Heinz-Peter Gumm/
Werner Poguntke

Boolesche Algebra

B·I·

Hochschultaschenbücher

Band 604

Boolesche Algebra

von
Dr. Heinz-Peter Gumm
Dr. Werner Poguntke
Technische Hochschule Darmstadt

Bibliographisches Institut Mannheim/Wien/Zürich
B. I.-Wissenschaftsverlag

CIP-Kurztitelaufnahme der Deutschen Bibliothek

Gumm, Heinz-Peter:
Boolesche Algebra / von Heinz-Peter Gumm;
Werner Poguntke. - Mannheim; Wien; Zürich:
Bibliographisches Institut, 1981.
(BI-Hochschultaschenbücher; Bd. 604)
ISBN 3-411-00604-8
NE: Poguntke, Werner:; GT

Druck und Bindearbeit: Hain-Druck GmbH, Meisenheim/Glan
Printed in Germany
ISBN 3-411-00604-8

VORWORT

Die vorliegende Ausarbeitung basiert auf einem Manuskript, das von uns zu mehreren Vorlesungen über "Boolesche Algebra" an der Technischen Hochschule Darmstadt vorbereitet und anhand der dabei gewonnenen Erfahrungen überarbeitet wurde.

Die Vorlesungen richteten sich an Studenten nach dem Vorexamen bzw. Vordiplom und wurden in der Mehrzahl von Lehramtskandidaten für das Fach Mathematik, jedoch auch von angehenden Diplom-Mathematikern und Informatikern besucht. Überwiegend an diesem Leserkreis will sich das Buch orientieren, wobei sicherlich Studierende der Natur- oder Ingenieurwissenschaften ebenfalls für sie Interessantes darin entdecken können. Aufgrund der wenig einheitlichen Erwartungen der Hörer- bzw. der zu erwartenden Leserschaft haben wir uns um eine Darstellung bemüht, die den rein mathematischen Zugang mit einem anwendungsorientierten zu verbinden sucht. Im Ergebnis bedeutet dies, daß Methoden zur Vereinfachung "Boolescher Terme" und "Venn-Diagramme", aber auch der Stonesche Darstellungssatz behandelt werden. Inwieweit die Behandlung stellenweise zu knapp oder auch unausgewogen geraten ist, mag der Leser selbst beurteilen.

Eingestreute Beispiele und Übungsaufgaben sollen insbesondere den Leser unterstützen, der das Buch zum Selbststudium verwenden möchte. Lösungsvorschläge zu den Aufgaben sind am Ende des Buches zu finden.

Wir danken Klaus Keimel für einige Verbesserungsvorschläge und Traudel Ridder für das sorgfältige Herstellen der maschinengeschriebenen Fassung.

Darmstadt, im August 1981

Heinz-Peter Gumm
Werner Poguntke

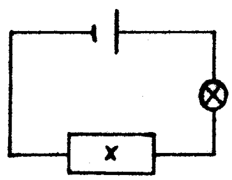
INHALTSVERZEICHNIS

§ 1. SCHALTALGEBRA, MENGENALGEBRA, AUSSAGENLOGIK

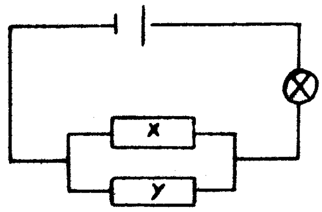
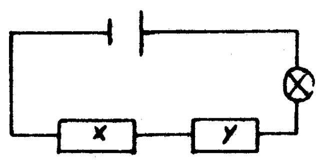
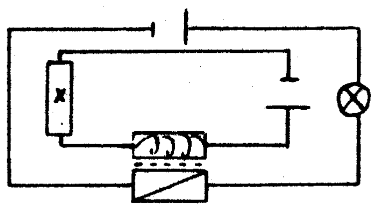
Es gibt kaum ein Teilgebiet der Algebra, das in so zahlreichen außermathematischen Bereichen angewendet wird wie die Boolesche Algebra. Als "Erfinder" der Booleschen Algebra wird George Boole (1815-1864) angesehen, der in seinem Buch "An investigation of the laws of thought" (1854) eine *Algebra der Logik* einführte. Heute hat diese Algebra der Logik eine Fülle von Anwendungen nicht nur in der mathematischen Logik und in der Maß- und Wahrscheinlichkeitstheorie, sondern auch in der Technik bei der Konstruktion elektrischer Schaltkreise und "intelligenter" Maschinen gefunden.

Wir wollen mit der Schaltalgebra beginnen, um den mathematischen Begriff der Booleschen Algebra zu motivieren. Eine exakte Grundlegung wird sich aus den beiden nächsten Paragraphen ergeben. Zunächst werden die Grundbegriffe erläutert.

Ein bistabiles Schaltelement (Ein-Aus-Schalter) kann die Zustände 0 (offen) oder 1 (geschlossen) haben.



Man hat sich einen Stromkreis vorzustellen, in dem eine durch das Symbol ⊗ dargestellte Lampe genau dann aufleuchtet, wenn x im Zustand 1 ist. Durch Kombinationen von bistabilen Schaltelementen erhält man Schaltkreise. Wir beschränken uns auf drei Verknüpfungen, und zwar die Parallelschaltung, die Serienschaltung und die Komplementierung (siehe die folgende Tabelle).

	Diagrammdarstellung	algebraische Bezeichnung
Parallelschaltung (Oder-Schaltung)		$x+y$
Serienschaltung (Und-Schaltung)		$x\cdot y$
Komplementierung (Non-Schaltung)		x'

Im Diagramm für die Non-Schaltung soll durch das Symbol  ein Relaisschalter angedeutet werden, der die Eigenschaft hat, daß durch den "unteren Draht" dann und nur dann Strom fließt, wenn der obere gesperrt ist.

Die Funktionsweisen der drei Verknüpfungen werden durch die zugehörigen Schaltfunktionen beschrieben:

x	y	x+y
0	0	0
0	1	1
1	0	1
1	1	1

x	y	x·y
0	0	0
0	1	0
1	0	0
1	1	1

x	x'
0	1
1	0

Mit anderen Worten soll z.B. $x+y$ den Zustand 1 haben, wenn dies für x oder y (oder beide) der Fall ist. Es handelt sich hier also um Eigenschaften, wie sie elektrischen Schaltungen tatsächlich zukommen.

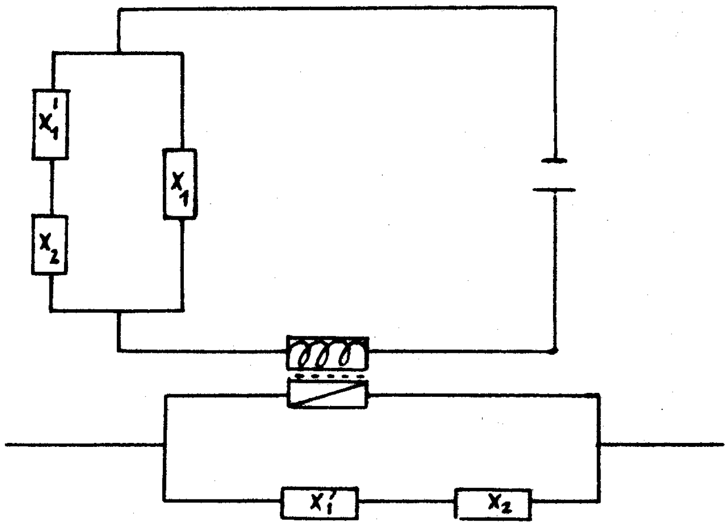
Jede Schaltung mit einer endlichen Anzahl bistabiler Schaltelemente, die sich durch Parallel-, durch Serienschaltungen und durch Komplementierungen ergibt, heißt ein (Serien-Parallel-)Schaltkreis. Dies soll so verstanden werden, daß nicht nur Schaltelemente, sondern auch bereits aufgebaute Schaltkreise zu größeren parallel- oder seriengeschaltet bzw. komplementiert werden. Der Vollständigkeit halber bezieht man den stets geschlossenen Schaltkreis 1 und den stets offenen Schaltkreis 0 mit ein. Präziser als die obige Beschreibung ist die folgende induktive Definition:

1.1 Definition von Schaltkreisen:

a) Jedes Schaltelement x ist ein Schaltkreis, ebenso 0 und 1.
b) Sind s und t Schaltkreise, so auch $s+t$, $s \cdot t$ und s'.
c) Jeder Schaltkreis entsteht, indem a) und b) endlich oft angewendet werden.

Man beachte, daß man "denselben" Schaltkreis zum Aufbau eines neuen Schaltkreises mehrfach benutzen darf.
In der Diagrammdarstellung eines Schaltkreises ist es üblich, die Symbole für die äußere Spannungsquelle und die Lampe wegzulassen; ferner stellt man ein komplementiertes Schaltelement einfach durch $-\boxed{x'}-$ dar.

1.2 Beispiel:



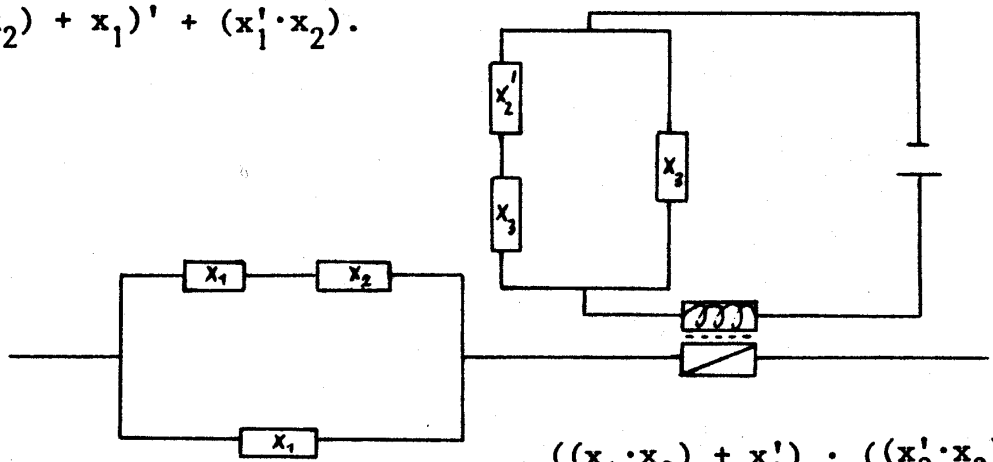
Die obige induktive Definition eines Schaltkreises liefert ein Verfahren, jeden Schaltkreis (mit Schaltelementen $x_1,\dots,x_n$) mit einem algebraischen Ausdruck zu belegen.

1.3 Beispiel:

a) Zu dem in 1.2 dargestellten Schaltkreis gehört der Term

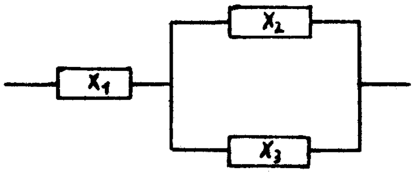
$((x_1'\cdot x_2) + x_1)' + (x_1'\cdot x_2)$.

b)



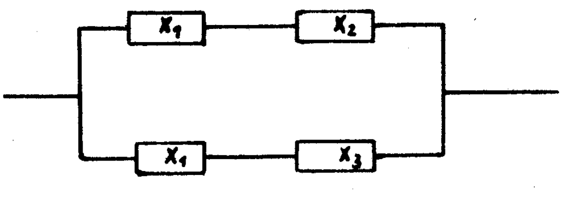
$((x_1\cdot x_2) + x_1') \cdot ((x_2'\cdot x_3) + x_3)'$

c)



$x_1 \cdot (x_2 + x_3)$

d)



$(x_1\cdot x_2) + (x_1\cdot x_3)$

Wir berechnen nun die zu c) und d) gehörenden Schaltfunktionen $f\colon \{0,1\}^3 \to \{0,1\}$, indem wir ihre Wertetabellen aufstellen:

x_1	x_2	x_3	x_2+x_3	$x_1\cdot(x_2+x_3)$	$x_1\cdot x_2$	$x_1\cdot x_3$	$(x_1\cdot x_2)+(x_1\cdot x_3)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Der Vergleich der fünften mit der letzten Spalte zeigt, daß die Schaltungen in c) und d) dieselbe Schaltfunktion besitzen. Die beiden Schaltkreise sind in ihrer Wirkungsweise äquivalent, was wir durch

$$x_1 \cdot (x_2+x_3) \equiv (x_1\cdot x_2) + (x_1\cdot x_3)$$

ausdrücken (man liest "≡" als "äquivalent").
Wir haben nicht verwendet, daß x_1, x_2 und x_3 Schaltelemente sind, denn auch Schaltkreise können nur die Zustände 0 bzw. 1 annehmen. Daher haben wir für beliebige Schaltkreise u,v,w das distributive Gesetz

$$u \cdot (v+w) \equiv (u\cdot v) + (u\cdot w).$$

Es soll nun von einem festen Vorrat von Schaltelementen $x_1,\ldots,x_n$ ausgegangen werden, so daß die zugehörigen Schaltfunktionen immer als Abbildungen von $\{0,1\}^n$ nach $\{0,1\}$ aufzufassen sind. Wir wollen einige wichtige, für Schaltkreise gültige Äquivalenzen aufschreiben; ihre Gültigkeit ist in den meisten Fällen offensichtlich und kann problemlos mit Hilfe von Operationstafeln nachgewiesen werden:

(1)	$u+u \equiv u$	$(\overline{1})$	$u\cdot u \equiv u$
(2)	$u+v \equiv v+u$	$(\overline{2})$	$u\cdot v \equiv v\cdot u$
(3)	$u+(v+w) \equiv (u+v)+w$	$(\overline{3})$	$u\cdot(v\cdot w) \equiv (u\cdot v)\cdot w$
(4)	$u+(u\cdot v) \equiv u$	$(\overline{4})$	$u\cdot(u+v) \equiv u$
(5)	$u\cdot(v+w) \equiv (u\cdot v)+(u\cdot w)$	$(\overline{5})$	$u+(v\cdot w) \equiv (u+v)\cdot(u+w)$
(6)	$u + 0 \equiv u$	$(\overline{6})$	$u \cdot 1 \equiv u$
(7)	$u + 1 \equiv 1$	$(\overline{7})$	$u \cdot 0 \equiv 0$
(8)	$u + u' \equiv 1$	$(\overline{8})$	$u \cdot u' \equiv 0$

Es gelten zahlreiche weitere Äquivalenzen, etwa die De Morganschen Regeln

$$(u+v)' \equiv u'\cdot v' \qquad \text{und} \qquad (u\cdot v)' \equiv u'+v'.$$

Wir zeigen, daß diese schon aus (1) bis (8) und $(\bar{1})$ bis $(\bar{8})$ folgen. (Da die Äquivalenz von Schaltkreisen über die Gleichheit der zugehörigen Schaltfunktionen erklärt ist, kann mit "$\equiv$" wie mit dem Gleichheitszeichen gerechnet werden. Wir werden im nächsten Paragraphen genauer darauf eingehen.)

1. Beweisschritt: Wir zeigen zunächst, daß $u+v \equiv 1$ und $u\cdot v \equiv 0$ die Äquivalenz $v \equiv u'$ nach sich zieht (Eindeutigkeit des Komplements). Dies folgt aus $v \underset{(6)}{\equiv} v + 0 \underset{(\bar{8})}{\equiv} v + (u\cdot u') \underset{(\bar{5})}{\equiv} (v+u)\cdot(v+u') \underset{(2)}{\equiv} 1\cdot(v+u') \underset{(\bar{6})}{\equiv} v+u'$

und $u' \underset{(6)}{\equiv} u'+(u\cdot v) \underset{(\bar{5})}{\equiv} (u'+u)\cdot(u'+v) \underset{(2,8)}{\equiv} 1\cdot(u'+v) \underset{(\bar{2},6)}{\equiv} u'+v \underset{(2)}{\equiv} v+u'$.

2. Beweisschritt: Nun wird gezeigt, daß $(u+v) + (u'\cdot v') \equiv 1$ und $(u+v)\cdot(u'\cdot v') \equiv 0$ ist. Dies folgt mit

$$(u+v) + (u'\cdot v') \underset{(3)}{\equiv} u + (v + (u'\cdot v')) \underset{(\bar{5})}{\equiv} u + ((v+u')\cdot(v+v'))$$

$$\underset{(8,\bar{6})}{\equiv} u + (v+u') \underset{(2,3)}{\equiv} (u+u') + v \underset{(2,8,7)}{\equiv} 1 \quad \text{und}$$

$$(u+v)\cdot(u'\cdot v') \underset{(\bar{2},\bar{3})}{\equiv} u'\cdot(v'\cdot(u+v)) \underset{(5)}{\equiv} u'\cdot((v'\cdot u) + (v'\cdot v))$$

$$\underset{(\bar{2},\bar{8},6)}{\equiv} u'\cdot(v'\cdot u) \underset{(\bar{2},\bar{3})}{\equiv} (u\cdot u')\cdot v \underset{(\bar{2},\bar{8},\bar{7})}{\equiv} 0.$$

Aus erstem und zweiten Beweisschritt ergibt sich nun, daß allgemein $(u+v)' \equiv u'\cdot v'$ gilt. $(u\cdot v)' \equiv u'+v'$ wird analog gezeigt.

<u>Zur Mengenalgebra:</u>

Sei X eine Menge und $\mathbb{P}(X)$ die Potenzmenge, also die Menge aller Teilmengen von X. Für $A,B \in \mathbb{P}(X)$ setze man nun $A+B := A\cup B$, $A\cdot B := A\cap B$, $A' := \bar{A}$ (Komplement $X\setminus A$ von A in X), ferner $1 := X$ und $0 := \emptyset$ (leere Menge). Man sieht, daß sämtliche Gesetze (1)-(8) und $(\bar{1})$-$(\bar{8})$ für die Elemente von $\mathbb{P}(X)$ gültig sind, wenn man "$\equiv$" als Gleichheit liest. Da die De Morganschen Regeln allein unter Benutzung dieser Gesetze bewiesen wurden, gelten diese auch für die Mengenalgebra. Wir wissen somit auch, daß stets $\overline{(A\cup B)} = \bar{A}\cap\bar{B}$ und $\overline{(A\cap B)} = \bar{A}\cup\bar{B}$ ist.

Zur Aussagenlogik:

Sei X eine Menge von Aussagen, die jeweils entweder wahr oder falsch sind. Man verknüpft Aussagen A,B auf folgende Weise:

$A \vee B$ ("A oder B") ist genau dann wahr, wenn A wahr ist oder wenn B wahr ist (oder wenn beide wahr sind);

$A \wedge B$ ("A und B") ist genau dann wahr, wenn sowohl A als auch B wahr sind.

$\neg A$ ("Nicht-A") ist genau dann wahr, wenn A falsch ist.

W ist die Aussage "$1=1$" und immer wahr.

F ist die Aussage "$1 \neq 1$" und immer falsch.

(Wir setzen voraus, daß X unter diesen Verknüpfungen abgeschlossen ist und $W,F \in X$ gilt.)

Setzt man hier $A+B := A \vee B$, $A \cdot B := A \wedge B$, $A' := \neg A$, $1 := W$ und $0 := F$, und ersetzt man "$\equiv$" durch das Zeichen "$<=>$" (logisch äquivalent), so stellt man wiederum die Gültigkeit der Gesetze (1)-(8) und $(\overline{1})$ bis $(\overline{8})$ fest. Als Konsequenz ergeben sich somit hier die logischen Äquivalenzen

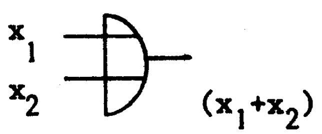
$$\neg(A \vee B) <=> \neg A \wedge \neg B \quad \text{und} \quad \neg(A \wedge B) <=> \neg A \vee \neg B.$$

Die Gemeinsamkeiten der Schaltalgebra, der Mengenalgebra und der Aussagenlogik lassen es sinnvoll erscheinen, die Gesetze (1)-(8) und $(\overline{1})$-$(\overline{8})$ als abstraktes Axiomensystem näher zu untersuchen. Dies führt uns zum Begriff einer Booleschen Algebra.

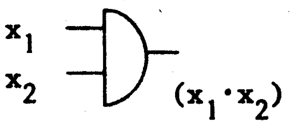
Zuvor jedoch wollen wir noch auf eine heute gebräuchliche Variante der Schaltalgebra eingehen:

Logische Schaltungen

Schaltkreise in modernen hochentwickelten Maschinen werden heute nicht mehr mit einfachen Kontaktschaltern und Relais realisiert, sondern mit Hilfe von Halbleiterbauelementen. Solche Bauelemente können die Aufgabe mehrerer Schalter gleichzeitig übernehmen. Neben dem geringen Platzbedarf sind vor allem die extrem kurzen Schaltzeiten und die minimale Störanfälligkeit von Bedeutung. In der Regel handelt es sich um Schaltglieder, auch Gatter genannt, mit mehreren Eingängen und einem Ausgang. Die gebräuchlichsten dieser Gatter werden symbolisch folgendermaßen dargestellt:

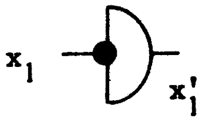


das OR-Gatter, das der Parallelschaltung der Schaltelemente x_1 und x_2 entspricht;



das AND-Gatter entspricht der Serienschaltung von x_1 und x_2;

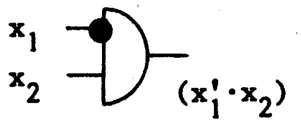
das NON-Gatter wird durch das Schaltbild



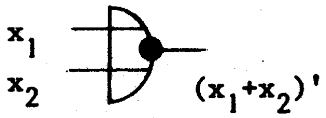
oder auch nur durch

dargestellt.

