star_k)$ algebraische Strukturen. Eine Abbildung $\Phi : M \to N$ heißt *Homomorphismus*, falls gelten:

$$\forall\, i \in \{1, \ldots, k\}\ \forall\, a, b \in M\ :\ \Phi(a \circ_i b) \ = \ \Phi(a) \star_i \Phi(b).$$

Homomorphismen bezeichnet man auch als *strukturerhaltende Abbildungen*.

Ein bijektiver Homomorphismus heißt ein *Isomorphismus*. Ein Isomorphismus $\Phi : M \to M$ einer algebraischen Struktur in sich heißt auch *Automorphismus*.

Beispiele (4.6)

a) Der natürliche Logarithmus $\ln : \mathbb{R}^+ \to \mathbb{R}$ ist ein Homomorphismus zwischen den algebraischen Strukturen $(\mathbb{R}^+, \cdot)$ und $(\mathbb{R}, +)$. Es gilt bekanntlich das Logarithmengesetz $\ln(xy) = \ln x + \ln y$ für $x, y \in \mathbb{R}^+$. ln ist sogar ein Isomorphismus.

b) Die Umkehrabbildung $\exp : (\mathbb{R},+) \to (\mathbb{R}^+,\cdot)$ ist ebenso ein Isomorphismus mit $\exp(x+y) = \exp(x)\cdot\exp(y)$.

c) Die Determinante von (n,n)–Matrizen ist ein Homomorphismus $\det : (\mathbb{R}^{(n,n)},\cdot) \to (\mathbb{R},\cdot)$, denn es gilt der Determinaten-Multiplikationssatz $\det(A\cdot B) = \det A \cdot \det B$. Die Abbildung det ist (für $n > 1$) nicht bijektiv, also auch kein Isomorphismus.

d) Die Komplementbildung $\overline{\cdot} : (\mathcal{P}(M),\cup) \to (\mathcal{P}(M),\cap)$ mit $\overline{A} := M \setminus A$ ist ein Homomorphismus, da ja $\overline{A\cup B} = \overline{A}\cap\overline{B}$ gilt. Da ferner $\overline{\overline{A}} = A$ gilt, ist die Komplementbildung auch bijektiv, also ein Isomorphismus.

e) Die Quadratbildung in der Menge der komplexen Zahlen, $f : (\mathbb{C},\cdot) \to (\mathbb{C},\cdot)$, definiert durch $f(z) := z^2$, $z \in \mathbb{C}$, ist ein Homomorphismus, denn es gilt ja $(zw)^2 = z^2\,w^2$.

Definition (4.7) (Verband, Boolesche Algebra)

a) Eine algebraische Struktur $(V, \wedge, \vee)$ heißt *Verband*, falls gelten

I) Beide Verknüpfungen $\wedge$ und $\vee$ erfüllen das Kommutativ- und das Assoziativgesetz.

II) Es gelten die Absorptionsgesetze

$$\begin{aligned} \forall\, a, b \in V &: \quad a \wedge (a \vee b) = a \\ \forall\, a, b \in V &: \quad a \vee (a \wedge b) = a \end{aligned}$$

b) Einen Verband heißt *distributiv*, falls beide Distributivgesetze erfüllt sind:

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

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

$$\begin{aligned} \forall\, a \in V \ &: \ 0 \wedge a = 0, \quad 0 \vee a = a \\ \forall\, a \in V \ &: \ 1 \wedge a = a, \quad 1 \vee a = 1. \end{aligned}$$

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

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

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

Beispiele (4.8):

a) Sei M eine Menge. Nach den Regeln der Mengenalgebra (2.10) ist $(\mathcal{P}(M), \cap, \cup)$ ein distributiver Verband.