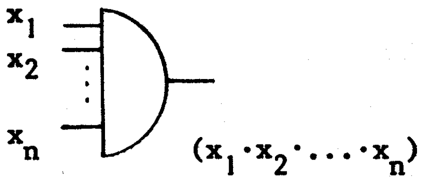
Häufig verbindet man das NON-Gatter auch mit anderen Schaltelementen, so ergibt sich etwa

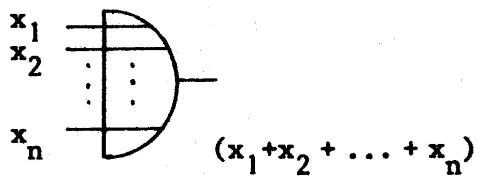


oder

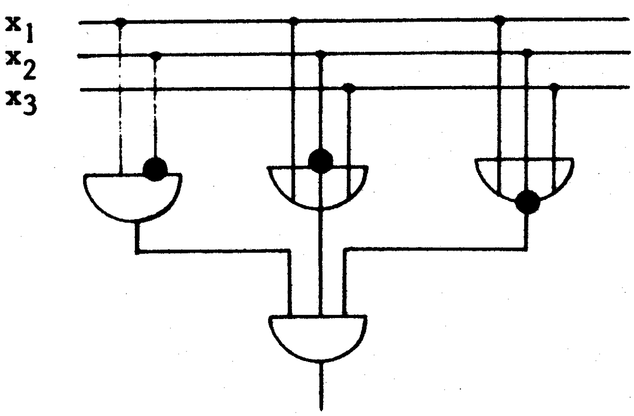


Bei der Darstellung von Schaltkreisen verzichtet man auf die Darstellung von Spannungsquellen oder Relais; letztere sind i.A. in die Bausteine integriert. Kompliziertere Schaltbilder geraten in dieser Symbolik meist übersichtlicher. Zur weiteren Vereinfachung läßt man auch AND-Gatter und OR-Gatter mit mehr als zwei Eingängen zu:





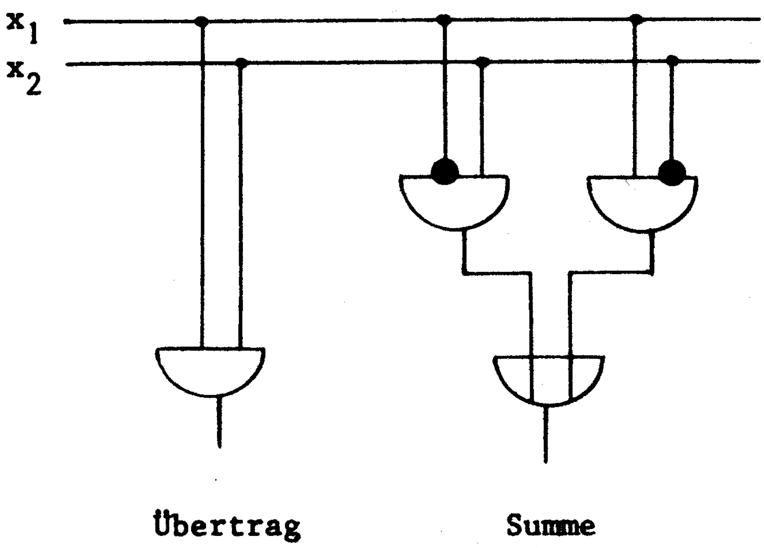
Damit entspricht das folgende Schaltbild



etwa dem Ausdruck $(x_1 \cdot x_2') \cdot (x_1 + x_2' + x_3) \cdot (x_1 + x_2 + x_3)'$.

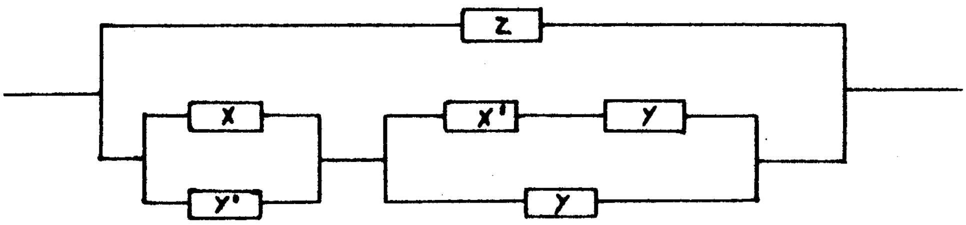
Es sei zum Schluß noch erwähnt, daß in der Praxis auch Schaltelemente und Schaltkreise mit mehreren Ausgängen eine wichtige Rolle spielen. Wir werden diese Situation jedoch nicht behandeln, sondern uns mit einem Beispiel und dem Hinweis begnügen, daß etwa ein Schaltkreis mit zwei Ausgängen durch zwei (übliche) Schaltkreise, einen für jeden Ausgang, beschrieben werden kann.

Als Beispiel für eine Schaltung mit zwei Ausgängen geben wir untenstehend die Schaltung eines sogenannten "Halbaddierers", der zwei einstellige Binärzahlen 0 bzw. 1 addiert und mit Summe und Übertrag, d.h. als zweistellige Binärzahl darstellt:



Übungsaufgaben:

1.



a) Welcher algebraische Ausdruck ist obigem Schaltkreis zugeordnet?

b) Man benutze (1)-(8) und $(\overline{1})$-$(\overline{8})$, um den in a) erhaltenen Ausdruck zu vereinfachen. Man vereinfache den Schaltkreis.

2. Zeige, daß für beliebige Schaltkreise u,v,w gilt:

a) $(u')' \equiv u$ b) $(u\cdot(v+w))' \equiv u' + (v'\cdot w')$

3. In der Aussagenlogik definiert man $A \Rightarrow B$ als die Aussage $(\neg A) \vee B$. Was wäre die "$\Rightarrow$" entsprechende Operation in der Mengenalgebra? Was heißt es für $A,B \in \mathbb{P}(X)$, daß $(A \Rightarrow B) = X$ ist?

§ 2. BOOLESCHE ALGEBREN

2.1 Definition: Sei B eine Menge, und seien $0,1$ Elemente aus B. Weiter seien zweistellige Operationen $+$ und $\cdot$ sowie eine einstellige Operation $'$ auf B erklärt. Dann ist $(B; +, \cdot, ', 0,1)$ eine Algebra[*)]. $(B; +, \cdot, ', 0,1)$ heißt Boolesche Algebra, falls folgende Gesetze für beliebige $x,y,z \in B$ gelten:

(B_1)	$x+x = x$	$(\overline{B}_1)$	$x\cdot x = x$	(Idempotenz)
(B_2)	$x+y = y+x$	$(\overline{B}_2)$	$x\cdot y = y\cdot x$	(Kommutativität)
(B_3)	$x+(y+z) = (x+y)+z$	$(\overline{B}_3)$	$x\cdot(y\cdot z) = (x\cdot y)\cdot z$	(Assoziativität)
(B_4)	$x+(x\cdot y) = x$	$(\overline{B}_4)$	$x\cdot(x+y) = x$	(Absorption)
(B_5)	$x+(y\cdot z) = (x+y)\cdot(x+z)$	$(\overline{B}_5)$	$x\cdot(y+z) = (x\cdot y)+(x\cdot z)$	(Distributivität)
(B_6)	$x+0 = x$	$(\overline{B}_6)$	$x\cdot 1 = x$	
(B_7)	$x+1 = 1$	$(\overline{B}_7)$	$x\cdot 0 = 0$	
(B_8)	$x+x' = 1$	$(\overline{B}_8)$	$x\cdot x' = 0$	

Anmerkung: In der Literatur werden statt des Zeichens "$+$" auch "$\vee$", "$\cup$" oder "$\sqcup$" und anstelle von "$\cdot$" auch "$\wedge$", "$\cap$" oder "$\sqcap$" verwendet.

2.2 Beispiele:

a) Sei X eine Menge und $\mathbb{P}(X)$ die Potenzmenge von X. Dann ist $(\mathbb{P}(X); \cup, \cap, \overline{\ \ }, \emptyset, X)$ eine Boolesche Algebra.

b) Sei X eine unendliche Menge und $\mathbb{E}(X)$ die Menge aller derjenigen Teilmengen A von X, für die gilt: A ist endlich oder $\overline{A}$ ist endlich. Dann ist $(\mathbb{E}(X); \cup, \cap, \overline{\ \ }, \emptyset, X)$ eine Boolesche Algebra.

c) Sei T ein topologischer Raum und $\mathbb{B}(T)$ die Menge aller Teilmengen von T, die sowohl offen als auch abgeschlossen sind. Dann ist $(\mathbb{B}(T); \cup, \cap, \overline{\ \ }, \emptyset, T)$ eine Boolesche Algebra.

d) Sei T_{30} die Menge $\{1,2,3,5,6,10,15,30\}$ aller Teiler der Zahl 30. Setzt man für $x \in T_{30}$ $x' := \frac{30}{x}$, so ist $(T_{30}; \mathrm{kgV}, \mathrm{ggT}, ', 1, 30)$ eine Boolesche Algebra.

---

*) Genauer spricht man von einer "Algebra vom Typ $(2,2,1,0,0)$", weil $+$ und $\cdot$ zweistellige, $'$ eine einstellige und 0 und 1 "nullstellige" Operationen sind.

<u>Anmerkung:</u> Ist in einer Booleschen Algebra $(B; +, \cdot, ', 0, 1)$ $0=1$, so folgt für beliebiges $x \in B$: $x = x+0 = x+1 = 1$, das heißt B ist einelementig. Sehen wir von diesem Trivialfall ab, so können wir also für Boolesche Algebren stets $0 \neq 1$ annehmen.

Das in 2.1 angegebene Axiomensystem ist nicht minimal, d.h. es sind Axiome darunter, die bereits aus den anderen folgen. Es gibt sogar ein Axiomensystem, das nur aus *einer* (allerdings sehr "langen") Gleichung besteht. Für das Rechnen in Booleschen Algebren ist es aber zweckmäßiger, von Gesetzen ähnlich denen in 2.1 auszugehen.
Vertauscht man in irgendeinem der Axiome (B_1)-(B_8) bzw. $(\overline{B}_1)$-$(\overline{B}_8)$ "+" mit "·" und "0" mit "1", so erhält man ein anderes dieser Axiome, das zum vorgegebenen <u>duale</u> Axiom. Daraus folgern wir:

2.3 <u>Lemma:</u> Ist $(B; +, \cdot, ', 0, 1)$ eine Boolesche Algebra, so ist auch $(B; \cdot, +, ', 1, 0)$ eine Boolesche Algebra; man nennt letztere die (zur vorgegebenen) <u>duale Boolesche Algebra</u>.

Es ergibt sich damit das <u>Dualitätsprinzip</u> für Boolesche Algebren:

2.4 <u>Satz:</u> Gilt eine Gleichung in allen Booleschen Algebren, so gilt auch die zu ihr duale Gleichung in allen Booleschen Algebren.

<u>Beweis:</u> Sei (G) eine Gleichung, die in allen Booleschen Algebren gilt. Sei $(\overline{G})$ die zu (G) duale Gleichung, $(B; +, \cdot, ', 0, 1)$ eine Boolesche Algebra. Es gilt (G) in der dualen Algebra $(B; \cdot, +, ', 1, 0)$. Dies ist aber gleichbedeutend damit, daß $(\overline{G})$ in $(B; +, \cdot, ', 0, 1)$ gilt.

Als nächstes wollen wir uns einige weitere Rechenregeln für Boolesche Algebren verschaffen.

2.5 <u>Lemma:</u> In jeder Booleschen Algebra gilt für beliebige Elemente x,y,z:

(a) Aus $x \cdot y = 0$ und $x+y = 1$ folgt $y = x'$ (Eindeutigkeit des Komplements).
(b) $(x+y)' = x' \cdot y'$
(c) $(x \cdot y)' = x'+y'$
(d) $(x')' = x$, $1' = 0$, $0' = 1$
(e) Die Aussagen $x \cdot y' = 0$, $x \cdot y = x$ und $x+y = y$ sind äquivalent.
(f) Ist $x \cdot y = x \cdot z$ und $x+y = x+z$, so folgt bereits $y = z$.

Beweis:

(a) wurde in § 1 für Schaltkreise (und deren Äquivalenz) gezeigt; da dort nur die Gesetze (1)-(8) und $(\overline{1})$-$(\overline{8})$ benutzt wurden, kann der Beweis kopiert werden. Dasselbe gilt für (b) und (c).

(d) Dies ergibt sich sofort aus (a), da x Komplement von x' und 0 Komplement von 1 ist.

(e) Aus $x\cdot y' = 0$ folgt $x = x\cdot 1 = x\cdot(y+y') = (x\cdot y) + (x\cdot y') = x\cdot y$. Aus $x\cdot y = x$ folgt $x+y = (x\cdot y) + y = y$. Aus $x+y = y$ bekommt man wiederum $x\cdot y' = x.(x+y)' = x\cdot(x'\cdot y') = (x\cdot x')\cdot y' = 0\cdot y' = 0$.

(f) Sei $x\cdot y = x\cdot z$ und $x+y = x+z$. Dann hat man
$y = y+(x\cdot y) = y+(x\cdot z) = (y+x)\cdot(y+z) = (x+z)\cdot(y+z) = z+(x\cdot y) = z+(x\cdot z) = z$.

Wir wollen nun eine Vereinbarung zur Vereinfachung der Schreibweise treffen. Wie oft bei der Multiplikation üblich (etwa von Polynomen über den reellen Zahlen), lassen wir im folgenden den Punkt als Zeichen für Multiplikation weg: statt $x\cdot y$ schreiben wir einfach xy. Die Assoziativgesetze (B_3) und $(\overline{B}_3)$ erlauben es uns ferner, Klammern bei Summen (Produkten) mit mehr als zwei Summanden (Faktoren) wegzulassen: wir schreiben einfach $x+y+z$ bzw. xyz. Weiter wird vereinbart, daß "Punktrechnung vor Strichrechnung" geht, so daß Klammern um Produkte wegfallen können: z.B. wird anstatt $(x\cdot y) + ((y\cdot z) + (z\cdot x))$ einfach $xy + yz + zx$ geschrieben.

Der nun folgende Begriff der Unteralgebra wurde bereits durch die Beispiele b) und c) in 2.2 nahegelegt.

2.6 Definition: Sei $(B; +, \cdot, ', 0, 1)$ eine (Boolesche) Algebra. Eine Teilmenge C von B heißt abgeschlossen, wenn folgende Bedingungen erfüllt sind:

(i) $0 \in C$, $1 \in C$.

(ii) Ist $x \in C$, so gilt auch $x' \in C$.

(iii) Sind $x,y \in C$, so folgt $x+y \in C$ und $x\cdot y \in C$.

Ist C eine abgeschlossene Teilmenge von B, so kann man die Operationen $+,\cdot$ und $'$ auf C einschränken und erhält eine Algebra $(C; +, \cdot, ', 0, 1)$. Diese heißt eine Unteralgebra von $(B; +, \cdot, ', 0, 1)$.

2.7 Lemma: Eine Unteralgebra einer Booleschen Algebra ist stets wieder eine Boolesche Algebra.

Beweis: Wegen $C \subseteq B$ gelten die Gesetze (B_1)-(B_8) und $(\overline{B}_1)$-$(\overline{B}_8)$ insbesondere auch für alle Elemente aus C.

Es folgt eine weitere Vereinbarung zu unserer Schreibeweise:
Ist $(B; +, \cdot, ', 0, 1)$ eine (Boolesche) Algebra, so werden wir, wenn keine Mißverständnisse zu befürchten sind, von der "(Booleschen) Algebra B" sprechen und entsprechend von der "Unteralgebra C", wenn C eine abgeschlossene Teilmenge von B ist.

2.8 Satz: Sei B eine (Boolesche) Algebra und $(B_i)_{i\in I}$ eine Familie von Unteralgebren von B. Dann ist auch $\bigcap\{B_i \mid i\in I\}$ eine Unteralgebra von B.

Beweis: Wir haben zu zeigen, daß $\bigcap\{B_i \mid i\in I\}$ abgeschlossen ist. Da für jedes $i\in I$ gilt $0,1 \in B_i$, folgt auch $0,1 \in \bigcap\{B_i \mid i\in I\}$. Sei $x \in \bigcap\{B_i \mid i\in I\}$; es ist $x \in B_i$ für jedes $i\in I$ und, da jedes der B_i abgeschlossen ist, auch $x' \in B_i$ für jedes $i\in I$; es folgt $x' \in \bigcap\{B_i \mid i\in I\}$. Der Nachweis der Eigenschaft (iii) verläuft entsprechend.

2.9 Folgerung: Sei B eine (Boolesche) Algebra und sei X eine beliebige Teilmenge von B. Dann existiert eine *kleinste* Unteralgebra von B, die X umfaßt. M.a.W. gibt es eine Unteralgebra C von B mit den folgenden Eigenschaften:
(i) $X \subseteq C$
(ii) Für jede Unteralgebra D von B mit $X \subseteq D$ gilt $C \subseteq D$.
(Wegen (ii) ist diese Unteralgebra eindeutig bestimmt; sie wird die von X erzeugte Unteralgebra von B genannt und mit $\langle X\rangle_B$ bezeichnet.)

Beweis: Sei $(B_i)_{i\in I}$ die Familie aller Unteralgebren von B, die X enthalten. $C := \bigcap\{B_i \mid i\in I\}$ erfüllt offenbar die Bedingung (i). Ist nun D eine Unteralgebra von B mit $X \subseteq D$, so folgt $D = B_j$ für ein $j\in I$ und damit natürlich $C \subseteq D$; folglich ist auch (ii) erfüllt.

Eine andere Beschreibung der von X erzeugten Unteralgebra von B liefert der folgende Satz.

2.10 Satz: Sei X eine Teilmenge der (Booleschen) Algebra B. Definiert man induktiv

$X_o \;:= X \cup \{0,1\}$ und (für $n \geq 0$)

$X_{n+1} := X_n \cup \{x+y \mid x,y \in X_n\} \cup \{xy \mid x,y \in X_n\} \cup \{x' \mid x \in X_n\}$,

so gilt $\langle X\rangle_B = \bigcup\{X_n \mid n \in \mathbb{N}\}$.

Beweis: Man hat $X \subseteq \langle X\rangle_B$ und wegen der Abgeschlossenheit von $\langle X\rangle_B$ auch $X_o \subseteq \langle X\rangle_B$. Die Abgeschlossenheit hat auch zur Folge, daß $X_n \subseteq \langle X\rangle_B$ stets $X_{n+1} \subseteq \langle X\rangle_B$ nach sich zieht. Mithin hat man per Induktion $\bigcup\{X_n \mid n \in \mathbb{N}\} \subseteq \langle X\rangle_B$.
Wir weisen nun nach, daß $\bigcup\{X_n \mid n \in \mathbb{N}\}$ abgeschlossen ist; nach der Definition von $\langle X\rangle_B$ ist dann der Beweis erbracht.
Offenbar gilt $0,1 \in \bigcup\{X_n \mid n \in \mathbb{N}\}$. Es wird nun die Abgeschlossenheit unter "+" gezeigt; die restlichen Schritte verlaufen analog.
Seien also $x,y \in \bigcup\{X_n \mid n \in \mathbb{N}\}$. Es existieren also $s,t \in \mathbb{N}$ mit $x \in X_s$ und $y \in X_t$. Sei o.B.d.A. $s \leq t$. Wegen $X_s \subseteq X_t$ folgt $x,y \in X_t$ und $x+y \in X_{t+1} \subseteq \bigcup\{X_n \mid n \in \mathbb{N}\}$.

2.11 Definition: Sei C eine Unteralgebra der (Booleschen) Algebra B, $X \subseteq C$ Teilmenge von C. X heißt ein Erzeugendensystem von C, falls $\langle X\rangle_B = C$ gilt. Gibt es eine endliche Teilmenge X_o von B mit $\langle X_o\rangle_B = C$, so heißt C endlich erzeugt.

2.12 Beispiele:

a) Sei S eine beliebige Menge. $\{\emptyset, S\}$ ist eine Unteralgebra von $\mathbb{P}(S)$.
b) Sei T ein topologischer Raum. Die Boolesche Algebra $\mathbb{B}(T)$ aller offen-abgeschlossenen Teilmengen von T ist eine Unteralgebra von $\mathbb{P}(T)$.
c) In der Booleschen Algebra $\mathbb{P}(\{1,2,3,4\})$ bestimmen wir die Unteralgebra, die von $X = \{\{1\}, \{1,2\}\}$ erzeugt wird. Mit 2.10 erhalten wir:

$X_o = \{\{1\}, \{1,2\}, \emptyset, \{1,2,3,4\}\}$;

$X_1 = \{\{1\}, \{1,2\}, \emptyset, \{1,2,3,4\}, \{2,3,4\}, \{3,4\}\}$;

$X_2 = \{\{1\}, \{1,2\}, \emptyset, \{1,2,3,4\}, \{2,3,4\}, \{3,4\}, \{1,3,4\}, \{2\}\}$;

$X_3 = X_2$, also auch $X_2 = X_3 = X_4 = \dots$.

Damit ist $\langle X\rangle_{\mathbb{P}(\{1,2,3,4\})} = X_2$.

Übungsaufgaben:

4. Sei B eine Boolesche Algebra und $b \in B$. Man zeige, daß $\{0,b,b',1\}$ eine Unteralgebra von B ist. Was ist $\langle\emptyset\rangle_B$?

5. Was ist die kleinste Mächtigkeit eines Erzeugendensystems von T_{30} ?

6. Sei B eine Boolesche Algebra und $b \in B$. Zeige, daß $\{bx \mid x \in B\} \cup \{b'+x \mid x \in B\}$ eine Unteralgebra von B ist.

7. Man beweise, daß die Boolesche Algebra $\mathbb{E}(\mathbb{N})$ (vgl. 2.2b)) nicht endlich erzeugt ist. (Anspruchsvolle Aufgabe).

Das Bestreben, verschiedene (Boolesche) Algebren vergleichen zu wollen, führt zum Begriff des Homomorphismus.

2.13 Definition: Eine Abbildung $\phi: B \to C$ heißt Homomorphismus von $(B; +, \cdot, ', 0, 1)$ nach $(C; \tilde{+}, \tilde{\cdot}, \tilde{'}, \tilde{0}, \tilde{1})$, falls für alle $x,y \in B$ folgende Bedingungen erfüllt sind:

(i) $\phi(0) = \tilde{0}$, $\phi(1) = \tilde{1}$

(ii) $\phi(x') = (\phi(x))^{\tilde{'}}$

(iii) $\phi(x+y) = \phi(x) \mathbin{\tilde{+}} \phi(y)$ und $\phi(x \cdot y) = \phi(x) \mathbin{\tilde{\cdot}} \phi(y)$.

Ist ϕ surjektiv (injektiv), so sagt man, ϕ sei ein Homomorphismus von B auf (in) C; ein bijektiver Homomorphismus heißt Isomorphismus.

Das folgende Lemma ist leicht zu beweisen, doch wichtig anzumerken.

2.14 Lemma: Seien B,C und D (Boolesche) Algebren und $\phi: B \to C$, $\psi: C \to D$ Homomorphismen. Dann gilt:

(a) $\psi \circ \phi$ ist ein Homomorphismus von B nach D.

(b) Ist ϕ ein Isomorphismus, so auch $\phi^{-1}: C \to B$.

Definitionsgemäß sind Homomorphismen strukturerhaltende Abbildungen. Gibt es einen Isomorphismus zwischen B und C, so sagen wir, B und C seien isomorph und schreiben $B \cong C$. Isomorphe Algebren sind bezüglich ihrer Struktur identisch - sie unterscheiden sich nur in der "Natur" ihrer Grundmengen.

2.15 <u>Beispiele:</u>

a) $\phi\colon \mathbb{P}(\{a,b,c\}) \to \{0,1\}$ sei definiert durch

$$\phi(S) := \begin{cases} 1, & \text{falls } c \in S \\ 0, & \text{falls } c \notin S. \end{cases}$$

Dann ist ϕ ein Homomorphismus von $(\mathbb{P}(\{a,b,c\}); \cup, \cap, \overline{}, \emptyset, \{a,b,c\})$ auf die zweielementige Boolesche Algebra $(\{0,1\}; +, \cdot, ', 0, 1)$.

b) $\phi\colon T_{30} \to \{0,1\}$ sei definiert durch

$$\phi(x) := \begin{cases} 1, & \text{falls } x \text{ teilbar durch } 5 \\ 0 & \text{sonst.} \end{cases}$$

ϕ ist Homomorphismus von T_{30} auf $\{0,1\}$.

c) $\phi\colon T_{30} \to \mathbb{P}(\{2,3,5\})$ sei definiert durch

$$\phi(x) := \{p \mid p \text{ ist Primteiler von } x\}.$$

ϕ ist ein Isomorphismus.

2.16 <u>Lemma:</u> Sei $\phi\colon B \to C$ ein Homomorphismus von der Algebra B nach der Algebra C. Dann gilt:

(a) $\phi(B) := \{\phi(x) \mid x \in B\}$ ist eine Unteralgebra von C.

(b) Ist B Boolesch, so auch $\phi(B)$.

<u>Beweis:</u> (a) Es ist die Abgeschlossenheit von $\phi(B)$ zu zeigen. Seien $a,b \in \phi(B)$. Es existieren $x,y \in B$ mit $\phi(x) = a$ und $\phi(y) = b$. Da B abgeschlossen ist, hat man $x+y \in B$ und $\phi(x+y) \in \phi(B)$. Nun ist aber $\phi(x+y) = \phi(x) + \phi(y)$*), und damit folgt $\phi(x) + \phi(y) = a+b \in \phi(B)$. Entsprechend verlaufen die übrigen Beweisschritte.

(b) Die Gültigkeit der Axiome (B_1)-(B_8) und $(\overline{B}_1)$-$(\overline{B}_8)$ ist nachzuweisen. Exemplarisch zeigen wir die Richtigkeit von (B_5). Seien $a,b,c \in \phi(B)$. Wir haben also $x,y,z \in B$ mit $\phi(x) = a$, $\phi(y) = b$ und $\phi(z) = c$. Es folgt dann $a+bc = \phi(x) + \phi(y)\phi(z) = \phi(x) + \phi(yz) = \phi(x+yz) = \phi((x+y)(x+z))$ $= \phi(x+y)\phi(x+z) = (\phi(x) + \phi(y))(\phi(x) + \phi(z)) = (a+b)(a+c)$.

---

*) Wir verzichten im folgenden darauf, für entsprechende Operationen in verschiedenen Algebren auch verschiedene Zeichen zu benutzen - sonst hätten wir hier natürlich $\phi(x+y) = \phi(x) \hat{+} \phi(y)$ (oder ähnliches) schreiben müssen.

Sei nun ϕ ein Homomorphismus von B nach C. Wir definieren

$$\ker \phi := \{(x,y) \mid x,y \in B \text{ und } \phi(x) = \phi(y)\}.$$

$\ker \phi$ heißt der Kern von ϕ.
Man erkennt leicht, daß $\ker \phi$ eine Äquivalenzrelation auf B ist. $\ker \phi$ hat jedoch weitere interessante Eigenschaften. Dazu definieren wir:

2.17 Definition: Eine Äquivalenzrelation Θ auf der Algebra $(B; +, \cdot, ', 0, 1)$ heißt Kongruenz(-relation), falls für alle $x_1, x_2, y_1, y_2 \in B$ gilt:

(i) $(x_1, y_1) \in \Theta$ zieht $(x_1', y_1') \in \Theta$ nach sich.
(ii) Mit $(x_1,y_1),(x_2,y_2) \in \Theta$ gilt auch
(x_1+x_2, y_1+y_2), $(x_1 \cdot x_2, y_1 \cdot y_2) \in \Theta$.
(Man sagt auch, Θ "respektiere" die Operationen $+, \cdot$ und $'$.)

2.18 Lemma: Sei $\phi: B \to C$ ein Homomorphismus. Dann ist $\ker \phi$ eine Kongruenz auf B.

Beweis: Mit $(x,y) \in \ker \phi$ bzw. $\phi(x) = \phi(y)$ gilt auch $(\phi(x))' = (\phi(y))'$, also $\phi(x') = \phi(y')$ und $(x',y') \in \ker \phi$.
Seien (x_1,y_1), $(x_2,y_2) \in \ker \phi$. Man hat $\phi(x_1) = \phi(y_1)$ und $\phi(x_2) = \phi(y_2)$. Es folgt
$\phi(x_1+x_2) = \phi(x_1) + \phi(x_2) = \phi(y_1) + \phi(y_2) = \phi(y_1+y_2)$ und entsprechend $\phi(x_1 \cdot x_2) = \phi(y_1 \cdot y_2)$, mithin $(x_1+x_2,\ y_1+y_2) \in \ker \phi$ und $(x_1 \cdot x_2,\ y_1 \cdot y_2) \in \ker \phi$.

Sei nun $(B; +, \cdot, ', 0, 1)$ eine Algebra und Θ eine Kongruenz auf B. Wir schreiben auch $x\Theta y$ statt $(x,y) \in \Theta$. Für $x \in B$ bezeichne $[x]\Theta$ die Kongruenzklasse von Θ, die x enthält, also $[x]\Theta = \{b \in B \mid x\Theta b\}$. Man beachte, daß $[x]\Theta = [y]\Theta$ gleichbedeutend ist mit $x\Theta y$.
Wir setzen $B/\Theta := \{[b]\Theta \mid b \in B\}$.

2.19 Lemma: Ist Θ eine Kongruenz auf der Algebra $(B; +, \cdot, ', 0, 1)$, so wird durch $[x]\Theta + [y]\Theta := [x+y]\Theta$, $[x]\Theta \cdot [y]\Theta := [x \cdot y]\Theta$ und $([x]\Theta)' := [x']\Theta$ eine Algebra $(B/\Theta; +, \cdot, ', [0]\Theta, [1]\Theta)$ erklärt.
(Diese nennt man eine Faktoralgebra von B.)

Beweis: Wir müssen zeigen, daß $+, \cdot, '$ Operationen auf B/Θ sind. M.a.W. muß nachgewiesen werden, daß die obigen Definitionen nicht von der

Auswahl der Repräsentanten in den Kongruenzklassen abhängen. Wenn also $[x_1]\Theta = [y_1]\Theta$ und $[x_2]\Theta = [y_2]\Theta$ ist, so muß $[x_1+x_2]\Theta = [y_1+y_2]\Theta$ sein. Dies ist aber gerade die Aussage der Verträglichkeit von Θ mit der Operation $+$. Entsprechendes gilt für $\cdot$ und $'$.

2.20 <u>Satz:</u> Seien $(B; +, \cdot, ', 0, 1)$ und $(C; +, \cdot, ', 0, 1)$ Algebren, Θ eine Kongruenzrelation auf B. Dann gilt:

(a) Definiert man $\phi_\Theta: B \to B/\Theta$ durch $\phi_\Theta(x) := [x]\Theta$, so ist ϕ_Θ ein surjektiver Homomorphismus mit $\ker \phi_\Theta = \Theta$.

(b) Ist $\phi: B \to C$ ein surjektiver Homomorphismus, so folgt $C \cong B/\ker \phi$.

<u>Beweis:</u> (a) Man sieht leicht ein, daß ϕ_Θ surjektiv und $\ker \phi_\Theta = \Theta$ ist. Weiter hat man aufgrund der Definition der Operationen in B/Θ $\phi_\Theta(x') = [x']\Theta = ([x]\Theta)' = (\phi_\Theta(x))'$; entsprechend folgt die Verträglichkeit mit $+$ und $\cdot$.

(b) Die Abbildung $\psi: B/\ker \phi \to C$ mit $\psi([b] \ker \phi) := \phi(b)$ ist offensichtlich wohldefiniert und bijektiv. Die Homomorphismusbedingung wird exemplarisch für $\cdot$ nachgeprüft:

$\psi([a] \ker \phi \cdot [b] \ker \phi) = \psi([a\cdot b] \ker \phi) = \phi(a\cdot b) = \phi(a)\cdot\phi(b) =$
$= \psi([a] \ker \phi) \cdot \psi([b] \ker \phi)$. Somit ist ψ ein Isomorphismus.

2.21 <u>Folgerung:</u> Ist B eine Boolesche Algebra und Θ eine Kongruenz auf B, so ist auch B/Θ eine Boolesche Algebra.

<u>Beweis:</u> Nach 2.20 ist B/Θ "homomorphes Bild" von B. Mit 2.16 folgt die Behauptung.

Einige kurze Erläuterungen zum Begriff der direkten Potenz sollen diesen Paragraphen abschließen.

Sei $(B; +, \cdot, ', 0, 1)$ eine Algebra und M eine beliebige Menge. Auf B^M, der Menge aller Abbildungen von M nach B, definieren wir Operationen $+$, $\cdot$ und $'$ durch "komponentenweises Rechnen": sind $g,h \in B^M$, so setzt man $(g+h)(m) := g(m) + h(m)$, $(g\cdot h)(m) := g(m)\cdot h(m)$ und $g'(m) := (g(m))'$ für $m \in M$. Die Elemente $0^M, 1^M \in B^M$ mit $0^M(m) := 0$ bzw. $1^M(m) := 1$ (für alle $m \in M$) sind die konstanten Funktionen mit Wert 0 bzw. 1. Man erhält so eine Algebra $(B^M; +, \cdot, ', 0^M, 1^M)$, die eine <u>(direkte) Potenz von B</u> genannt wird.

Der Beweis der folgenden Aussagen sei dem Leser als Übung empfohlen.

2.22 Lemma: Sei B eine Algebra, M eine Menge. Dann gilt:
(a) Für jedes $m \in M$ ist $\pi_m : B^M \to B$ mit $\pi_m(g) := g(m)$ ein surjektiver Homomorphismus.
(b) Ist B Boolesch, so auch B^M.

Die zweielementige Boolesche Algebra $(\{0,1\}; +, \cdot, ', 0, 1)$, die isomorph zu einer Unteralgebra jeder Booleschen Algebra ist, soll im folgenden stets mit $\mathbb{2}$ bezeichnet werden.
Wir wollen schließlich einen Satz zeigen, der an späterer Stelle erheblich verallgemeinert werden wird:

2.23 Satz: Für jede Menge X ist die Boolesche Algebra $\mathbb{P}(X)$ isomorph zu einer Potenz von $\mathbb{2}$.

Beweis: Man überzeugt sich leicht, daß die Abbildung $\psi : \mathbb{P}(X) \to \mathbb{2}^X$ mit

$$\psi(S)(m) := \begin{cases} 1, & \text{falls } m \in S \\ 0, & \text{falls } m \notin S \end{cases}$$

ein Isomorphismus ist.

<u>**Übungsaufgaben:**</u>

8. Man beschreibe die Kongruenzrelationen $\ker \phi$ zu den Homomorphismen in 2.15.

9. Sei $\mathbb{1}$ die "triviale", d.h. die einelementige Boolesche Algebra. Zeige, daß es für jede Boolesche Algebra B einen Homomorphismus $\alpha\colon B \to \mathbb{1}$ gibt, und bestimme $\ker \alpha$.

10. Sei X eine unendliche Menge. Zeige, daß
$\Theta := \{(A,B) \mid A,B \in \mathbb{P}(X),\ (A \cup B) \cap (\overline{A \cup B})$ ist endlich$\}$
eine Kongruenzrelation auf $\mathbb{P}(X)$ ist. Was ist $[\emptyset]\Theta$?

11. Sei M eine unendliche Menge. Für Elemente $f,g \in \mathbb{2}^M$ sagt man, f sei "fast überall gleich" g, falls die Menge $\{m \in M \mid f(m) \neq g(m)\}$ endlich ist. Man zeige, daß
$\Theta_F := \{(f,g) \mid f$ ist fast überall gleich $g\}$ eine Kongruenzrelation auf $\mathbb{2}^M$ ist.

12. Sei X eine Menge und $\phi\colon \mathbb{P}(X) \to \mathbb{2}$ ein Homomorphismus. Seien $A,B \in \mathbb{P}(X)$ mit $A \subseteq B$. Zeige, daß $\phi(B) = 0$ auch $\phi(A) = 0$ nach sich zieht.

§ 3. BOOLESCHE TERME

In den nächsten Paragraphen wollen wir die Theorie der Booleschen Algebren in der Schaltalgebra zur Anwendung bringen. Wir haben gesehen, daß einem Schaltkreis in eindeutiger Weise ein algebraischer Ausdruck zugeordnet ist und daß von diesem eine Schaltfunktion induziert wird. Wichtig für die Anwendungen ist das Problem, zu einer gegebenen Funktion $f\colon \mathbf{2}^n \to \mathbf{2}$ eine Schaltung zu finden, die diese Funktion realisiert.
Als einfaches Beispiel möge das folgende Problem dienen:

> "In einem Zimmer soll eine Lampe von drei verschiedenen Schaltern unabhängig ein- oder ausgeschaltet werden können. Man konstruiere einen Schaltkreis."

Wird noch willkürlich fortgesetzt, daß die Lampe nicht aufleuchten soll, falls alle Schalter offen sind, so erhält man die in der folgenden Tabelle beschriebene Schaltfunktion:

x	y	z	f(x,y,z)
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Unser Problem würde also lauten: "Ist es möglich, diese Funktion durch einen Schaltkreis zu realisieren? Wenn ja, wie findet man einen solchen?" Dieser und der folgende Paragraph werden uns in die Lage versetzen, solche und ähnliche Probleme auf einfache Weise zu lösen.

Sei $X = \{x_1, x_2, x_3, \dots\}$ eine Menge von Variablen und $0, 1, +, \cdot, {}', (,)$ Symbole, die nicht in X liegen. Unter einem <u>Booleschen Term</u> wollen wir einen Ausdruck verstehen, der sich aus den Variablen und den obigen Symbolen "sinnvoll" bilden läßt.

3.1 Definition von Booleschen Termen

a) Jede Variable x_i ist ein Boolescher Term, ebenso 0 und 1.

b) Sind p und q Boolesche Terme, so sind auch $(p+q)$, $(p\cdot q)$ und p' Boolesche Terme.

c) Boolesche Terme sind genau die Zeichenreihen (Ausdrücke), die sich mit a) und b) in endlich vielen Schritten konstruieren lassen.

Die Menge aller Booleschen Terme (über der Variablenmenge X) wollen wir mit $\mathcal{B}(X)$ bezeichnen.
Beispiele für Boolesche Terme sind $((x_1+x_3)'\cdot x_1')'$, x_5''', $((x_1\cdot x_1) + (x_2\cdot(x_3+x_7)))$. Man beachte, daß Boolesche Terme *nur dann* gleich sind, falls sie dieselbe Zeichenreihe darstellen - z.B. gilt $(x_1\cdot x_1) \neq x_1$, $0' \neq 1$, $x_1'' \neq x_1$, $(0+1) \neq 1$; dies ist analog der Situation bei Schaltkreisen (vgl. 3.1 mit 1.1!).
Aufgrund von 3.1 hat man nun sofort:

3.2 Bemerkung: $(\mathcal{B}(X); +, \cdot, ', 0, 1)$ ist eine Algebra, jedoch keine Boolesche Algebra.

Sei nun p ein Boolescher Term. Wir gehen von einem intuitiven Verständnis davon aus, daß eine Variable x_i in p "vorkommt".*)
Aus 3.1 ergibt sich, daß in jedem Booleschen Term nur endlich viele Variablen vorkommen können. Es wird für das weitere nichts ausmachen, daß wir X stets als endliche Menge $\{x_1,\ldots,x_n\}$ voraussetzen. Ein $p \in \mathcal{B}(X)$ werden wir gelegentlich auch als $p(x_1,\ldots,x_n)$ aufschreiben.

Ist B eine (Boolesche) Algebra, so induziert jedes $p \in \mathcal{B}(X)$ auf kanonische Weise eine Abbildung $p^B\colon B^n \to B$. Ist nämlich $(b_1,\ldots,b_n) \in B^n$, so erhält man $p^B(b_1,\ldots,b_n)$, indem man jedes in p vorkommende x_i durch das Element $b_i \in B$ ersetzt und den so erhaltenen Ausdruck in der Algebra B auswertet. Die Abbildung p^B nennt man die zu p gehörende Boolesche Funktion (auf B).

Formal müßte man p^B entsprechend zu Definition 3.1 induktiv definieren:

a) $x_i^B(b_1,\ldots,b_n) := b_i$ (x_i^B ist also die i-te Projektion),
$0^B(b_1,\ldots,b_n) := 0$, $1^B(b_1,\ldots,b_n) := 1$.

b) Ist $p = p_1+p_2$ (bzw. $p = p_1\cdot p_2$ bzw. $p = p_1'$) und sind p_1^B und p_2^B bereits definiert, so setzt man
$(p_1+p_2)^B(b_1,\ldots,b_n) := p_1^B(b_1,\ldots,b_n) + p_2^B(b_1,\ldots,b_n)$,
$(p_1\cdot p_2)^B(b_1,\ldots,b_n) := p_1^B(b_1,\ldots,b_n) \cdot p_2^B(b_1,\ldots,b_n)$ sowie
$(p_1')^B(b_1,\ldots,b_n) := (p_1^B(b_1,\ldots,b_n))'$.

---

*) Man könnte etwa definieren: x_i kommt in p vor, falls $p \notin \langle X - \{x_i\}\rangle_{\mathcal{B}(X)}$ gilt.

Man liest nun sofort ab:

3.3 <u>Folgerung:</u> Die Zuordnung $p \to p^B$ definiert einen Homomorphismus von $\mathcal{B}(X)$ nach B^{B^n}.