Es gibt ferner ein Nullelement $\emptyset$ und ein Einselement M. Der Verband ist auch komplementär mit $\overline{A} = M \backslash A$, also ist $(\mathcal{P}(M), \cap, \cup)$ eine Boolesche Algebra.

b) $(\mathbb{N}, \text{ggT}, \text{kgV})$ 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 (4.9)

Ist $(V, \wedge, \vee)$ Verband, so gelten die *Idempotenzgesetze*

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

Beweis:

$$\begin{aligned} a \wedge a &= a \wedge (a \vee (a \wedge a)) && \text{(Absorption)} \\ &= a \wedge (a \vee b) && (b := a \wedge a) \\ &= a. && \text{(Absorption)} \end{aligned}$$

Hiermit folgt ferner: $a \vee a = a \vee (a \wedge a) = a.$ $\square$

Satz (4.10) (Eindeutigkeit von 0, 1 und $\overline{a}$)

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: **zu a)**: Sind 0 und $\tilde{0}$ zwei Nullelemente, so gelten $0 \wedge \tilde{0} = 0$ und $\tilde{0} \wedge 0 = \tilde{0}$, also (Kommutativgesetz) $0 = \tilde{0}$.

zu b): Zu zeigen: $(a \wedge b = a \wedge c) \ \wedge \ (a \vee b = a \vee c) \ \Rightarrow \ b = c$.
Aufgrund des Absorptionsgesetzes gilt $b = b \vee (a \wedge b)$.
Nach Voraussetzung ist $a \wedge b = a \wedge c$. Anwendung des Distributivgesetzes ergibt $b = (b \vee a) \wedge (b \vee c) = (a \vee b) \wedge (b \vee c)$.

Wieder nach Voraussetzung gilt $a \vee b = a \vee c$ und somit $b = (a \vee c) \wedge (b \vee c) = (a \wedge b) \vee c$. Mit Hilfe der Voraussetzung und des Absorptionsgesetzes ergibt sich schliesslich $b = (a \wedge b) \vee c = (a \wedge c) \vee c = c$.

zu c): Sind $\overline{a}$ und $\tilde{a}$ zwei komplementäre Elemente zu a, so folgt

$$a \wedge \overline{a} = a \wedge \tilde{a} = 0$$
$$a \vee \overline{a} = a \vee \tilde{a} = 1.$$

Aus der Kürzungsregel ergibt sich direkt $\overline{a} = \tilde{a}$. Die weiteren Aussagen (doppeltes Komplement, de Morgansche Regeln) sind zur Übung empfohlen. □

Verbände und verbandsgeordnete Mengen.

Definition (4.10): Ist $(V, \leq)$ eine geordnete Menge und existiert zu beliebigen $a, b \in V$ stets $\inf(a, b)$ und $\sup(a, b)$, vgl. (3.14), so heißt $(V, \leq)$ eine *verbandsgeordnete Menge*.

Wir zeigen nun, dass Verbände und verbandsgeordnete Mengen im Wesentlichen dasselbe sind.

Satz (4.11)

a) Ist $(V, \wedge, \vee)$ ein Verband, so definiert man $a \leq b :\Leftrightarrow a \wedge b = a$. Dann ist $(V, \leq)$ eine verbandsgeordnete Menge und es gilt

$$a \wedge b = \inf(a, b), \quad a \vee b = \sup(a, b)$$

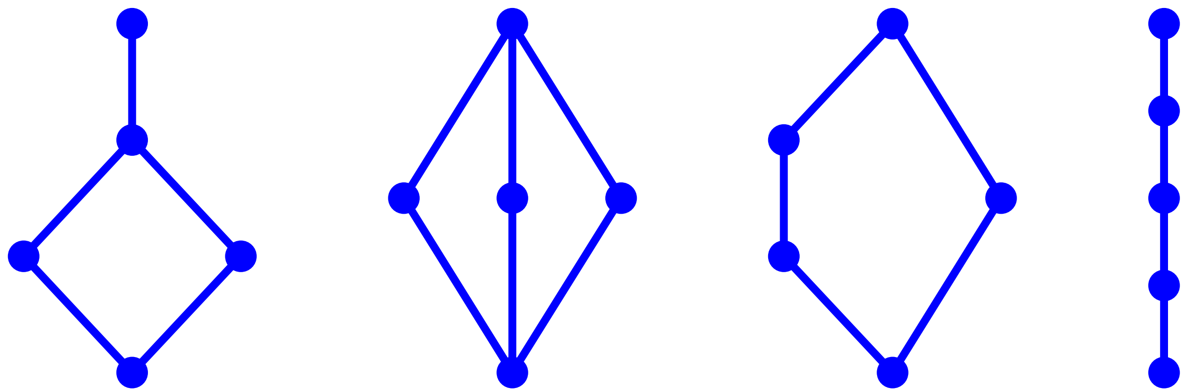
b) Ist umgekehrt $(V, \leq)$ eine verbandsgeordnete Menge, so definiert man die beiden Verknüpfungen $\wedge$ und $\vee$ vermöge

$$a \wedge b := \inf(a, b), \quad a \vee b := \sup(a, b).$$

Dann ist $(V, \wedge, \vee)$ ein Verband und es gilt:

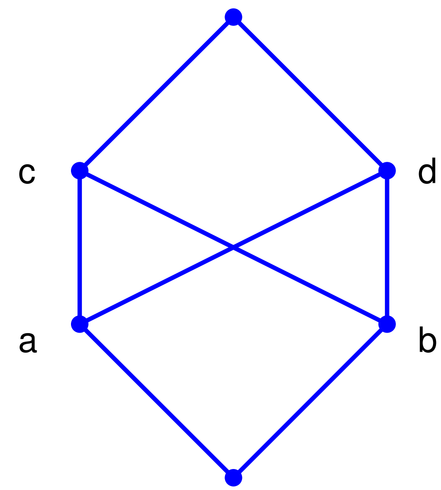
$$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b.$$

Aufgrund des obigen Satzes lassen sich endliche Verbände durch die Hasse-Diagramme der zugehörigen verbandsgeordneten Mengen graphisch darstellen. Die Eigenschaft, dass $\sup(a,b)$ und $\inf(a,b)$ existieren, bedeutet, dass je zwei Punkte des Hasse-Diagramms *eindeutig nach oben und nach unter verbunden* sind. Dies erklärt den Namen Verband. Beispiele mit fünf Elementen sind



Diamant Pentagon

Das folgende Hasse-Diagramm definiert dagegen keinen Verband, da beispielsweise inf(c, d) nicht existiert.



Beweis zu (4.11):

zu a) Sei $(V, \wedge, \vee)$ ein Verband und es werde definiert $a \leq b :\Leftrightarrow a \wedge b = a$. Dann ist $\leq$ eine Ordnung. Denn: $a \leq a$ gilt wegen (4.9). Weiter, ist $a \leq b$ und $b \leq a$, so folgt aus der Definition $a = a \wedge b = b \wedge a = b$. Schließlich folgt aus $a \leq b$ und $b \leq c$, dass $a \wedge b = a$ und $b \wedge c = b$ ist und somit mit dem Absorptionsgesetz

$$a \vee b \;=\; b \vee a \;=\; b \vee (a \wedge b) \;= b,$$

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

womit $a \leq c$ gezeigt ist. Zugleich haben wir gesehen

$$a \wedge b \;=\; a \;\Leftrightarrow\; a \vee b \;=\; b. \tag{$*$}$$

Seien nun $a, b \in V$; wir zeigen $a \wedge b = \inf(a, b)$. Zunächst folgt wieder mit dem Absortionsgesetz und $(*)$

$$(a \wedge b) \vee a \;=\; a \;\Leftrightarrow\; (a \wedge b) \wedge a \;=\; (a \wedge b) \;\Leftrightarrow\; a \wedge b \;\leq a.$$

Analog zeigt man $a \wedge b \leq b$, so dass $a \wedge b$ eine untere Schranke von a, b ist. Ist c nun eine beliebige untere Schranke von a, b, so gelten $c \wedge a = c$, $c \vee a = a$, $c \wedge b = c$ und $c \vee b = b$ und somit

$$c \wedge (a \wedge b) \;=\; (c \wedge a) \wedge b \;=\; c \wedge b \;=\; c,$$

d.h. $c \leq (a \wedge b)$. Damit ist $a \wedge b$ die größte untere Schranke, also

$a \wedge b = \inf(a,b)$. Analog sieht man: $a \vee b = \sup(a,b)$.

zu b) Sei umgekehrt $(V, \leq)$ eine verbandsgeordnete Menge. Dann gelten

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

sowie die analogen Ausssagen für $\vee$. Weiter gelten

$$a \wedge (a \vee b) = \inf(a, \sup(a,b)) = a, \quad a \vee (a \wedge b) = \sup(a, \inf(a,b)) = a.$$

Damit ist gezeigt, dass $(V, \wedge, \vee)$ ein Verband ist. Der Zusatz folgt aus $(*)$. $\square$

Sieht man sich die obigen Beweise und auch die Verbandsaxiome genauer an, so stellt man völlige Symmetrie bezüglich der Operationen $\wedge$ und $\vee$ fest. Hieraus resultiert das so genannte *Dualitätsprinzip der Verbandstheorie*.