<u>Anmerkung:</u> B^{B^n} ist die Potenzalgebra von B mit $M = B^n$. B^{B^n} ist als Menge die Menge aller n-stelligen Operationen auf B.

Die Elemente von $\mathcal{B}(X)$ korrespondieren (in eindeutiger Weise) zu den Schaltkreisen.

Setzt man in 3.3 für B die zweielementige Boolesche Algebra $\mathbf{2}$, so ist $\mathbf{2}^{\mathbf{2}^n}$ gerade die Menge aller Abbildungen von $\mathbf{2}^n$ in $\mathbf{2}$. Gibt es für eine solche Abbildung $f \in \mathbf{2}^{\mathbf{2}^n}$ einen Term p mit $p^{\mathbf{2}} = f$, so können wir f durch den p entsprechenden Serien-Parallel-Schaltkreis "realisieren".
Im folgenden Abschnitt werden wir

- zeigen, daß es zu jeder Abbildung $f \in \mathbf{2}^{\mathbf{2}^n}$ ein $p \in \mathcal{B}(X)$ gibt mit $p^{\mathbf{2}} = f$, daß m.a.W. die Zuordnung $p \to p^{\mathbf{2}}$ surjektiv ist;
- eine Methode angeben, wie man ein solches p findet.

§ 4. DISJUNKTIVE NORMALFORMEN

In 3.3 haben wir gesehen, daß die Abbildung $-^B$, die jedem Booleschen Term p die Boolesche Funktion p^B zuordnet, ein Homomorphismus von $\mathcal{B}(X)$ nach B^{B^n} ist. Wichtig für den Spezialfall $B = \mathbf{2}$ ist nun:

4.1 <u>Satz:</u> $-^{\mathbf{2}}$ ist ein surjektiver Homomorphismus von $\mathcal{B}(X)$ auf $\mathbf{2}^{\mathbf{2}^n}$.

Vor dem Beweis von 4.1 soll eine weitere Bezeichnung eingeführt werden: ist $f \in \mathbf{2}^{\mathbf{2}^n}$, so nennen wir die Menge

$$T(f) := \{(\alpha_1,\ldots,\alpha_n) \mid \alpha_i \in \mathbf{2},\ f(\alpha_1,\ldots,\alpha_n) = 1\}$$

den <u>Träger von f</u>.
Ferner werden wir die Schreibweise a^α (a Element einer Algebra, $\alpha \in \{0,1\}$) verwenden; dabei soll $a^0 := a'$ und $a^1 := a$ sein.

<u>Beweis von 4.1:</u> Wir betrachten zunächst zu einer beliebigen 0-1-Folge $(\alpha_1,\ldots,\alpha_n) \in \mathbf{2}^n$ die Funktion $\chi_{(\alpha_1,\ldots,\alpha_n)}: \mathbf{2}^n \to \mathbf{2}$, die folgendermaßen definiert ist:

$$\chi_{(\alpha_1,\ldots,\alpha_n)}(a_1,\ldots,a_n) := \begin{cases} 1, & \text{falls } a_1 = \alpha_1,\ a_2 = \alpha_2,\ \ldots,\ a_n = \alpha_n \\ 0, & \text{sonst.} \end{cases}$$

Wir behaupten, daß es zu dieser Funktion ein Urbild in $\mathcal{B}(X)$ gibt, nämlich den Booleschen Term $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_1}$; m.a.W. ist die Behauptung:

$$\chi_{(\alpha_1,\ldots,\alpha_n)} = (x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n})^{\mathbf{2}} .$$

Dies kann man sich folgendermaßen klarmachen: Zunächst ist für $\alpha,\beta \in \mathbf{2}$ offenbar $\beta^\alpha = 1$ gleichbedeutend mit $\alpha = \beta$; dies bedeutet aber, daß $(x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n})^{\mathbf{2}}(\beta_1,\ldots,\beta_n) = \beta_1^{\alpha_1} \cdot \ldots \cdot \beta_n^{\alpha_n}$ nur im Falle $(\beta_1,\ldots,\beta_n) = (\alpha_1,\ldots,\alpha_n)$ den Wert 1 annimmt.

Nun sei $f: \mathbf{2}^n \to \mathbf{2}$ beliebig. Wir behaupten, daß

$$f = \sum_{(\alpha_1,\ldots,\alpha_n) \in T(f)} \chi_{(\alpha_1,\ldots,\alpha_n)}$$

gilt, wobei das Σ-Zeichen seine offensichtliche Bedeutung hat. Für ein beliebiges $(\beta_1,\ldots,\beta_n) \in \mathbf{2}^n$ ist nämlich genau dann

$$\sum_{(\alpha_1,\ldots,\alpha_n)\in T(f)} (\chi_{(\alpha_1,\ldots,\alpha_n)}(\beta_1,\ldots,\beta_n)) = 1,$$

wenn mindestens *ein* Summand den Wert 1 hat, also $(\beta_1,\ldots,\beta_n) \in T(f)$ bzw. $f(\beta_1,\ldots,\beta_n) = 1$ gilt.

Damit ist gezeigt, daß f von dem Booleschen Term

$$\sum_{(\alpha_1,\ldots,\alpha_n)\in T(f)} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$$ induziert wird.

Wir wollen die sich aus dem Beweis von 4.1 ergebende stärkere Aussage noch einmal herausstellen:

4.2 <u>Folgerung:</u> Für eine beliebige Abbildung $f\colon \mathbf{2}^n \to \mathbf{2}$ gilt

$$f = \Big(\sum_{(\alpha_1,\ldots,\alpha_n)\in T(f)} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}\Big)^{\mathbf{2}} .$$

Jede solche Abbildung ist also eine Boolesche Funktion.

Gehen wir nun einmal zu dem am Anfang des vorigen Paragraphen geschilderten Problem der Lampe zurück, die von drei Schaltern aus unabhängig geschaltet werden sollte. Es ergab sich die folgende Funktionstabelle:

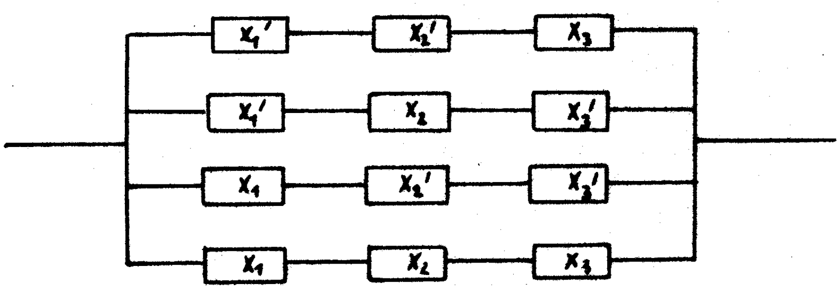
x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Es ist also $T(f) = \{(0,0,1),\ (0,1,0),\ (1,0,0),\ (1,1,1)\}$.

Mit Folgerung 4.2 hat man

$$f = (x_1' \, x_2' \, x_3 + x_1' \, x_2 \, x_3' + x_1 \, x_2' \, x_3' + x_1 \, x_2 \, x_3)^{\mathbf{2}} .$$

Damit kann man f durch einen Serien-Parallel-Schaltkreis darstellen:



Dieser kann natürlich noch vereinfacht werden, etwa durch Anwendung der Distributivgesetze.

<u>Anmerkung:</u> Die Verwendung des Summenzeichens in Booleschen Termen (in 4.1 und 4.2) ist eigentlich nicht gerechtfertigt, da in $\mathcal{B}(X)$ Assoziativ- und Kommutativitätsgesetze nicht gelten. Wir können dies jedoch damit verteidigen, daß alle "richtigen" Booleschen Terme, die durch Umordnen und Umklammern entstehen können, *äquivalent* sind in dem Sinne, daß sie stets gleiche Boolesche Funktionen induzieren. Dieser Äquivalenzbegriff wird unser nächstes Thema sein.

<u>Übungsaufgaben:</u>

13. Man realisiere die Schaltfunktionen, die durch die folgende Tabelle gegeben sind, durch einen Schaltkreis:

x_1	x_2	x_3	$f(x_1,x_2,x_3)$	$g(x_1,x_2,x_3)$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	0
0	1	1	0	0
1	0	0	1	1
1	0	1	0	1
1	1	0	0	0
1	1	1	0	1

14. Für ein Gremium von drei Personen soll eine Abstimmungsschaltung entworfen werden. Ein Lämpchen soll brennen, wenn die Mehrheit "dafür ist", d.h. wenn mindestens zwei Personen ihre Schalter schließen. Schreibe die Schaltfunktion in einer Tabelle auf und entwirf eine Schaltung.

15. In einem zweitürigen Wagen soll die Innenbeleuchtung brennen, falls eine der Türen offen ist oder ein Schalter im Innenraum betätigt wird. Man entwerfe eine Schaltung.

4.3 Definition: Eine Gleichung ist ein Paar $(p,q) \in \mathcal{B}(X)^2$. Eine Gleichung (p,q) gilt in einer (Booleschen) Algebra $\underline{B}$, falls $p^B = q^B$ ist, also die Terme p und q dieselbe Boolesche Funktion auf B induzieren. Wir schreiben $p \underset{B}{\equiv} q$, falls die Gleichung (p,q) in B gilt, und $p \equiv q$, falls (p,q) in *allen* Booleschen Algebren gilt; im Falle $p \equiv q$ sagt man, p und q seien äquivalent.

4.4 Beispiel: Wir wollen uns klarmachen, daß die Gleichung $((x_1 \cdot (x_2+x_3)), ((x_1 \cdot x_2) + (x_1 \cdot x_3)))$ in allen Booleschen Algebren gilt, also $x_1 \cdot (x_2+x_3) \equiv (x_1 \cdot x_2) + (x_1 \cdot x_3)$. Es ist für eine beliebige Boolesche Algebra B $(x_1 \cdot (x_2+x_3))^B = ((x_1 \cdot x_2) + (x_1 \cdot x_3))^B$ zu zeigen. Nun folgt aber für $b_1, b_2, b_3 \in B$: $(x_1 \cdot (x_2+x_3))^B(b_1,b_2,b_3) = b_1 \cdot (b_2+b_3) = b_1b_2 + b_1b_3 = ((x_1 \cdot x_2) + (x_1 \cdot x_3))^B(b_1,b_2,b_3)$, womit alles bewiesen ist. Entsprechend kann man die Gesetze (B_1)-(B_8) und $(\overline{B}_1)$-$(\overline{B}_8)$ als Gleichungen schreiben, die in allen Booleschen Algebren gelten.

4.5 Lemma: Für jede Boolesche Algebra B ist $\underset{B}{\equiv}$ eine Kongruenzrelation auf $\mathcal{B}(X)$. $\equiv$ ist ebenfalls eine Kongruenzrelation auf $\mathcal{B}(X)$.

Beweis: $p \underset{B}{\equiv} q$ ist gleichbedeutend mit $p^B = q^B$, also ist $\underset{B}{\equiv}$ der Kern des Homomorphismus $-^B : \mathcal{B}(X) \to B^{B^n}$. Da $\equiv$ der Durchschnitt aller $\underset{B}{\equiv}$ ist, ist alles gezeigt, denn der Schnitt von Kongruenzrelationen ist, wie man leicht nachrechnet, stets wieder eine Kongruenz$\bullet$

Die Aussage von 4.5 kann man so interpretieren, daß man mit Gleichungen operieren kann, wie man es intuitiv von dem Konzept "Gleichung" auch erwartet: beispielsweise darf man auf beiden Seiten einer Gleichung "Gleiches" addieren und erhält wieder eine Gleichung, usw.

Betrachten wir uns einmal den Term $(x_1 + ((x_2+x_3)' \cdot x_4))'$. Mit Hilfe der De Morganschen Regeln und der Distributivgesetze leitet man ab:

$$(x_1+((x_2+x_3)' \cdot x_4))' \equiv (x_1+x_2'x_3'x_4)' \equiv x_1' \cdot (x_2+x_3+x_4') \equiv x_1'x_2 + x_1'x_3 + x_1'x_4' .$$

Ähnlich kann man mit jedem Term verfahren. Wendet man zunächst die De Morganschen Regeln und danach die Distributivgesetze an, so kann man einen äquivalenten Term finden, der eine Summe von Produkttermen ist. Dabei ist ein Produktterm ein Term der Form $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$. (Wir verzichten hier wieder auf eine Klammerung, da die Aussage für jede Klammerung gilt.) Man schafft also die Komplemente mit Hilfe der De Morganschen

Gesetze "nach innen" und multipliziert dann mit dem Distributivgesetz ($\overline{B}_5$) aus.

In den Produkttermen unseres Beispiels fehlen noch einige Faktoren; z.B. ist $x_1'x_2$ nicht von der Form $x_1^{\alpha_1} \cdot \ldots \cdot x_4^{\alpha_4}$, die Variablen x_3 und x_4 kommen in $x_1'x_2$ nicht vor; dem kann durch "Aufblasen" abgeholfen werden:

$$x_1'x_2 \equiv x_1'x_2(x_3+x_3')(x_4+x_4') \equiv x_1'x_2x_3x_4 + x_1'x_2x_3x_4' + x_1'x_2x_3'x_4 + x_1'x_2x_3'x_4'.$$

Entsprechend verfährt man mit den Termen $x_1'\cdot x_3$ und $x_1'\cdot x_4'$. Summation ergibt dann einen Term, der eine Summe von Produkttermen ist und äquivalent ist zu dem Ausgangsterm p. Den so erhaltenen Term, in dem aufgrund der Kommutativ- und Idempotenzgesetze o.B.d.A. jeder Produktterm höchstens einmal als Summand auftaucht, nennen wir <u>die disjunktive Normalform von p</u>, kurz auch DNF.

4.6 <u>Beispiel:</u> $(x_1 + (x_2\cdot x_3))'$ soll in disjunktiver Normalform geschrieben werden:

$$\left.\begin{array}{l} (x_1 + (x_2\cdot x_3))' \equiv \\ \equiv x_1' \cdot (x_2\cdot x_3)' \equiv \end{array}\right\} \text{de Morgansche Regeln}$$

$$\left.\begin{array}{l} \equiv x_1' \cdot (x_2'+x_3') \equiv \\ \equiv x_1'x_2' + x_1'x_3' \equiv \end{array}\right\} \text{Distributivgesetz}$$

$$\left.\begin{array}{l} \equiv x_1'x_2'(x_3+x_3') + x_1'x_3'(x_2+x_2') \equiv \\ \equiv x_1'x_2'x_3 + x_1'x_2'x_3' + x_1'x_2x_3' + x_1'x_2'x_3' \equiv \end{array}\right\} \begin{array}{l}\text{"Aufblasen"} \\ \text{(und Kommutativgesetz)}\end{array}$$

$$\left.\begin{array}{l} \equiv x_1'x_2'x_3 + x_1'x_2'x_3' + x_1'x_2'x_3' \equiv \\ \equiv x_1'x_2'x_3 + x_1'x_2'x_3' + x_1'x_2x_3' \end{array}\right\} \text{Idempotenz}$$

Dem folgenden Satz kommt in der Theorie der Booleschen Algebren zentrale Bedeutung zu:

4.7 <u>Satz</u> (NORMALFORMENTHEOREM):
Zu jedem Booleschen Term p gibt es *genau einen* äquivalenten Term in disjunktiver Normalform.

<u>Beweis:</u> Daß es überhaupt einen zu p äquivalenten Term in disjunktiver Normalform gibt, haben wir an Beispielen demonstriert; wir haben auch eine Methode angegeben, wie man einen solchen findet. Den leichten Induktionsbeweis, daß diese Methode stets zum Ziel führt, wollen wir auslassen. Nun gibt es genau 2^{2^n} viele Terme (bei n Variablen) in disjunktiver

Normalform. Andererseits läßt sich nach 4.2 jede Funktion $f: \mathbf{2}^n \to \mathbf{2}$ als Boolesche Funktion eines Terms in disjunktiver Normalform auffassen, weshalb zwei verschiedene Terme in disjunktiver Normalform nicht äquivalent sein können. Somit kann ein beliebiger Boolescher Term p auch nur zu *einem* Term in disjunktiver Normalform äquivalent sein.

Jeder Boolesche Term ist also äquivalent zu einer Summe von Produkttermen $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, wobei $\alpha_i \in \{0,1\}$ ist. Welche Produktterme treten nun aber in der Summe auf? Die Antwort gibt uns 4.2; sie lautet:

4.8 <u>Folgerung:</u> Für jeden Booleschen Term $p(x_1,\ldots,x_n)$ gilt

$$p(x_1,\ldots,x_n) \equiv \sum_{(\alpha_1,\ldots,\alpha_n) \in T(p^{\mathbf{2}})} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} .$$

(Wir erinnern daran, daß $T(p^{\mathbf{2}}) = \{(\alpha_1,\ldots,\alpha_n) \in \mathbf{2}^n \mid p^{\mathbf{2}}(\alpha_1,\ldots,\alpha_n) = 1\}$ der Träger von $p^{\mathbf{2}}$ ist.)

Ist ein Boolescher Term p gegeben, so sagen uns 4.2 bzw. 4.8, daß man zum Aufstellen der disjunktiven Normalform von p nur den Träger von $p^{\mathbf{2}}$ zu ermitteln braucht. (Nebenbei sei bemerkt, daß 4.2 auch im Beweis von 4.7 - Existenz eines äquivalenten Terms in disjunktiver Normalform - hätte benutzt werden können.)

4.9 <u>Beispiel:</u> Wir suchen die disjunktive Normalform von $p(x_1,x_2,x_3) := (x_1 \cdot (x_2+x_3))'$. Zur Ermittlung des Trägers stellen wir eine Tabelle auf:

x_1	x_2	x_3	$p^{\mathbf{2}}(x_1,x_2,x_3)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Also ist $T(p^{\mathbf{2}}) = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0)\}$ und
$p \equiv x_1'x_2'x_3' + x_1'x_2'x_3 + x_1'x_2x_3' + x_1'x_2x_3 + x_1x_2'x_3'$.

Einige weitere Folgerungen aus dem Normalformentheorem und 4.8 sollen den Abschluß dieses Paragraphen bilden.

4.10 Folgerung: Sind $p(x_1,\dots,x_n)$ und $q(x_1,\dots,x_n)$ Boolesche Terme, so sind p und q genau dann äquivalent, wenn sie denselben Träger besitzen.

4.11 Folgerung: Gilt die Gleichung (p,q) in der Booleschen Algebra $\mathbf{2}$, so gilt sie in allen Booleschen Algebren. ($p \underset{\mathbf{2}}{\equiv} q$ ist gleichbedeutend mit $p \equiv q$.)

Die Aussage von 4.11 ist außergewöhnlich in dem Sinne, daß es bei den meisten algebraischen Strukturen eines bestimmten Typs (etwa bei Gruppen) *nicht* der Fall ist, daß man die *allgemeine* Gültigkeit von Gleichungen für diese Strukturen an *einer* endlichen Struktur "abtesten" kann. Man hat hier noch als Konsequenz, daß es einen Algorithmus gibt, der zu je zwei vorgelegten Booleschen Termen p und q (in endlich vielen Schritten) entscheiden kann, ob $p \equiv q$ gilt oder nicht; man sagt, das "Wortproblem für Boolesche Algebren" sei "entscheidbar".

Der Vollständigkeit halber muß noch erwähnt werden, daß es dual zur disjunktiven Normalform natürlich die konjunktive Normalform gibt. Ohne damit arbeiten zu wollen, halten wir nur fest:

4.12 Folgerung: Für einen beliebigen Booleschen Term $p(x_1,\dots,x_n)$ gilt

$$p(x_1,\dots,x_n) \equiv \prod_{(\alpha_1,\dots,\alpha_n) \notin T(p^{\mathbf{2}})} (x_1^{\alpha_1'} + \dots + x_n^{\alpha_n'}) .$$

Beweis: Man schreibe p' in disjunktiver Normalform und komplementiere beide Seiten.

§ 5. SCHALTALGEBRA II

Die Elemente von $\mathcal{B}(X)$ (mit $X = \{x_1,\ldots,x_n\}$) korrespondieren, wie wir gesehen haben, zu den Serien-Parallel-Schaltkreisen, die aus einem festen Vorrat von n Schaltelementen aufgebaut sind.
Durch Kombination der Aussagen von 4.1, 2.20(b) und 4.11 können wir unsere Erkenntnisse über Schaltkreise und Schaltfunktionen wie folgt zusammenfassen:

5.0 <u>Satz:</u> Die Abbildung $\sigma: \mathcal{B}(X)/\equiv \;\to \mathbf{2}^{\mathbf{2}^n}$ mit $\sigma([p]\equiv) := p^{\mathbf{2}}$ ist ein Isomorphismus.

Als eine weitere Konsequenz daraus soll festgehalten werden, daß die Menge der Projektionen $\{\pi_1,\ldots,\pi_n\}$ $(\pi_i := x_i^{\mathbf{2}} \in \mathbf{2}^{\mathbf{2}^n})$ die Algebra $\mathbf{2}^{\mathbf{2}^n}$ erzeugt. (Dies ist natürlich nur eine Umformulierung unserer alten Erkenntnis, daß jede Boolesche Funktion $\mathbf{2}^n \to \mathbf{2}$ Schaltfunktion ist.)