Satz (4.12) (Dualitätsprinzip)

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 (4.13)

a) Besitzt ein Verband V ein Null– und Einselement, so gilt: $0 = \min V$ und $1 = \max V$.

b) Jeder *endliche* Verband besitzt ein Null– und ein Einselement.

Beweis:

zu a) Aus den definierenden Eigenschaften eines Null-/Einselementes folgt für alle $a \in V$: $0 = \inf(0, a)$ und $1 = \sup(1, a)$. Hieraus ergibt sich die Behauptung.

zu b) Sei $V = \{x_1, \ldots, x_n\}$. Durch den folgenden Algorithmus lassen sich Null- und Einselement berechnen

$$\begin{array}{l} u := v := x_1, \\ \text{for } k = 2, 3, \ldots, n \\ \qquad u := \inf(u, x_k), \\ \qquad v := \sup(v, x_k), \\ \text{end } k; \end{array}$$

Nach Durchlaufen der Schleife ist $u = \min V =: 0$ und $v = \max V =: 1$. (Beachte Satz (4.11)!) $\square$

Wir gehen nun daran, eine Basisdarstellung für die Elemente einer Booleschen Algebra zu entwickeln.

Hierzu werden die kleinsten Elemente oberhalb des Nullelements herangezogen, die so genannten Atome.

Definition (4.14)

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 (4.15)

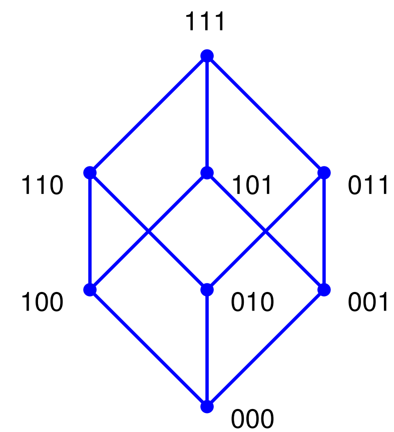
a) $(\mathcal{P}(M), \cup, \cap)$ hat die Atome $\{a\}$, $a \in M$. Ist M endlich, so ist $(\mathcal{P}(M), \cup, \cap)$ atomar.
b) Im distributiven Verband $(\mathbb{N}, \mathrm{ggT}, \mathrm{kgV})$ ist $p \in \mathbb{N}$ genau dann ein Atom, wenn p prim ist. Ein Element $n \in \mathbb{N}$ besitzt jedoch 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 $\mathbf{e}_i := (0, \ldots, 0, 1, 0, \ldots, 0)$, $i = 1, \ldots, n$, 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

$$\mathbf{x} = \bigvee_{\{i\colon x_i = 1\}} \mathbf{e}_i.$$

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

In der nebenstehenden Skizze ist das Hasse-Diagramm der Booleschen Algebra $(\mathbb{B}^3, \wedge, \vee)$ angegeben.
Man vergleiche dies beispielsweise mit dem Hasse-Diagramm von $(\mathcal{P}(\{1, 2, 3\}), \cap, \cup)$, vgl. (3.13).



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

Satz (4.16) (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.

Beweis:

zu a) Sind y_1, y_2 Atome, so gilt nach Definition

$$\begin{aligned} & ((y_1 \le y_2) \lor (y_1 \land y_2 = 0)) \;\land\; ((y_2 \le y_1) \lor (y_1 \land y_2 = 0)) \\ \Rightarrow \quad & (y_1 \le y_2 \;\land\; y_2 \le y_1) \;\lor\; (y_1 \land y_2 = 0) \\ \Rightarrow \quad & (y_1 = y_2) \;\lor\; (y_1 \land y_2 = 0) \qquad \square \end{aligned}$$

zu b) Zu zeigen ist: $x \neq 0 \Rightarrow \exists\, y \in V : (y \text{ Atom } \land y \le x)$.

Beweis analog zur Konstruktion von Null- und Einselement:

$y_0 := x$,
for $k = 0, 1, 2, \dots$
  Falls y_k ein Atom ist: Abbruch!
  Andernfalls: $\exists\, b \in V : [\neg(y_k \le b) \land (y_k \land b \neq 0)]$,
  $\Rightarrow$ Für $y_{k+1} := y_k \land b$ gilt: $0 < y_{k+1} < y_k$.
end k;

Da V *endlich* ist, muss die obige Schleife nach endlich vielen Schritten mit einem gesuchten Atom $y := y_k$ abbrechen. $\square$

zu c) Zu zeigen ist: V ist atomar.