Es muß noch darauf hingewiesen werden, daß in der Literatur zur Booleschen Algebra häufig nicht genau zwischen den Strukturen $\mathcal{B}(X)$, $\mathcal{B}(X)/\equiv$ und $\mathbf{2}^{\mathbf{2}^n}$ differenziert wird. Dies führt nicht zu schwerwiegenden Fehlern, jedoch kann die Klarheit der Zusammenhänge verlorengehen.

Wir wenden uns jetzt dem Problem zu, zu einer gegebenen Schaltfunktion $f: \mathbf{2}^n \to \mathbf{2}$ einen möglichst *einfachen* Booleschen Term p (bzw. Schaltkreis) mit $p^{\mathbf{2}} = f$ zu finden. Es leuchtet ein, daß dies bei der technischen Realisierung von Schaltkreisen aus Kostengründen eine Rolle spielt.
Sehen wir uns ein Beispiel an.
$f: \mathbf{2}^3 \to \mathbf{2}$ sei durch folgende Tabelle gegeben:

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Die disjunktive Normalform von f lautet

$$x_1'x_2'x_3 + x_1'x_2x_3' + x_1x_2'x_3' + x_1x_2'x_3 + x_1x_2x_3' + x_1x_2x_3.$$

Wir erhalten also einen Term mit $|T(f)|$ vielen Summanden und benötigen somit zur Realisierung von f $3\cdot|T(f)| = 18$ Schaltelemente. Die konjunktive Normalform von f ist $(x_1+x_2+x_3)(x_1+x_2'+x_3')$ und führt zu einer Realisierung von f mit nur sechs Schaltelementen. Wir rechnen mit der konjunktiven Normalform weiter und erhalten

$$\begin{aligned}(x_1+x_2+x_3)(x_1+x_2'+x_3') &\equiv x_1 + (x_2+x_3)(x_2'+x_3')\\ &\equiv x_1 + x_2x_2' + x_2x_3' + x_3x_2' + x_3x_3'\\ &\equiv x_1 + x_2x_3' + x_2'x_3.\end{aligned}$$

Die dem letzten Term entsprechende Schaltung ist sicher von den bisher angebotenen die einfachste. Dieser Term ist eine Summe von Produkten von (eventuell komplementierten) Variablen; diese Produkte sind jedoch nicht (notwendig) Produktterme der Art, wie sie in einer disjunktiven Normalform auftreten - z.B. kommen ja die Variablen x_2 und x_3 in dem ersten Produkt (nämlich x_1) nicht vor.

Es soll nun die Relation "einfacher als" zwischen Termen genauer gefaßt werden. Da wir bereits wissen, daß wir zu jedem Term eine Summe von Produkten finden können, die zu diesem äquivalent ist (z.B. die disjunktive Normalform), können wir uns dabei auf Summen von Produkten (Abkürzung: SvP) beschränken.

5.1 <u>Definition:</u> Sei p ein SvP-Term. Wir setzen
$s(p)$:= Anzahl der Summanden von p;
$v(p)$:= Anzahl der in p vorkommenden Variablen, wobei mehrfach vorkommende Variablen entsprechend mehrfach gezählt werden.

5.2 <u>Beispiel:</u> Für $p = x_1x_2'x_3 + x_1x_3$ hat man $s(p) = 2$ und $v(p) = 5$.

5.3 <u>Definition:</u> Seien p und q SvP-Terme. p heißt <u>einfacher als</u> q, falls $s(p) < s(q)$ und $v(p) \leq v(q)$
oder $s(p) \leq s(q)$ und $v(p) < v(q)$ ist.

5.4 <u>Beispiel:</u> $x_1x_2'x_3 + x_1x_3$ ist einfacher als $x_1x_3 + x_2x_3'x_4x_5'$, x_1x_2 ist einfacher als x_1+x_2; dagegen sind $x_1x_2' + x_3x_4$ und $x_1+x_2+x_3$ bezüglich der Einfachheit nicht vergleichbar.

Uns interessiert die Relation "einfacher als" nur zwischen äquivalenten Termen. Der sich ergebende Optimalitätsbegriff ist in der folgenden Definition beschrieben:

5.5 <u>Definition:</u> Ein SvP-Term p heißt <u>minimal</u>, wenn es keinen zu p äquivalenten SvP-Term q gibt, der einfacher ist als p.

Unser Problem besteht also darin, zu einem gegebenen SvP-Term p einen äquivalenten minimalen SvP-Term q zu finden.
Nun ist es zwar keine Beschränkung der Allgemeinheit anzunehmen, daß p ein SvP-Term ist - sehr wohl jedoch ist dies die Annahme, daß der gesuchte (möglichst einfache) Term wieder ein solcher zu sein habe. Zur Lösung des *allgemeinen* Problems (ohne diese Annahme) sind keine guten Verfahren bekannt. Weiter sollte angemerkt werden, daß auch in Definition 5.3 ("einfacher als") noch eine gewisse Willkür steckt; die gewählte Definition hat den Vorzug, einigermaßen plausibel und außerdem im weiteren gut "verarbeitbar" zu sein.

Das nächste Ziel ist es, Eigenschaften der Summanden in einem minimalen SvP-Term herauszuarbeiten. Diese Eigenschaften werden später zu Methoden führen, diese Summanden zu finden.

5.6 <u>Definition:</u> Seien p und q Terme. Man sagt, p <u>impliziere</u> q (in Zeichen: $p \hookrightarrow q$), falls $T(p^{\mathbf{2}}) \subseteq T(q^{\mathbf{2}})$ gilt.

Ohne Beweis merken wir an, daß $p \hookrightarrow q$ auch mit $p \cdot q \equiv p$ gleichbedeutend ist. Ferner besagen $p \hookrightarrow q$ und $q \hookrightarrow p$ zusammen gerade $p \equiv q$.

5.7 <u>Beispiele:</u> Es gilt $x_1 \hookrightarrow x_1 + x_2$, $x_1x_2 \hookrightarrow x_1$, $x_1x_2'x_3 \hookrightarrow x_1x_3$.

5.8 <u>Definition:</u> Seien $p_o, p \in \mathcal{B}(X)$ und p_o ein Produkt. p_o heißt ein <u>Primimplikant</u> von p, wenn $p_o \hookrightarrow p$ ist, jedoch für alle anderen in p_o enthaltenen Produkte $\overline{p}_o$ (die m.a.W. durch Weglassen von Buchstaben in p_o entstehen) gilt $\overline{p}_o \not\hookrightarrow p$.

5.9 <u>Beispiel:</u> Sei $p := x_1x_2 + x_1x_2'x_3 + x_1'x_2'x_3$. $p_o := x_1x_3$ ist ein Primimplikant: $T(p_o^{\mathbf{2}}) = \{(\alpha_1,\alpha_2,\alpha_3) \mid \alpha_1 = \alpha_3 = 1\}$, und für $\alpha_1 = \alpha_3 = 1$ hat man $p^{\mathbf{2}}(\alpha_1,\alpha_2,\alpha_3) = 1\cdot\alpha_2 + 1\cdot\alpha_2'\cdot 1 + 0\cdot\alpha_2'\cdot 1 = \alpha_2+\alpha_2' = 1$, also gilt $T(p_o^{\mathbf{2}}) \subseteq T(p^{\mathbf{2}})$ bzw. $p_o \hookrightarrow p$. p_o hat nur zwei echte Teilprodukte, nämlich x_1 und x_3. Wegen $(1,0,0) \in T(x_1^{\mathbf{2}}) \setminus T(p^{\mathbf{2}})$ und $(0,1,1) \in T(x_3^{\mathbf{2}}) \setminus T(p^{\mathbf{2}})$ ist sowohl $x_1 \not\hookrightarrow p$ als auch $x_3 \not\hookrightarrow p$. Damit ist

p_o als Primimplikant von p nachgewiesen.

Der nun folgende Satz zeigt die Bedeutung der Primimplikanten für das Auffinden minimaler SvP-Terme (zur Vorbereitung löse man Aufg. 18 und 19):

5.10 __Satz:__ Sei p ein minimaler SvP-Term. Dann ist p eine Summe von Primimplikanten von p.

__Beweis:__ Sei $p = p_1 + p_2 + \dots + p_k$, wobei jedes p_i ein Produkt sei. Wir nehmen o.B.d.A. an, p_1 sei kein Primimplikant. Dann gibt es ein in p_1 enthaltenes (einfacheres) $\overline{p}_1$ mit $\overline{p}_1 \Rightarrow p$. Wir erhalten $\overline{p}_1 + p_2 + \dots + p_k \Rightarrow p + p_2 + \dots + p_k \equiv p$. Aus der trivialerweise gültigen Beziehung $p_1 \Rightarrow \overline{p}_1$ folgt umgekehrt
$p = p_1 + p_2 + \dots + p_k \Rightarrow \overline{p}_1 + p_2 + \dots + p_k$ und damit
$p \equiv \overline{p}_1 + p_2 + \dots + p_k$. Somit ist ein einfacherer zu p äquivalenter Term gefunden, was der Minimalität von p widerspricht.

Der vorstehende Satz gibt eine *notwendige* Bedingung für das Vorliegen eines minimalen SvP-Terms an. Daß die Bedingung noch nicht hinreichend ist, zeigt das folgende Beispiel:

5.11 __Beispiel:__ Sei $p := x_1x_2 + x_1x_3 + x_2x_3'$. Alle Summanden sind Primimplikanten von p, jedoch ist p nicht minimal: $p \equiv x_1x_3 + x_2x_3'$.

Jeder SvP-Term p ist äquivalent zur Summe aller seiner Primimplikanten. Dies folgt aus 5.10 und der Tatsache, daß p zu einem minimalen SvP-Term äquivalent ist.
Unsere Strategie für das Auffinden eines minimalen SvP-Terms, der zu p äquivalent ist, wird darin bestehen,
erstens p als Summe aller Primimplikanten von p darzustellen und
zweitens in dieser Darstellung "überflüssige" Primimplikanten zu streichen. Die __Verschmelzungsmethode__ geht diesen Weg.
Es erscheint natürlich umständlich, zunächst *alle* Primimplikanten zu bestimmen, und dann wieder einen Teil von ihnen zu streichen. Ein allgemeines Verfahren, das diesen Weg abkürzt, ist bisher nicht bekannt.

Übungsaufgaben:

16. Man stelle den Term $(x_1+x_2x_3)(x_1'x_2+x_4)'$ in disjunktiver und in konjunktiver Normalform dar.

17. Zeige, daß die Gleichung $(xy' + x'y + yz' + y'z,\ xy' + x'z + yz')$ in jeder Booleschen Algebra gilt.

18. Zeige: Für Boolesche Terme p und q ist $p \hookrightarrow q$ gleichbedeutend mit $p+q \equiv q$.

19. Man weise für beliebige Boolesche Terme p,q,r nach:
    a) Aus $p \hookrightarrow q$ folgt $p \hookrightarrow q+r$
    b) Aus $p \hookrightarrow q$ und $p \hookrightarrow r$ folgt $p \hookrightarrow q\cdot r$
    c) Aus $p \hookrightarrow q$ und $r \hookrightarrow q$ folgt $p+r \hookrightarrow q$.

20. Zeige: Die Relation "$\hookrightarrow$" auf $\mathcal{B}(X)$ ist reflexiv und transitiv.

21. Man beweise: Ist $p = p_1 + p_2 + \dots p_k$ ein SvP-Term und p_2 ein Teilterm von p_1, so folgt $p \equiv p_2 + \dots + p_k$.

Die Verschmelzungsmethode

Seien $p,q \in \mathcal{B}(X)$ Produkte (von Variablen und komplementierten Variablen). Da wir uns in diesem Zusammenhang für Terme nur "bis auf Äquivalenz" interessieren, wollen wir voraussetzen, daß p (und q) keine Variablen mehrfach enthalten. Außerdem denken wir uns die Faktoren von p und von q in ihrer natürlichen Reihenfolge aufgeschrieben.

Gibt es *genau eine* Variable x_i, die in p als Faktor vorkommt und deren Komplement x_i' in q als Faktor vorkommt (oder umgekehrt), so bezeichnen wir den Term $\tilde{p}\cdot\tilde{q}$, wobei $\tilde{p}$ durch Weglassen von x_i (bzw. x_i') und $\tilde{q}$ durch Weglassen von x_i' (bzw. x_i) aus p und q hervorgehen, als die <u>Verschmelzung von p und q</u>. (Die Verschmelzung von x_i und x_i' sei 1).

5.12 <u>Beispiel:</u> Die Verschmelzung von $x_1x_2x_3$ und $x_2x_3'x_4$ ist $x_1x_2x_4$. Die Verschmelzung von $x_1x_2'x_3'x_5$ und $x_1x_2'x_3x_4$ ist $x_1x_2'x_4x_5$. $x_1x_2'x_3$ und $x_1'x_2x_3$ haben keine Verschmelzung. (Man beachte, daß auch $\tilde{p}\cdot\tilde{q}$ auf eine Form gebracht wird, in der jede Variable höchstens einmal vorkommt.)

5.13 Lemma: Seien p und q Produktterme und sei r die Verschmelzung von p und q. Dann gilt: $p+q \equiv p + q + r$.

Beweis: $p+q \Rightarrow p+q+r$ ist klar (siehe auch Übungsaufgabe 18). Wir müssen im Hinblick auf Korollar 5.7 noch zeigen: $p+q+r \Rightarrow p+q$.
Sei x_i die Variable, die in p unkomplementiert und in q komplementiert vorkommt. Seien $\tilde{p}$ und $\tilde{q}$ wie in der Definition der Verschmelzung durch Weglassen von x_i bzw. x_i' gebildet. Man hat also $r = \tilde{p}\cdot\tilde{q}$. Sei $(\alpha_1,\ldots,\alpha_n) \in T((p+q+r)^1)$. Wir dürfen sogar annehmen $(\alpha_1,\ldots,\alpha_n) \in T(r^1)$, da andernfalls $(\alpha_1,\ldots,\alpha_n)$ schon aus $T((p+q)^1)$ ist. Ist also $(\alpha_1,\ldots,\alpha_n) \in T(r^1) = T((\tilde{p}\cdot\tilde{q})^1) = T(\tilde{p}^1) \cap T(\tilde{q}^1)$ und o.B.d.A. $\alpha_i = 1$, so gilt:
$(\alpha_1,\ldots,\alpha_n) \in T(\tilde{p}^1) \cap T(x_i^1) = T(p^1) \subseteq T((p+q)^1)$

Um alle Primimplikanten einer SvP zu finden, betrachten wir folgende zwei Operationen:

I. Eliminiere jeden Summanden, der einen anderen Summanden (der vorgelegten SvP) als Teilterm enthält.

II. Addiere die Verschmelzung zweier Summanden, falls diese noch nicht als Summand vorkommt und auch keinen Summanden als Teilterm enthält.

5.14 Satz: Wendet man auf eine SvP die Operationen I und II wiederholt in beliebiger Reihenfolge an, so gelangt man nach endlich vielen Schritten zu einer äquivalenten SvP, auf die keine dieser Operationen mehr anwendbar ist. Diese ist dann die Summe aller Primimplikanten.

Bevor wir zum Beweis dieses Satzes kommen, wollen wir die Methode an einem Beispiel demonstrieren.

5.15 Beispiel: Gegeben sei die SvP

$$p = x_1x_2x_3' + x_1x_2'x_3x_4' + x_1x_2' + x_1'x_2x_3' + x_1'x_2'x_3'x_4 .$$

Man erhält

$$\begin{aligned}
p &\equiv x_1x_2x_3' + x_1x_2' + x_1'x_2x_3' + x_1'x_2'x_3'x_4 && \text{(Operation I)}\\
&\equiv x_1x_2x_3' + x_1x_2' + x_1x_3' + x_1'x_2x_3' + x_1'x_2'x_3'x_4 && \text{(Operation II)}\\
&\equiv x_1x_2' + x_1x_3' + x_1'x_2x_3' + x_1'x_2'x_3'x_4 && \text{(Operation I)}\\
&\equiv x_1x_2' + x_1x_3' + x_1'x_2x_3' + x_2x_3' + x_1'x_2'x_3'x_4 && \text{(Operation II)}
\end{aligned}$$

$$\equiv x_1x_2' + x_1x_3' + x_2x_3' + x_1'x_2'x_3'x_4 \qquad \text{(Operation I)}$$
$$\equiv x_1x_2' + x_1x_3' + x_2x_3' + x_1'x_2'x_3'x_4 + x_1'x_3'x_4 \qquad \text{(Operation II)}$$
$$\equiv x_1x_2' + x_1x_3' + x_2x_3' + x_1'x_3'x_4 \qquad \text{(Operation I)}$$
$$\equiv x_1x_2' + x_1x_3' + x_2x_3' + x_1'x_3'x_4 + x_3'x_4 \qquad \text{(Operation II)}$$
$$\equiv x_1x_2' + x_1x_3' + x_2x_3' + x_3'x_4.$$

Auf die letzte SvP ist keine der Operationen I und II mehr anwendbar. Sie ist also die Summe aller Primimplikanten von p.

Wir kommen nun zum Beweis von Satz 5.14:

Zunächst überzeugen wir uns davon, daß die Operationen I und II eine SvP in eine dazu äquivalente SvP überführen. Für die Operation I folgt dies aus dem Absorptionsgesetz (4), für die Operation II aus Lemma 5.13. Dann überlegen wir uns, daß wir nach endlich vielen Schritten auf eine SvP kommen, auf die die Operationen I und II nicht mehr anwendbar sind, daß der Prozeß also stoppt. Da es (für eine vorgegebene Anzahl von verschiedenen Variablen) nur endlich viele SvP gibt, müssen wir nur zeigen, daß wir uns nicht "im Kreis drehen" können.
Sobald wir nämlich einen Produktterm q mit Hilfe von I gestrichen haben, kann dieser mittels II nicht mehr erzeugt werden: in allen folgenden Schritten wird immer ein Summand $\bar{q}$ existieren, der in q als Teilterm enthalten ist. Gibt es also einen "Kreis", so muß dieser allein durch Anwendung von II entstehen. II erhöht aber nur die Anzahl der Summanden, und folglich ist ein solcher "Kreis" unmöglich.
Schließlich zeigen wir, daß wir zum Schluß, wenn also weder I noch II anwendbar ist, eine SvP vorliegen haben, die die Summe aller Primimplikanten unseres Ausgangsterms p ist. Nehmen wir an, p_o sei ein Primimplikant unserer SvP $\bar{p}$, auf die weder Operation I noch Operation II anwendbar ist, und p_o sei nicht als Summand in $\bar{p}$ vertreten. Wir wollen daraus einen Widerspruch herleiten. Da p_o Primimplikant von $\bar{p}$ ist, enthält p_o sicher keinen Summanden von $\bar{p}$ als Teilterm, da für jeden Summanden p_i von $\bar{p}$ gilt $p_i \Rightarrow \bar{p}$. Durch Heranmultiplizieren von Variablen bzw. komplementierten Variablen erweitern wir p_o zu einem Produktterm $\bar{p}_o$, der maximale Länge hat bezüglich der Eigenschaft, keinen Summanden von $\bar{p}$ als Teilterm zu enthalten. Aus dieser Eigenschaft ergibt sich sofort, daß $\bar{p}_o$ nicht alle Variablen $x_1,\dots,x_n$ enthalten kann, denn $\bar{p}_o \Rightarrow \bar{p}$ gilt ja immer noch. Die Variable x_i komme also *nicht* in

$\overline{p}_o$ vor. Wir betrachten nun die Produktterme $\overline{p}_o x_i$ und $\overline{p}_o x_i'$. Beide müssen nach Definition von $\overline{p}_o$ je einen Summanden von $\overline{p}$ enthalten. Seien q_1 und q_2 diese Summanden. q_1 ist also von der Form $r_1 \cdot x_i$ und q_2 von der Form $r_2 \cdot x_i'$, wobei r_1 und r_2 in $\overline{q}_o$ enthalten sind. Es existiert also die Verschmelzung von q_1 und q_2. Da diese in $\overline{p}_o$ enthalten ist, enthält sie demnach keinen Summanden von $\overline{p}$. Mithin ist Operation II auf $\overline{p}$ anwendbar, was unserer Annahme widerspricht.

Wir wissen nun, daß jeder Primimplikant von p als Summand in $\overline{p}$ auftaucht. Nun zeigen wir, daß auch tatsächlich jeder Summand von $\overline{p}$ ein Primimplikant ist.
Der Summand r von $\overline{p}$ sei kein Primimplikant. Wegen $r \Rightarrow p$ muß es also einen in r enthaltenen Teilterm r_o geben, der Primimplikant von p ist. Da nach dem soeben Gezeigten r_o ein Summand von $\overline{p}$ ist, ist Operation I auf $\overline{p}$ anwendbar, entgegen unserer Voraussetzung.

Wir haben nun eine Methode gefunden, alle Primimplikanten einer SvP $p = p_1 + \ldots + p_n$ zu finden. Seien $q_1,\ldots,q_k$ alle Primimplikanten von p. Dann ist nach Satz 5.10 jede minimale, zu p äquivalente SvP die Summe einiger dieser Primimplikanten. Mithin ist insbesondere $p \equiv q_1 + \ldots + q_k$ (vgl. Übungsaufgabe 19). Das bedeutet, daß wir zunächst p als Summe aller Primimplikanten von p darstellen und dann "überflüssige" Primimplikanten wieder streichen können. Welche Summanden einer SvP sind aber überflüssig?

5.16 <u>Definition:</u> Sei p ein Produktterm und q eine SvP; p heißt <u>überflüssig in $p+q$</u>, wenn $p+q \equiv q$ (d.h. wenn $p \Rightarrow q$) gilt.

5.13 <u>Beispiel:</u> x_2x_4 ist überflüssig in $p = x_2'x_3 + x_2x_3' + x_2x_4 + x_3x_4 + x_1x_4$. Zu zeigen ist also, daß für beliebige $(\alpha_1,\ldots,\alpha_4) \in 2^4$ aus $\alpha_2 \cdot \alpha_4 = 1$, also aus $\alpha_2 = \alpha_4 = 1$ stets schon $\alpha_2'\alpha_3 + \alpha_2\alpha_3' + \alpha_3\alpha_4 + \alpha_1\alpha_4 = 1$ folgt. Aus $\alpha_2 = \alpha_4 = 1$ ergibt sich dieser Ausdruck tatsächlich zu $0 + \alpha_3' + \alpha_3 + \alpha_1 = 1$. Ebenso zeigt man, daß x_3x_4 überflüssig in p ist. Streicht man jedoch x_2x_4 in p, so gelangt man zu dem Term $\overline{p} = x_2'x_3 + x_2x_3' + x_3x_4 + x_1x_4$, der äquivalent zu p ist, in dem x_3x_4 aber nicht mehr überflüssig ist! Entsprechend ist die Situation, wenn man x_3x_4 in p streicht. Da es sonst keine überflüssigen Summanden in p gibt, und da p Summe aller Primimplikanten von p ist, gibt es genau zwei minimale SvP, die äquivalent zu p sind, nämlich $x_2'x_3 + x_2x_3' + x_3x_4 + x_1x_4$ und

$x_2'x_3 + x_2x_3' + x_2x_4 + x_1x_4$.

Nachdem man also den Ausgangsterm p als Summe der Primimplikanten dargestellt hat, bestimmt man zunächst alle überflüssigen Summanden in der Darstellung von p, streicht einen davon und verfährt auf dieselbe Weise mit dem so entstandenen einfacheren Term. Man gelangt so schließlich zu einem Term, der keine überflüssigen Summanden mehr besitzt. Einen solchen Term nennen wir irredundant. Indem man diesen Prozeß auf alle möglichen Weisen durchführt, findet man alle irredundanten Darstellungen von p. Unter diesen wähle man sich eine minimale Darstellung aus, und man hat so einen minimalen, zu p äquivalenten Term gefunden.

Dies wird durch eine Tabelle erleichtert. Sei z.B.

$$p = x_1x_3' + x_1x_2 + x_1'x_3 + x_2x_3 + x_2'x_3'x_4' + x_1'x_2'x_4'.$$

p ist schon als Summe aller seiner Primimplikanten geschrieben. (Man prüfe zur *Übung* nach, daß I und II nicht anwendbar sind.) Wir stellen eine Tabelle auf, deren Zeilen und Spalten den Primimplikanten von p entsprechen:

	x_1x_3'	x_1x_2	$x_1'x_3$	x_2x_3	$x_2'x_3'x_4'$	$x_1'x_2'x_4'$
x_1x_3'	-	x_2	0	0	$x_2'x_4'$	0
x_1x_2	x_3'	-	0	x_3	0	0
$x_1'x_3$	0	0	-	x_2	0	$x_2'x_4'$
x_2x_3	0	x_1	x_1'	-	0	0
$x_2'x_3'x_4'$	x_1	0	0	0	-	x_1'
$x_1'x_2'x_4'$	0	0	x_3	0	x_3'	-

Die Tabelle entsteht so: In die Diagonale trägt man nichts ein. Um den Eintrag an der Stelle (i,j) zu finden, setzt man die Faktoren in dem i-ten Primimplikanten $=1$ und setzt diese Werte in den j-ten Primimplikanten ein (soweit die Variablen von p_i auch in p_j vorkommen); das so erhaltene Ergebnis ergibt den Eintrag an der Stelle (i,j). In dem Beispiel setzt man in der ersten Zeile $x_1 = 1$, $x_3' = 1$, also $x_1 = 1$,

$x_3 = 0$. Aus x_1x_2 wird dann $1 \cdot x_2 \equiv x_2$, aus $x_1'x_3$ wird $1' \cdot 0 \equiv 0$, aus x_2x_3 wird $x_2 \cdot 0 \equiv 0$ usw.

Sei nun s_i die Summe der Terme der i-ten Zeile unserer Tabelle. Falls $s_i \equiv 1$ ist, dann ist der i-te Primimplikant p_i überflüssig. In der Tat bedeutet $s_i \equiv 1$ nämlich: Wenn p_i den Wert 1 hat, dann hat auch die Summe der anderen Primimplikanten den Wert 1, d.h.

$$p_i \Rightarrow p_1 + \dots + p_{i-1} + p_{i+1} + \dots + p_n$$

und folglich

$$p = p_1 + \dots + p_n \equiv p_1 + \dots + p_{i-1} + p_{i+1} + \dots + p_n.$$

In unserem Beispiel sind x_1x_2, x_2x_3, $x_2'x_3'x_4'$ und $x_1'x_2'x_4'$ überflüssig. Man kann nun *einen* dieser überflüssigen Primimplikanten streichen. Für die restlichen Primimplikanten macht man wieder eine solche Tabelle; diese erhält man einfach durch Streichen der Zeile und Spalte der vorhergehenden Tabelle, die dem gestrichenen Primimplikanten entsprechen. In der neuen Tabelle bestimmen wir wieder die überflüssigen Primimplikanten usw., bis kein Primimplikant mehr überflüssig ist. Die übriggebliebenen Primimplikanten ergeben eine irredundante Darstellung für p.
In unserem Beispiel erhält man vier irredundante Darstellungen. (Man vollziehe dies zur Übung nach):

$$\begin{aligned} p &\equiv x_1x_3' + x_1'x_3 + x_2x_3 + x_2'x_3'x_4' \\ &\equiv x_1x_3' + x_1'x_3 + x_2x_3 + x_1'x_2'x_4' \\ &\equiv x_1x_3' + x_1'x_3 + x_1x_2 + x_2'x_3'x_4' \\ &\equiv x_1x_3' + x_1'x_3 + x_1x_2 + x_1'x_2'x_4' \end{aligned}$$

Diese sind alle minimal ($s(p) = 4$, $v(p) = 9$).

<u>Zusammenfassung:</u> Um die minimalen, zu einem vorgegebenen Term p äquivalenten SvP zu bekommen, geht man so vor:

1. Bestimmung einer zu p äquivalenten SvP (Ausmultiplizieren unter Verwendung der Distributivgesetze);
2. Bestimmung aller Primimplikanten (Verschmelzungsmethode);
3. Bestimmung aller irredundanten Darstellungen durch sukzessives Streichen überflüssiger Primimplikanten;
4. Aufsuchen der minimalen unter den irredundanten Darstellungen.

Ist eine Boolesche Funktion $f: \mathbf{2}^n \to \mathbf{2}$ gegeben und eine Darstellung durch eine minimale SvP gesucht, so stellt man zunächst die disjunktive Normalform für f auf und wendet auf diese obiges Verfahren an.

Es soll noch auf die häufig benutzte <u>Karnaugh-Methode</u> zur Ermittlung minimaler SvP hingewiesen werden. Es handelt sich um eine graphische Methode, die allerdings nur auf Boolesche Ausdrücke mit höchstens sechs Variablen anwendbar ist.
Wir wollen die Methode nur an einem Beispiel (mit 4 Variablen) illustrieren - ansonsten sei auf die Literatur verwiesen.
Wir betrachten die DNF

$$\underline{x_1'\cdot x_2\cdot x_3'\cdot x_4' + x_1'\cdot x_2\cdot x_3'\cdot x_4 + x_1\cdot x_2'\cdot x_3'\cdot x_4 + x_1\cdot x_2'\cdot x_3\cdot x_4 + x_1\cdot x_2\cdot x_3'\cdot x_4}$$
$$\underline{+ x_1\cdot x_2\cdot x_3\cdot x_4' + x_1\cdot x_2\cdot x_3\cdot x_4}\ .$$

	$x_1\cdot x_2$	$x_1\cdot x_2'$	$x_1'\cdot x_2'$	$x_1'\cdot x_2$
$x_3\cdot x_4$	X	X		
$x_3\cdot x_4'$	X			
$x_3'\cdot x_4'$				X
$x_3'\cdot x_4$	X	X		X

In der nebenstehenden Tafel werden diejenigen der 16 Kästchen angekreuzt, die zu einem in der vorgelegten DNF auftretenden Produktterm korrespondieren. Dabei ist die Tabelle so angelegt, daß nebeneinanderliegende Kästchen solchen Produkttermen entsprechen, die sich bezüglich genau eines Buchstaben unterscheiden - man beachte, daß demnach auch $x_1\cdot x_2\cdot x_3\cdot x_4$ und $x_1\cdot x_2\cdot x_3'\cdot x_4$ "nebeneinander liegen"! (Man denke sich die gegenüberliegenden Ränder der Tafel jeweils zusammengeklebt, es entsteht ein <u>Torus</u>.) Man ersetzt nun Gruppen nebeneinanderliegender Produktterme durch kürzere Produktterme; dabei muß jedes angekreuzte Kästchen erfaßt werden.

	$x_1\cdot x_2$	$x_1\cdot x_2'$	$x_1'\cdot x_2'$	$x_1'\cdot x_2$
$x_3\cdot x_4$	X	X		
$x_3\cdot x_4'$	X			
$x_3'\cdot x_4'$				X
$x_3'\cdot x_4$	X	X		X

Dieses "Quadrat" wird ersetzt durch $x_1\cdot x_4$

Wird ersetzt durch $x_1\cdot x_2\cdot x_3$

Wird ersetzt durch $x_1'\cdot x_2\cdot x_3'$

Zunächst sucht man nach Gruppen von acht Produkttermen, die zwei "nebeneinanderliegende" Zeilen bzw. Spalten besetzen. Diese entsprechen einem Summanden x_i oder x_i' in einer minimalen SvP. Danach fahndet man nach "Quadraten", also Gruppen von vier nebeneinanderliegenden Produkttermen, diese entsprechen dann einem Summanden mit zwei Variablen in der minimalen SvP. Als nächstes faßt man Gruppen von zwei nebeneinanderliegenden Produkttermen zusammen (ihre Verschmelzung wird ein Summand in der minimalen SvP) und addiert zum Schluß die noch übrig gebliebenen "isolierten" Produktterme.

So gelangt man in unserem Beispiel zu der minimalen SvP
$x_1x_4 + x_1x_2x_3 + x_1'x_2x_3'$.
Eine mathematische Begründung der Karnaugh-Methode kann man ohne große Schwierigkeiten finden.

Übungsaufgaben:

22. Man bestimme alle Primimplikanten von

    a) $x_1'x_2x_3x_4' + x_1x_2x_3 + x_1'x_3'x_4 + x_1'x_3x_4$

    b) $x_1x_2x_3x_4 + x_1x_2x_3'x_4x_5 + x_1x_2'x_3x_4x_5 + x_1x_2'x_3x_4'x_5 + x_1x_3'x_4'x_5 + x_1'x_2'x_3x_4x_5 + x_1'x_2x_3'x_4x_5' + x_1x_2'x_3'x_4'$.

23. Finde minimale, zu den Termen in der vorigen Aufgabe äquivalente Summen von Produkttermen.

24. Eine Abstimmungsschaltung wie in Übungsaufgabe 14 soll für ein Gremium von vier Personen entworfen werden. Bei Stimmengleichheit soll eine der vier Personen, der Präsident etwa, den Ausschlag geben. Finde eine minimale Schaltung.

§ 6. ANWENDUNGEN IN DER LOGIK

Wir wollen unter einer Aussage einen in der Umgangssprache formulierten Satz verstehen, dem in sinnvoller Weise (zu jedem Zeitpunkt) genau eine der beiden Eigenschaften "wahr" bzw. "falsch" zugeordnet werden kann (vgl. § 1). Beispielsweise sind "Heute schneit es", "Der Ball ist rund", "Wenn der Hahn kräht auf dem Mist, dann ändert sich das Wetter, oder es bleibt wie es ist" solche Aussagen. In dem letztgenannten Beispiel wurde eine Aussage aus mehreren elementaren Aussagen zusammengesetzt. Nach einer sinngemäßen Umformung erkennt man, daß der obigen Aussage zwei elementare Aussagen, nämlich "Der Hahn kräht auf dem Mist" und "Das Wetter ändert sich" zugrundeliegen. Steht A für die Aussage "Der Hahn kräht auf dem Mist" und B für "Das Wetter ändert sich", so können wir abkürzend schreiben:

"Wenn A dann (B oder nicht B)".

Durch Verknüpfung von Aussagen durch "oder", "und", "wenn ... dann ..." und "nicht" kann man also von gegebenen Aussagen zu komplizierteren Aussagen gelangen.

Um zu einer mathematischen Behandlung dieser Situation überzugehen, verabredet man zunächst, daß man einer Aussage den Wahrheitswert 1 zuordnet, falls sie richtig ist, und den Wahrheitswert 0, falls sie falsch ist. Repräsentieren die Buchstaben A und B Aussagen, so setzt man für die neuen Aussagen $A \vee B$ (A oder B), $A \wedge B$ (A und B) bzw. $\neg A$ (nicht A) die folgenden Wahrheitswerte in Abhängigkeit der Wahrheitswerte von A und B fest:

A	B	$A \vee B$	$A \wedge B$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

A	$\neg A$
0	1
1	0

Es fällt nun auf, daß diese Tabellen gerade die Operationen $+, \cdot, '$ der zweielementigen Booleschen Algebra $\mathbf{2}$ beschreiben.

In der Logik ist es üblich, auch die Aussage $A \Rightarrow B$ (wenn A dann B) zu betrachten, deren Wahrheitswerte durch die folgende Tabelle festgelegt sind:

A	B	A => B
0	0	1
0	1	1
1	0	0
1	1	1

Wir erkennen sofort, daß wir $A \Rightarrow B$ auch durch $\neg A \vee B$ ausdrücken können und wollen deshalb $A \Rightarrow B$ nur als Abkürzung für $\neg A \vee B$ verstehen.

Sei nun p ein Boolescher Term. Wir verwenden vorübergehend die Zeichen $\vee, \wedge$ und $\neg$ anstelle von $+, \cdot$ und $'$. Man nennt p dann auch eine Aussageform.

Ist p also eine Aussageform, die die Variablen $x_1, x_2, \ldots, x_n$ enthält, so erhält man eine Aussage, indem man die Variablen $x_1, x_2, \ldots, x_n$ durch Aussagen $A_1, A_2, \ldots, A_n$ ersetzt. Ist dann α_i der Wahrheitswert von A_i für $i = 1, \ldots, n$, dann hat die so entstandene neue Aussage $p(A_1, A_2, \ldots, A_n)$ den Wahrheitswert $p^{2}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

6.1 Beispiel: Die zusammengesetzte Aussage laute: "Heute ist Sonntag, aber es stimmt nicht, daß die Sonne scheint und das Schwimmbad geöffnet ist."

Mit der Entsprechung

$$\begin{aligned} \text{Heute ist Sonntag} &\leftrightarrow x_1 \\ \text{Die Sonne scheint} &\leftrightarrow x_2 \\ \text{Das Schwimmbad ist geöffnet} &\leftrightarrow x_3 \end{aligned}$$

hat die Aussage die Aussageform $x_1 \wedge \neg(x_2 \wedge x_3)$.

Ist nun heute ein sonniger Sonntag mit geschlossenem Schwimmbad, so haben wir $(\alpha_1, \alpha_2, \alpha_3) = (1,1,0)$, und der Wahrheitswert unserer Aussage ist $1 \cdot (1 \cdot 0)' = 1$ – die Aussage stimmt.

Sind p und q Aussageformen, so sagen wir wie bisher: p und q sind äquivalent, falls $p \equiv q$ gilt, vgl. Definition 4.3.

6.2 Beispiel: Die Aussageformen $x \Rightarrow (y \Rightarrow z)$ und $y \Rightarrow (x \Rightarrow z)$ sind äquivalent, denn nach der Definition gilt:

$$\begin{aligned} x \Rightarrow (y \Rightarrow z) &:= \neg x \vee (\neg y \vee z) \quad \text{und} \\ y \Rightarrow (x \Rightarrow z) &:= \neg y \vee (\neg x \vee z). \end{aligned}$$

(Man setze zur Veranschaulichung für x,y,z Aussagen ein, beispielsweise "Es regnet", "Ich habe einen Schirm", "Ich bleibe trocken".)

6.3 Definition: Eine Aussageform p heißt eine Tautologie, falls $p \equiv 1$ ist, falls p also immer wahr ist, gleichgültig was wir für die Variablen von p einsetzen.

Beispielsweise sind $x \vee \neg x$, $(x \wedge y) \Rightarrow x$, $x \Rightarrow (y \Rightarrow x)$ solche Tautologien.

6.4 Definition: Eine Aussageform p heißt widersprüchlich, falls $p \equiv 0$ ist. Eine endliche Menge $\{p_1, p_2, \ldots, p_n\}$ von Aussageformen heißt konsistent, falls die Aussageform $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ *nicht* widersprüchlich ist.

6.5 Beispiele: $x \wedge \neg x$ ist widersprüchlich, $\{x \vee y,\ x \Rightarrow y,\ x \Rightarrow \neg y\}$ ist konsistent, dagegen ist $\{x,\ x \Rightarrow y,\ x \Rightarrow \neg y\}$ nicht konsistent, denn

$$x \wedge (x \Rightarrow y) \wedge (x \Rightarrow \neg y) \equiv x \wedge (\neg x \vee y) \wedge (\neg x \vee \neg y) \equiv$$
$$\equiv x \wedge (\neg x \vee (y \wedge \neg y)) \equiv x \wedge (\neg x \vee 0) \equiv x \wedge \neg x \equiv 0.$$

Anhand der bisherigen Überlegungen in diesem Abschnitt ist klargeworden, daß die im 3. und 4. Abschnitt erhaltenen Ergebnisse über Boolesche Ausdrücke und die von ihnen induzierten Funktionen ausreichen, um die gewöhnlich auftretenden aussagenlogischen Probleme zu lösen. Wir wollen diesen Abschnitt mit drei Beispielen abschließen, die einige für die Aussagenlogik typische Fragestellungen deutlich machen.

6.6 Beispiel: Arnold möchte mit Udo, Volker und Willi zum Rockfestival gehen. Die drei wollen sich jedoch einen Spaß machen und konfrontieren ihn damit: Udo will nicht kommen, wenn Volker nicht kommt. Volker und Willi kommen beide oder kommen beide nicht. Außerdem verspricht Willi zu kommen, falls Udo und Volker beide nicht kommen. Mit wem kann Arnold rechnen?

Ordnen wir den Aussagen "Udo kommt", "Volker kommt", "Willi kommt" die Variablen u,v,w zu, so erhalten wir die Aussageform

$$(\neg v \Rightarrow \neg u) \wedge ((v \wedge w) \vee (\neg v \wedge \neg w)) \wedge ((\neg u \wedge \neg v) \Rightarrow w).$$

Kürzen wir diese Aussageform mit p ab, so fragen wir also: bei welcher Wahrheitswerteverteilung $(\alpha_1, \alpha_2, \alpha_3)$ auf (u,v,w) wird $p^{\mathbf{2}}(\alpha_1, \alpha_2, \alpha_3) = 1$, d.h. wir fragen nach $T(p^{\mathbf{2}})$.

Man kann nun mit Hilfe einer Tabelle den Träger berechnen (und erhält $T(p^{2}) = \{(0,1,1), (1,1,1)\}$) oder aber p direkt in eine leichter zu interpretierende Form bringen:

$$\begin{aligned} p &\equiv (v \vee \neg u) \wedge (v \vee \neg w) \wedge (\neg v \vee w) \wedge (u \vee v \vee w) \\ &\equiv v \wedge w. \end{aligned}$$

Man liest jedenfalls ab, daß Volker und Willi kommen - bei Udo bleibt es ungewiß.

Im nächsten Beispiel soll eine Fülle von Einzelaussagen (etwa eines Politikers) zu einer verständlichen Gesamtaussage zusammengefaßt werden.

6.7 Beispiel: "Entweder wird die Mark abgewertet, oder, falls der Export nicht zurückgeht, müssen die Preise eingefroren werden. Wird die Mark nicht abgewertet, so geht der Export zurück, und die Preise werden nicht eingefroren. Werden die Preise eingefroren, dann wird der Export nicht zurückgehen, und die Mark darf nicht abgewertet werden."
Was heißt das?