Zunächt zwei Hilfsaussagen über komplementäre Elemente:

(1) $\forall\, a,b \in V:\ \overline{a \wedge b} = \overline{a} \vee \overline{b},\ \overline{a \vee b} = \overline{a} \wedge \overline{b}$ (de Morgan)

(2) $\forall\, a,b \in V:\ a \leq b \Rightarrow \overline{a} \vee b = 1.$

Sei nun $x \in V,\ x \neq 0$, und sei $Y := \{y :\ y$ Atom $\wedge\, y \leq x\}$.
Nach b) ist $Y \neq \emptyset$ und mit V endlich auch $Y = \{y_1, \ldots, y_m\}$.
Wir setzen $a := y_1 \vee \ldots \vee y_m$ und zeigen $a = x$.
Sei $b := x \wedge \overline{a}$. Dann gilt $x \vee b = x \vee (x \wedge \overline{a}) = x$, also $b \leq x$.
Angenommen, dass $b \neq 0$ ist. Dann existiert nach Teil b) ein Atom y mit $y \leq b \leq x$, also $y \in Y$. O.E.d.A. sei $y = y_1$. Damit

$$\begin{aligned} 0 &= y_1 \wedge \overline{y_1} = (y_1 \wedge b) \wedge \overline{y_1} = (y_1 \wedge x \wedge \overline{y_1 \vee \ldots \vee y_m}) \wedge \overline{y_1} \\ &= (y_1 \wedge x \wedge \overline{y_1} \wedge \ldots \wedge \overline{y_m}) \wedge \overline{y_1} = y_1 \wedge x \wedge \overline{y_1} \wedge \ldots \wedge \overline{y_m} \\ &= y_1 \wedge b = y_1, \end{aligned}$$

was der Eigenschaft, dass y_1 Atom ist, widerspricht!
Damit ist $b = x \wedge \overline{a} = 0$.

Weiter sieht man mit (2)

$$\begin{aligned} x \vee \overline{a} &= x \vee (\overline{y_1} \wedge \ldots \wedge \overline{y_m}) = (x \vee \overline{y_1}) \wedge \ldots \wedge (x \vee \overline{y_m}) \\ &= 1 \wedge \ldots \wedge 1 = 1. \end{aligned}$$

Damit ist insgesamt gezeigt: $x \wedge \overline{a} = 0$ und $x \vee \overline{a} = 1$.
Aus der Eindeutigkeit des Komplements ergibt sich $x = a$. $\square$

zu d) Zu zeigen ist die Eindeutigkeit der Basisdarstellung $x = y_1 \vee \ldots \vee y_m$. Sei also $x = y_1 \vee \ldots \vee y_m = \tilde{y}_1 \vee \ldots \vee \tilde{y}_n$ mit Atomen y_j bzw. $\tilde{y}_k$. Für $j \in \{1, \ldots, m\}$ ergibt sich

$$y_j = y_j \vee x = y_j \vee (\tilde{y}_1 \vee \ldots \vee \tilde{y}_n) = (y_j \wedge \tilde{y}_1) \vee \ldots \vee (y_j \wedge \tilde{y}_n).$$

Nach a) existiert ein Index k_j mit $y_j = \tilde{y}_{k_j}$. Damit ist gezeigt $\{y_1, \ldots, y_m\} \subset \{\tilde{y}_1, \ldots, \tilde{y}_n\}$. Genauso ist die umgekehrte Inklusion zu sehen. $\square$

zu e), f) Wir zeigen: Hat V die Atome $Y = \{y_1, \ldots, y_m\}$, so ist $(V, \wedge, \vee)$ isomorph zur Booleschen $(\mathcal{P}(Y), \cap, \cup)$. Dazu definiert man $\Phi : V \to \mathcal{P}(Y)$ vermöge $\Phi(x) := Y_x := \{y \in Y : y \leq x\}$.

Man zeigt dann (Übungsaufgabe!), dass Φ ein bijektiver Homomorphismus ist. $\square$

Niels Henrik Abel (1802 - 1829)

George Boole
(1815-1864)

Harvey Stone
(1903-1989)