Wir setzen x für "Die Mark wird abgewertet", y für "Der Export geht zurück" und z für "Die Preise werden eingefroren". Dann lassen sich die obigen Aussagen schreiben:

$$p_1 := x \vee (\neg y \Rightarrow z), \quad p_2 := \neg x \Rightarrow (y \wedge \neg z) \quad \text{und}$$
$$p_3 := z \Rightarrow (\neg y \wedge \neg x).$$

Wir erhalten $p_1 \equiv x \vee y \vee z$, $p_2 \equiv x \vee (y \wedge \neg z)$ und $p_3 \equiv \neg z \vee (\neg y \wedge \neg x)$, also

$$\begin{aligned} p_1 \wedge p_2 \wedge p_3 &\equiv (x \vee y \vee z) \wedge (x \vee (y \wedge \neg z)) \wedge (\neg z \vee (\neg y \wedge \neg x)) \\ &\equiv (x \vee (y \wedge \neg z)) \wedge (\neg z \vee (\neg y \wedge \neg x)) \equiv (x \wedge \neg z) \vee (y \wedge \neg z) \\ &\equiv \neg z \wedge (x \vee y) \equiv \underline{\neg z \wedge (\neg x \Rightarrow y)}. \end{aligned}$$

Das Gesagte ist also gleichbedeutend mit der Aussage "Die Preise werden nicht eingefroren, und wenn die Mark nicht abgewertet wird, dann geht der Export zurück".

Im letzten Beispiel wird nachgeprüft, ob man aus gewissen gegebenen Aussagen eine andere "logisch schließen" kann:

6.8 Beispiel: "Ist f stetig, dann ist g oder h differenzierbar. Ist g nicht differenzierbar, dann ist f nicht stetig, aber beschränkt.

Eine hinreichende Bedingung für die Differenzierbarkeit von g oder von h ist die Beschränktheit von f."

Kann man aus diesen Aussagen schließen, daß g differenzierbar ist?

Wir setzen

x_1 für "f ist stetig", x_2 für "g ist differenzierbar", x_3 für "h ist differenzierbar" und x_4 für "f ist beschränkt".

Ferner wird abgekürzt

$p_1 := x_1 \Rightarrow (x_2 \vee x_3)$, $p_2 := \neg x_2 \Rightarrow (\neg x_1 \wedge x_4)$, $p_3 := x_4 \Rightarrow (x_2 \vee x_3)$.

Die Frage ist nun, ob die Aussageform

$$p_1 \wedge p_2 \wedge p_3 \Rightarrow x_2$$

eine Tautologie ist. Zunächst erhalten wir

$$\begin{aligned} p_1 \wedge p_2 \wedge p_3 &\equiv (\neg x_1 \vee x_2 \vee x_3) \wedge (x_2 \vee (\neg x_1 \wedge x_4)) \wedge (\neg x_4 \vee x_2 \vee x_3) \\ &\equiv (x_2 \vee (\neg x_1 \wedge x_4)) \wedge (x_2 \vee x_3 \vee \neg x_4) \\ &\equiv x_2 \vee (\neg x_1 \wedge x_3 \wedge x_4). \end{aligned}$$

Damit folgt

$$p_1 \wedge p_2 \wedge p_3 \Rightarrow x_2 \equiv x_2 \vee (\neg x_1 \wedge x_3 \wedge x_4) \Rightarrow x_2 \equiv \neg x_1 \wedge x_3 \wedge x_4 \Rightarrow x_2,$$

die Aussageform ist also *keine* Tautologie: es entsteht eine falsche Aussage, wenn für x_1 und x_2 falsche und für x_3 und x_4 wahre Aussagen eingesetzt werden. Für die Ausgangsfrage heißt das: ist f unstetig und beschränkt und h differenzierbar, so braucht g nicht differenzierbar zu sein.

Übungsaufgaben:

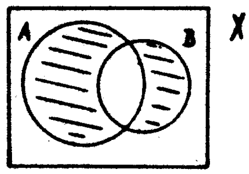
25. Zeige, daß $(\neg x \Rightarrow \neg y) \Rightarrow (y \Rightarrow x)$ eine Tautologie ist.

26. Sind die folgenden Mengen von Aussageformen widersprüchlich oder konsistent?
 a) $M_1 = \{(x \Rightarrow y) \Rightarrow z,\ \ (\neg x \vee y) \Rightarrow (z \wedge y),\ \ z \Rightarrow (\neg x \Rightarrow y)\}$
 b) $M_1 \cup \{\neg(y \Rightarrow z)\}$
 c) $M_1 \cup \{y \Rightarrow z\}$.

27. Aus einem (fiktiven) Chemie-"Kochbuch":
 "Fällt ein weißer Niederschlag aus, dann enthält die Probe entweder Natrium oder Ammoniak. Ist kein Natrium in der Probe, dann enthält sie Eisen. Ist Eisen vorhanden, und fällt ein weißer Niederschlag, dann kann kein Ammoniak in der Probe sein."
 Was ist also sicher vorhanden, falls ein weißer Niederschlag fällt?

§ 7. BOOLESCHE RINGE

Aus der Mengenlehre kennt man die symmetrische Differenz $A \Delta B$ zweier Mengen $A,B \subseteq X$:



$$A \Delta B := (A \setminus B) \cup (B \setminus A)$$
$$= (A \cap \overline{B}) \cup (\overline{A} \cap B).$$

Diese Operation Δ kann in beliebigen Booleschen Algebren betrachtet werden:

7.1 Definition: Sei $(B; +, \cdot, ', 0, 1)$ eine Boolesche Algebra, $a,b \in B$; das Element $a \Delta b := a \cdot b' + a' \cdot b \in B$ heißt die symmetrische Differenz von a und b.

Man rechnet leicht nach, daß $a \Delta b = (a+b) \cdot (a \cdot b)'$ gilt; für Mengen bedeutet dies $A \Delta B = (A \cup B) \cap (\overline{A \cap B}) = (A \cup B) \setminus (A \cap B)$, d.h. die symmetrische Differenz ist "Vereinigung minus Durchschnitt". Die entsprechende Verknüpfung in der Aussagenlogik ist das "ausschließende Oder", welches man umgangssprachlich meist durch die Formulierung "entweder - oder" ausdrückt.

7.2 Lemma: Die Operation $\Delta: B^2 \to B$ hat folgende Eigenschaften:

(a) $x \Delta y = y \Delta x$ (b) $x \Delta 0 = x$

(c) $x \Delta x = 0$ (d) $x \Delta (y \Delta z) = (x \Delta y) \Delta z$

(e) $x \cdot (y \Delta z) = (x \cdot y) \Delta (x \cdot z)$ (f) $x \Delta x' = 1$

Zum Beweis soll nur angemerkt werden, daß (a) bis (c) und (f) sofort einzusehen sind; (d) und (e) können leicht nachgerechnet werden.

Die Eigenschaften (a)-(d) aus 7.2 besagen, daß B bezüglich der Operation Δ eine kommutative Gruppe mit neutralem Element 0 ist; nach (c) ist jedes Element zu sich selbst invers. Um eine noch stärkere Aussage zu formulieren, erinnern wir zunächst an den Ringbegriff:

7.3 Definition: Ein kommutativer Ring mit 1 ist eine Algebra $(R; +, -, 0, \cdot, 1)$ vom Typ $(2,1,0,2,0)$ mit der Eigenschaft, daß $(R; +, -, 0)$ eine abelsche Gruppe ist und außerdem die folgenden Gesetze gelten:

(R_1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(R_2) $a \cdot b = b \cdot a$

(R_3) $a \cdot (b+c) = a \cdot b + a \cdot c$

(R_4) $1 \cdot a = a$

Ist außerdem jedes Element von R idempotent, d.h. gilt das Gesetz

(R_5) $x\cdot x = x$,

so ist $(R; +, -, 0, \cdot, 1)$ ein <u>Boolescher Ring</u>.

Durch Ausnutzung der Idempotenz folgt leicht, daß wegen $(x+x)\cdot(x+x) = x+x$ in einem Booleschen Ring stets $x+x = 0$ gelten muß.
Aufgrund von 7.2 überzeugt man sich nun sofort von der Richtigkeit des folgenden Satzes:

7.4 <u>Satz:</u> Für eine beliebige Boolesche Algebra $(B; +, \cdot, ', 0, 1)$ ist $(B; \Delta, id_B, 0, \cdot, 1)$ ein Boolescher Ring.

Es stellt sich nun die Frage, ob man die Boolesche Algebra auch umgekehrt aus dem Booleschen Ring $(B; \Delta, id_B, 0, \cdot, 1)$ "zurückgewinnen" kann. Daß dies in der Tat möglich ist, besagt:

7.5 <u>Lemma:</u> Sei $(B; +, \cdot, ', 0, 1)$ eine Boolesche Algebra, $(B; \Delta, id_B, 0, \cdot, 1)$ der zugehörige Boolesche Ring. Dann gilt

$$a+b = a \Delta b \Delta (a\cdot b) \quad \text{und} \quad x' = x\Delta 1.$$

<u>Beweis:</u> Man hat $a \Delta b \Delta (a\cdot b) = (a'b + ab') \Delta (ab)$

$$= (a'b + ab')'ab + (a'b + ab')(a' + b')$$
$$= (a+b')(a'+b)ab + a'b + ab'$$
$$= ab + a'b + ab'$$
$$= b + ab'$$
$$= a+b$$

und $x \Delta 1 = x'\cdot 1 + x\cdot 0 = x'$.

Es ist hilfreich, sich die Aussage von 7.5 an einem Mengendiagramm zu veranschaulichen.

Die in 7.5 gezeigten Beziehungen legen es nun nahe, umgekehrt auch zu jedem Booleschen Ring eine Boolesche Algebra zu betrachten:

7.6 <u>Satz:</u> Ist $(B; \Delta, -, 0, \cdot, 1)$ ein Boolescher Ring, und definiert man für $a,b \in B$ $a+b := a \Delta b \Delta (a\cdot b)$ und $a' := a \Delta 1$, so ist $(B; +, \cdot, ', 0, 1)$ eine Boolesche Algebra. Es gilt dann außerdem $x \Delta y = xy' + x'y$ für $x,y \in B$.

Beweis: Wir weisen die Gültigkeit des Distributivgesetzes $(x+y)(x+z) = x + yz$ nach und empfehlen das Nachrechnen der übrigen Axiome als Übung:

$$\begin{aligned}(x+y)(x+z) &= (x\Delta y\Delta xy)(x\Delta z\Delta xz) = x(x\Delta z\Delta xz)\ \Delta\ y(x\Delta z\Delta xz)\ \Delta\ xy(x\Delta z\Delta xz)\\ &= x\ \Delta\ xz\ \Delta\ xz\ \Delta\ xy\ \Delta\ yz\ \Delta\ xyz\ \Delta\ xy\ \Delta\ xyz\ \Delta\ xyz\\ &= x\ \Delta\ yz\ \Delta\ xyz\\ &= x + yz.\end{aligned}$$

Schließlich gilt:

$$\begin{aligned}xy' + x'y &= x(y\Delta 1)\ \Delta\ (x\Delta 1)y\ \Delta\ x(y\Delta 1)(x\Delta 1)y\\ &= xy\ \Delta\ x\ \Delta\ xy\ \Delta\ y\ \Delta\ xy\ \Delta\ xy\ \Delta\ xy\ \Delta\ xy\\ &= x\ \Delta\ y.\end{aligned}$$

Zusammenfassend haben wir damit gezeigt, daß die Gleichungen $x\Delta y = xy' + x'y$ einerseits und $x+y = x\Delta y\Delta xy$ bzw. $x' = x\Delta 1$ andererseits "zueinander inverse Vorschriften" beschreiben, aus einer Booleschen Algebra einen Booleschen Ring - und umgekehrt - zu machen. Dies bedeutet, daß man wahlweise eine der beiden Strukturen betrachten kann; man kann etwa Probleme über Boolesche Algebren in solche überführen, die Boolesche Ringe behandeln, und kann die Lösung dann in die Sprache der Booleschen Algebren rückübersetzen.

In § 4 hatten wir gesehen, daß jede Schaltfunktion $f: \{0,1\}^n \to \{0,1\}$ eine Boolesche Funktion ist, also aus den Projektionen $\pi_i = x_i$ $(i = 1,\dots,n)$ mit Hilfe der Operationen $+,\cdot,'$ "gebaut" werden kann. Die Ergebnisse des vorliegenden Abschnitts besagen, daß statt $+,\cdot,'$ auch die Operationen $\Delta,'$ verwendet werden können.
Wir wollen - dies nun eine informale Definition - eine Menge $\{f_1,\dots,f_k\}$ von Operationen auf der Menge $\{0,1\}$ eine adäquate Menge von Operationen nennen, falls man aus den $f_1,\dots,f_k$ und den Projektionen mit Hilfe von Ineinander-Einsetzen (Superposition) und Gleichsetzen von Variablen sämtliche Schaltfunktionen erhält.

7.7 Beispiel: $\{+,'\}$ ist eine adäquate Menge von Operationen, denn man kann $\cdot$ durch $x\cdot y = (x'+y')'$ erhalten und damit auch alle Schaltfunktionen.
Ebenso ist $\{\Rightarrow,'\}$ eine adäquate Menge von Operationen, wie man leicht nachweist; oft wird in der Logik von diesen Operationen ausgegangen.

Eine weitere wichtige zweistellige Operation ist der Sheffer-Strich $\uparrow$:

7.8 Satz: $x \uparrow y$ sei definiert als $x'+y'$. Dann ist $\{\uparrow\}$ eine adäquate Menge von Operationen.

Beweis: Dies folgt aus $x+y = (x\uparrow x) \uparrow (y\uparrow y)$ und $x' = x\uparrow x$.

Als Beispiel soll schließlich noch der Diskriminator d erwähnt werden, der folgendermaßen definiert ist:

$$d(x,y,z) := \begin{cases} z, & \text{falls } x = y \\ x, & \text{falls } x \neq y. \end{cases}$$

Auch $\{d,0,1\}$ ist eine adäquate Menge von Operationen.

Adäquate Mengen von Operationen können dazu dienen, logische Schaltungen anstelle mit Hilfe der "Schaltglieder" $+,\cdot,'$ mit anderen Schaltgliedern zu realisieren. Schaltglieder für den Sheffer-Strich bzw. den dualen Sheffer-Strich $(x\downarrow y := x'y')$ werden tatsächlich in der Technik häufig verwendet, wo sie unter den Namen "NAND" bzw. "NOR" bekannt sind.

Übungsaufgaben:

28. Zeige, daß $\{d,0,1\}$ eine adäquate Menge von Operationen ist. Gilt dies auch für $\{d,0\}$?

29. Zeige, daß jede Boolesche Algebra auch als Vektorraum über dem zweielementigen Körper GF(2) aufgefaßt werden kann. (Aus dieser Beobachtung ergibt sich ein kurzer Beweis dafür, daß die Ordnung jeder endlichen Booleschen Algebra eine Zweierpotenz ist.)

§ 8. BOOLESCHE VERBÄNDE

Bevor wir zum Verbandsbegriff kommen, soll kurz an einige Begriffe aus der Ordnungstheorie erinnert werden.

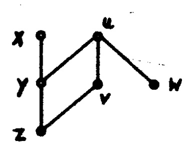
8.1 Definition: Eine Halbordnung ist ein Paar $(H,\leq)$, wobei H eine nicht-leere Menge ist und $\leq$ eine zweistellige Relation, die für alle $x,y,z \in H$ folgende Bedingungen erfüllt:

(H_1) $x \leq x$ (Reflexivität)

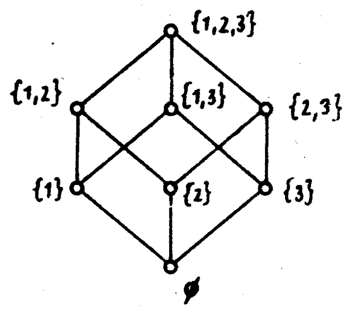
(H_2) Aus $x \leq y$ und $y \leq x$ folgt $x = y$ (Antisymmetrie).

(H_3) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$ (Transitivität).

Halbordnungen werden oft durch ihr Hasse-Diagramm beschrieben; z.B. beschreibt das Diagramm



die Halbordnung $H_6 = \{x,y,z,u,v,w\}$ mit $z \leq y \leq x$, $z \leq v \leq u$, $y \leq u$, $w \leq u$.
Man kann zu jeder endlichen Halbordnung (und auch zu einigen unendlichen) ein Hasse-Diagramm zeichnen; dabei läßt man Striche weg, die sich schon aus der Transitivität ergeben: im obigen Beispiel haben wir etwa z und u nicht durch einen Strich verbunden, obwohl $z \leq u$ gilt.
Um ein weiteres Beispiel zu geben, präsentieren wir hier ein Hasse-Diagramm der Halbordnung $(\mathbb{P}(\{1,2,3\}), \subseteq)$:



8.2 Definition: Sei $(H,\leq)$ eine Halbordnung, $M \subseteq H$ und $a,b \in H$.
a) a ist ein maximales (minimales) Element von M, falls $a \in M$ gilt und aus $a \leq x$ $(x \leq a)$ für $x \in M$ schon $x = a$ folgt.
b) Ist $a \in M$, und gilt $x \leq a$ $(a \leq x)$ für alle $x \in M$, so heißt a größtes (kleinstes) Element von M (und ist wegen der Antisymmetrie eindeu-

tig bestimmt).

c) a heißt eine obere (untere) Schranke von M, falls $x \leq a$ $(a \leq x)$ für alle $x \in M$ gilt (dabei muß a nicht zu M gehören).

8.3 Beispiel: M sei die Teilmenge $\{y,z,u,v,w\}$ der oben angegebenen Halbordnung H_6. M hat ein größtes Element, nämlich u, und kein kleinstes Element. Die minimalen Elemente von M sind z und w. M hat keine untere Schranke. Die Menge $N = \{y,v\}$ hat u als obere und z als untere Schranke.

Aus der Definition einer Halbordnung ergibt sich auch hier die Gültigkeit eines Dualtitätsprinzips:

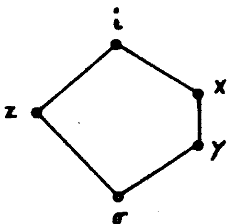
8.4 Lemma: Ist $(H,\leq)$ eine Halbordnung, so ist dies auch $(H,\geq)$, wenn man "$x \geq y$" als gleichbedeutend mit "$y \leq x$" festsetzt. $(H,\geq)$ heißt die zu $(H,\leq)$ duale Halbordnung. Bei der Dualisierung gehen die Begriffe "maximales Element", "größtes Element", "obere Schranke" über in die dualen Begriffe "minimales Element", "kleinstes Element", "untere Schranke".

8.5 Definition: Sei $(H,\leq)$ eine Halbordnung und M eine Teilmenge von H. Hat die Menge aller oberen Schranken von M ein kleinstes Element, so heißt dieses das Supremum von M, in Zeichen: sup M. Dual dazu ist das Infimum (inf M) definiert. Existieren $\sup\{x,y\}$ und $\inf\{x,y\}$ zu je zwei Elementen $x,y \in H$, so nennt man $(H,\leq)$ eine Verbandsordnung.

8.6 Beispiele:

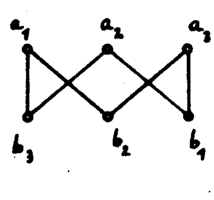
a) In der Halbordnung H_6 (s.o.) gilt z.B. $\sup\{y,v\} = u = \sup\{y,v,w\}$, $\inf\{y,v\} = z$, jedoch existiert $\inf\{v,w\}$ nicht. H_6 ist also keine Verbandsordnung.

b) Für jede Menge M ist $(\mathbb{P}(M),\subseteq)$ eine Verbandsordnung, denn für $A,B \in \mathbb{P}(M)$ gilt $\sup\{A,B\} = A \cup B$ und $\inf\{A,B\} = A \cap B$.

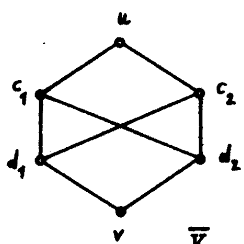


N_5

$\mathbb{N}$



K_6



$\overline{K}_4$

c) Von den in den obigen Diagrammen dargestellten Halbordnungen sind N_5 und $\mathbb{N}$ Verbandsordnungen, K_6 und $\overline{K}_4$ jedoch nicht: sup $\{a_1,a_2\}$ bzw. sup $\{d_1,d_2\}$ existieren nicht.

Für eine Verbandsordnung $(H,\leq)$ betrachten wir nun die zweistelligen Operationen sup: $H^2 \to H$ und inf: $H^2 \to H$. Es zeigt sich, daß die algebraische Struktur (H; sup, inf) eine Reihe von Gleichungen erfüllt, die auch in Booleschen Algebren gelten:

8.7 <u>Lemma:</u> Sei $(H,\leq)$ eine Verbandsordnung. Schreiben wir (für $a,b \in H$) $a+b$ statt sup $\{a,b\}$ und $a\cdot b$ statt inf $\{a,b\}$, so gelten in $(H;+,\cdot)$ die folgenden Gleichungen:

(V_1)	$x+x = x$	$(\overline{V}_1)$	$x\cdot x = x$
(V_2)	$x+y = y+x$	$(\overline{V}_2)$	$x\cdot y = y\cdot x$
(V_3)	$x+(y+z) = (x+y)+z$	$(\overline{V}_3)$	$x\cdot(y\cdot z) = (x\cdot y)\cdot z$
(V_4)	$x+(x\cdot y) = x$	$(\overline{V}_4)$	$x\cdot(x+y) = x$

<u>Beweis:</u> (V_1) und (V_2) sind sofort klar. Zum Nachweis von (V_3) betrachte man (für $x,y,z \in H$) $a := x + (y+z) = \sup\{x, \sup\{y,z\}\}$ und $b := (x+y) + z = \sup\{\sup\{x,y\},z\}$. Es ist $a \geq x$ und $a \geq \sup\{y,z\}$, also ist a eine obere Schranke von $\{x,y,z\}$. Damit gilt aber insbesondere $a \geq \sup\{x,y\}$ und folglich $a \geq \sup\{\sup\{x,y\},z\} = b$. Entsprechend folgt auch $b \geq a$ und mit der Antisymmetrie dann $a = b$. Für (V_4) braucht man nur, daß stets $\inf\{x,y\} \leq x$ ist: daraus folgt sofort $x + (x\cdot y) = \sup\{x, \inf\{x,y\}\} = x$ ●

Unter den Voraussetzungen von 8.7 gilt $a \leq b$ offenbar genau dann, wenn $a+b = b$ bzw. $a\cdot b = a$ ist. Eine Art Umkehrung liefert die folgende Aussage:

8.8 <u>Lemma:</u> Sei $(H;+,\cdot)$ eine Algebra (vom Typ (2,2)), die den Gesetzen (V_1)-(V_4) und $(\overline{V}_1)$-$(\overline{V}_4)$ genügt. Definiert man auf H eine binäre Relation $\leq$ durch

"$x \leq y$ genau dann, wenn $x\cdot y = x$ gilt",

so wird $(H,\leq)$ zur verbandsgeordneten Menge, und für je zwei Elemente $a,b \in H$ ist dann $\sup\{a,b\} = a+b$ und $\inf\{a,b\} = a\cdot b$.

<u>Beweis:</u> Zunächst wird gezeigt, daß für beliebige Elemente $a,b \in H$ die Beziehungen $a\cdot b = a$ und $a+b = b$ äquivalent sind:

aus $a \cdot b = a$ folgt $a+b = (a \cdot b)+b = b+(b \cdot a) = b$;
aus $a+b = b$ folgt $a \cdot b = a \cdot (a+b) = a$.
Als nächstes weisen wir nach, daß $(H,\le)$ eine Halbordnung ist.
Reflexivität: $x \cdot x = x$, also $x \le x$ für alle $x \in H$.
Transitivität: Sei $x \le y$ und $y \le z$, also $x \cdot y = x$ und $y \cdot z = y$.
Es folgt $x \cdot z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y = x$, also $x \le z$.
Antisymmetrie: Aus $x \le y$ und $y \le x$ folgt $x = x \cdot y = y \cdot x = y$.
Nun wird gezeigt, daß $x \cdot y = \inf\{x,y\}$ für beliebige $x,y \in H$ gilt. Wegen $(x \cdot y) \cdot x = x \cdot y$ und $(x \cdot y) \cdot y = x \cdot y$ folgt $x \cdot y \le x$ und $x \cdot y \le y$, d.h. $x \cdot y$ ist untere Schranke von $\{x,y\}$. Ist nun s eine beliebige untere Schranke von $\{x,y\}$, also $s \cdot x = s$ und $s \cdot y = s$, so folgt $s \cdot (x \cdot y) = (s \cdot x) \cdot y = s \cdot y = s$, d.h. $s \le x \cdot y$. Damit ist jedoch $x \cdot y$ als größte untere Schranke von $\{x,y\}$ nachgewiesen, d.h. $x \cdot y = \inf\{x,y\}$. Entsprechend zeigt man $x+y = \sup\{x,y\}$, indem man die Äquivalenz von "$x \le y$" und "$x+y = y$" verwendet.

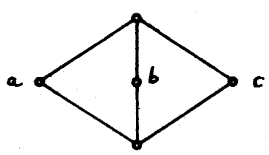
8.9 <u>Definition:</u> Eine Algebra $(H;+,\cdot)$, die den Gleichungen (V_1)-(V_4) und $(\overline{V}_1)$-$(\overline{V}_4)$ genügt, heißt ein <u>Verband</u>.

Zusammenfassend können wir somit feststellen:
Die Verbände stehen in eineindeutiger Korrespondenz zu den Verbandsordnungen, diese Korrespondenz wird durch 8.7 und 8.8 beschrieben. Daher ist es üblich, wenn man von einem Verband bzw. einer Verbandsordnung spricht, stets beides zu meinen, d.h. man hat dann Operationen $+,\cdot$ und eine Relation $\le$ gegeben.

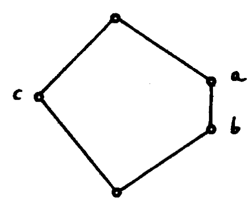
Ein Verband, in dem zusätzlich das Gesetz

$$x \cdot (y+z) = (x \cdot y) + (x \cdot z)$$

gilt, heißt <u>distributiver Verband</u>. In jedem distributiven Verband gilt auch das duale Gesetz $x + (y \cdot z) = (x+y) \cdot (x+z)$ (siehe Übungsaufgabe 31). Daß nicht jeder Verband distributiv sein muß, zeigen die folgenden Beispiele:



M_3



N_5

In beiden Fällen ist $a \cdot (b+c) \neq (a \cdot b) + (a \cdot c)$.

Gibt es in einem Verband ein größtes Element, so wird dieses mit "1" bezeichnet, entsprechend das kleinste Element (falls es existiert) mit "0". Für alle $x \in H$ gilt dann

$$x + 1 = 1 \quad \text{und} \quad x \cdot 0 = 0.$$

Das Beispiel $(\mathbb{Z},\leq)$ zeigt, daß ein Verband weder 0 noch 1 haben muß. Jedoch hat jeder endliche Verband ein größtes und ein kleinstes Element (siehe Übungsaufgabe 32).

Ein Verband mit 0 und 1, in dem zu jedem x ein Komplement y existiert (d.i. ein Element y mit $x+y = 1$ und $x \cdot y = 0$), heißt ein <u>komplementärer Verband</u>. Die oben dargestellten Verbände M_3 und N_5 sind komplementär; jedoch sind die Komplemente nicht eindeutig: in beiden sind a und b Komplemente von c. Jedoch gilt:

8.10 <u>Lemma:</u> Sei $(H;+,\cdot)$ ein distributiver Verband mit 0 und 1. Dann hat jedes Element höchstens ein Komplement.

<u>Beweis:</u> Seien $a,b,c \in H$ und sowohl b als auch c ein Komplement von a; es gilt also $a \cdot b = a \cdot c = 0$ und $a+b = a+c = 1$. Wir zeigen $b=c$. Es ist $b+c = (b+c)\cdot 1 = (b+c)\cdot(a+b) = ab + b + ac + bc = b + bc = b$ und entsprechend $b+c = (b+c)\cdot 1 = (b+c)\cdot(a+c) = ab + bc + ac + c = bc + c = c$. Damit folgt $b=c$.●

Da in einem komplementären distributiven Verband H Komplemente eindeutig sind, kann man in diesem Fall die Komplementbildung als einstellige Operation $': H \to H$ auffassen und erhält:

8.11 <u>Satz:</u> Ist $(H;+,\cdot)$ ein komplementärer distributiver Verband, und ist (für $x \in H$) x' das (eindeutig bestimmte) Komplement zu x, so ist $(H;\, +,\, \cdot,\, ',\, 0,\, 1)$ eine Boolesche Algebra. Umgekehrt ist für jede Boolesche Algebra $(B;\, +,\, \cdot,\, ',\, 0,\, 1)$ die Algebra $(B;+,\cdot)$ ein komplementärer distributiver Verband.

Wegen dieses Zusammenhangs wird ein komplementärer distributiver Verband auch <u>Boolescher Verband</u> genannt. Oft wird gar nicht zwischen einer Booleschen Algebra und dem dazugehörigen Booleschen Verband unterschieden.

<u>Übungsaufgaben:</u>

30. Für $n \in \mathbb{N}$ sei $T_n := \{k \in \mathbb{N} \mid k|n\}$ ($k|n$ steht für: "k ist Teiler von n."). Man zeichne ein Hasse Diagramm von $(T_{30}, |)$. Man zeige: $(T_n, |)$ ist eine distributive Verbandsordnung. Für welche n ist $(T_n, |)$ Boolesch?

31. Zeige, daß in jedem Verband $(H;+,\cdot)$ aus dem einen Distributivgesetz $x\cdot(y+z) = xy + xz$ das andere Gesetz $x+yz = (x+y)\cdot(x+z)$ folgt - und umgekehrt.

32. Man beweise:
    a) Ist $(V,\leq)$ eine Verbandsordnung und M eine endliche Teilmenge von V, so existieren $\sup M$ und $\inf M$ in V.
    b) Jeder endliche Verband hat 0 und 1.

§ 9. VOLLSTÄNDIGE ATOMARE BOOLESCHE ALGEBREN UND IHRE DARSTELLUNG

Sei V ein Verband. Zu jeder endlichen Teilmenge $S \subseteq V$ existieren in V das Supremum $\sup S$ und das Infimum $\inf S$ (siehe Übungsaufgabe 32). Existieren $\sup S$ und $\inf S$ zu jeder *beliebigen* Teilmenge S von V, so heißt V vollständig. Eine Boolesche Algebra wird vollständig genannt, wenn sie als Verband (vgl. 8.11) vollständig ist.

9.1 Beispiele:

a) Jeder endliche Verband ist vollständig, insbesondere also auch jede endliche Boolesche Algebra.
b) Für eine beliebige Menge M ist $(\mathbb{P}(M);\cup,\cap)$ ein vollständiger Verband: es ist $\sup S = \bigcup\{X \mid X\in S\}$ und $\inf S = \bigcap\{X \mid X\in S\}$ für $S \subseteq \mathbb{P}(M)$.
c) $(\mathbb{E}(\mathbb{N});\ \cup,\ \cap,\ \bar{\ },\ \emptyset,\ \mathbb{N})$ ist nicht vollständig (vgl. 2.2b) zur Definition von $\mathbb{E}(X)$ für eine Menge X). Man sieht dies daran, daß etwa die Menge $S = \{\{x\} \mid x\in\mathbb{N},\ x \text{ ist gerade}\} \subseteq \mathbb{E}(\mathbb{N})$ kein Supremum in $\mathbb{E}(\mathbb{N})$ besitzt: die Menge aller oberen Schranken besteht aus denjenigen Mengen natürlicher Zahlen, die alle geraden Zahlen enthalten und deren Komplement endlich ist; unter diesen Mengen gibt es jedoch keine kleinste.

Wir wollen vereinbaren, daß wir künftig statt $\sup S$ $(\inf S)$ auch $\sum\limits_{x\in S} x$ $(\prod\limits_{x\in S} x)$ schreiben.

9.2 Lemma: Sei B eine Boolesche Algebra, $S = \{x_i \mid i\in I\}$ eine Teilmenge von B und $y\in B$. Falls $\sum\limits_{i\in I} x_i$ existiert, so existiert auch $\sum\limits_{i\in I} (y\cdot x_i)$, und es gilt dann

$$y \cdot \sum_{i\in I} x_i = \sum_{i\in I} (y\cdot x_i).$$

Beweis: Zunächst ist klar, daß $y\cdot \sum\limits_{i\in I} x_i$ eine obere Schranke der Menge $\{y\cdot x_i \mid i\in I\}$ ist. Wir zeigen, daß es die kleinste obere Schranke ist. Sei dazu u eine beliebige obere Schranke von $\{y\cdot x_i \mid i\in I\}$, also $u \geq y\cdot x_i$ für alle $i\in I$. Wir erhalten

$$x_i = (y+y')\cdot x_i = yx_i + y'x_i \leq u + y'x_i \leq u + y'$$

und folgern $\sum\limits_{i\in I} x_i \leq u + y'$. Multiplikation mit y ergibt

$$y \cdot \sum_{i\in I} x_i \leq y\cdot(u+y') = y\cdot u \leq u,$$

und dies war zu beweisen.

9.3 <u>Folgerung:</u> In jeder vollständigen Booleschen Algebra gilt das "unendliche Distributivgesetz"

$$y \cdot \sum_{i \in I} x_i = \sum_{i \in I} (y \cdot x_i) \; .$$

Sei V ein Verband mit 0. Ein Element $a \in V$ heißt ein <u>Atom</u>, falls a ein minimales Element in $V \setminus \{0\}$ ist, d.h. falls $a > 0$ gilt und aus $0 < b \leq a$ folgt $b = a$. V heißt <u>atomar</u>, wenn für jedes $x \in V$ mit $x > 0$ ein Atom $a \leq x$ existiert.

9.4 <u>Beispiele:</u>

a) Jeder endliche Verband ist atomar (siehe Übungsaufgabe 33).
b) Für jede Menge M sind $\mathbb{P}(M)$ und $\mathbb{E}(M)$ atomar. Atome sind gerade die einelementigen Teilmengen von M.

9.5 <u>Lemma:</u> Sei V ein Verband mit 0 und a ein Atom von V. Für jedes Element x von V gilt $a \leq x$ oder $a \cdot x = 0$.

<u>Beweis:</u> Auf jeden Fall ist $a \cdot x \leq a$. Dies bedeutet aber, da a Atom ist, daß $a \cdot x = 0$ oder $a \cdot x = a$ (also $a \leq x$) gilt.

Wir haben nun genügend Hilfsmittel bereitgestellt, um den Hauptsatz dieses Abschnitts formulieren und beweisen zu können:

9.6 <u>Satz:</u> Eine Boolesche Algebra $(B; +, \cdot, ', 0, 1)$ ist genau dann zu einer Potenzmengenalgebra $(\mathbb{P}(M); \cup, \cap, \bar{\ }, \emptyset, M)$ isomorph, wenn sie vollständig und atomar ist.

<u>Beweis:</u> Aus 9.1 und 9.4 wissen wir, daß jede Potenzmengenalgebra (und damit auch jede zu einer solchen isomorphe Boolesche Algebra) vollständig und atomar ist.
Nun sei umgekehrt eine vollständige atomare Boolesche Algebra $(B; +, \cdot, ', 0, 1)$ gegeben, A sei die Menge aller Atome von B. Für $x \in B$ setzen wir

$$\psi(x) := \{a \in A \mid a \leq x\}.$$

Der Beweis ist fertig, wenn wir gezeigt haben, daß $\psi\colon B \to \mathbb{P}(A)$ ein Isomorphismus von $(B; +, \cdot, ', 0, 1)$ auf $(\mathbb{P}(A); \cup, \cap, -, \emptyset, A)$ ist.

Wir werden dies in drei Schritte zerlegen:

I. ψ ist ein Homomorphismus;

II. ψ ist injektiv;

III. ψ ist surjektiv.

<u>Zu I.:</u> $\psi(1) = A$ und $\psi(0) = \emptyset$ sind klar. Es bleibt zu zeigen, daß für beliebige $x,y \in B$ $\psi(x+y) = \psi(x) \cup \psi(y)$, $\psi(x\cdot y) = \psi(x) \cap \psi(y)$ und $\psi(x') = \overline{\psi(x)}$ gilt.

Ist $a \in \psi(x) \cup \psi(y)$, also o.B.d.A. $a \in \psi(x)$, so folgt mit $a \le x$ auch $a \le x+y$ und $a \in \psi(x+y)$. Sei umgekehrt $a \in \psi(x+y)$, also a ein Atom und $a \le x+y$. Wäre $a \not\le x$ und $a \not\le y$, so hätte man mit 9.5, daß $a\cdot x = 0$ und $a\cdot y = 0$ ist, folglich auch $a\cdot(x+y) = ax + ay = 0$ und $a \not\le x+y$ im Widerspruch zur Voraussetzung. Also muß $a \le x$ oder $a \le y$ und damit $a \in \psi(x) \cup \psi(y)$ sein.

Sei nun $a \in \psi(x\cdot y)$. Es folgt $a \le x\cdot y$, also $a \le x$ und $a \le y$, m.a.W. $a \in \psi(x) \cap \psi(y)$. Umgekehrt zieht $a \in \psi(x) \cap \psi(y)$ sofort $a \le x\cdot y$ und $a \in \psi(x\cdot y)$ nach sich.

Sei $a \in \psi(x')$ bzw. $a \le x'$. Wäre nun auch $a \le x$, so folgte $a \le x\cdot x' = 0$, ein Widerspruch. Also muß $a \in \overline{\psi(x)}$ sein. Ist umgekehrt $a \in \overline{\psi(x)}$ bzw. $a \not\le x$, so folgt $a \le x'$ und $a \in \psi(x')$, denn mit $a \not\le x'$ ergäbe sich der Widerspruch $a = a(x+x') = ax + ax' = 0$.

<u>Zu II.:</u> Da B atomar ist, gilt offenbar $\psi(x) = \emptyset$ nur für $x = 0$. Wir nehmen nun an, es gäbe $x \neq y$ mit $\psi(x) = \psi(y)$. Zunächst würde o.B.d.A. $x \neq x+y$ folgen und $\psi(x) = \psi(x+y)$. Dies zeigt, daß wir schon von vornherein $x < y$ voraussetzen können. Aus $\psi(y\cdot x') = \psi(y) \cap \psi(x') = \psi(x) \cap \overline{\psi(x)} = \emptyset$ folgt $y\cdot x' = 0$. Da außerdem $x+x' = y+x' = 1$ gilt sowie $x\cdot x' = 0$, haben sich sowohl x als auch y als Komplemente von x' herausgestellt, was $x=y$ und damit einen Widerspruch nach sich zieht.

<u>Zu III.:</u> Sei $S = \{x_i \mid i\in I\}$ eine Teilmenge von A und $s := \sum_{i\in I} x_i$. Wir zeigen $\psi(s) = S$.

$\psi(s) \supseteq S$ ist klar. Nehmen wir an, es gäbe ein $a \in A\setminus S$ mit $a \in \psi(s)$ bzw. $a \le s$. Man hätte dann $a = a\cdot s = a \cdot \sum_{i\in I} x_i = \sum_{i\in I} (a\cdot x_i)$ nach 9.3. Da a und alle x_i Atome sind und $a \neq x_i$ ist für jedes $i\in I$, würde dies $a\cdot x_i = 0$ für alle i und damit $a=0$ nach sich ziehen. Also ist $\psi(s) = S$.

9.7 <u>Folgerung:</u> Jede endliche Boolesche Algebra ist isomorph zu einer Potenzmengenalgebra.

Der <u>Beweis</u> ergibt sich mit 9.1 und 9.4.

Zusammen mit 2.23 erhält man nun auch:

9.8 <u>Folgerung:</u> Jede endliche Boolesche Algebra ist isomorph zu einer Potenz von $\mathbf{2}$.

Mit 9.6 haben wir gesehen, daß vollständige atomare Boolesche Algebren nichts anders als Potenzmengenalgebren "sind". Das Beispiel $\mathbb{E}(\mathbb{N})$ einer nicht vollständigen Booleschen Algebra (vgl. 9.1 c)) zeigt, daß dies noch nicht *alle* Booleschen Algebren erfaßt. Der Darstellungssatz des nächsten Paragraphen wird sich auf beliebige Boolesche Algebren beziehen, dafür jedoch nur die Isomorphie zu einer *Unteralgebra* einer Potenzmengenalgebra liefern.

Zum Ende dieses Abschnitts wollen wir eine Boolesche Algebra angeben, die zwar vollständig, jedoch nicht atomar ist:

9.9 <u>Beispiel:</u> Wir betrachten die Potenzmengenalgebra $\mathbb{P}(\mathbb{N})$ auf den natürlichen Zahlen und definieren auf $\mathbb{P}(\mathbb{N})$ eine Kongruenzrelation Θ, indem wir sagen, $A \Theta B$ solle genau in dem Falle gelten, daß die symmetrische Differenz $A \Delta B$ endlich ist. Die Boolesche Algebra $\mathbb{P}(\mathbb{N})/\Theta$ hat kein Atom. Nehmen wir an, wir hätten ein Atom $[A]\Theta$. Der Repräsentant A müßte unendlich sein, denn für jede endliche Menge $E \subseteq \mathbb{N}$ ist $[E]\Theta$ das Nullelement von $\mathbb{P}(\mathbb{N})/\Theta$. Man könnte A in zwei disjunkte unendliche Mengen zerlegen $(A = A_1 \cup A_2)$, und es würde folgen $[A]\Theta \underset{\neq}{>} [A_1]\Theta \underset{\neq}{>} [0]\Theta$ im Widerspruch zur Annahme, daß $[A]\Theta$ ein Atom ist.

<u>Übungsaufgaben:</u>

33. Man beweise, daß jeder endliche Verband atomar ist.

34. Zeige: Eine endliche Boolesche Algebra hat 2^n viele Elemente, wenn n die Anzahl der Atome ist.

35. Zeige: Zwei endliche Boolesche Algebren mit gleicher Elementzahl sind isomorph.

§ 10. DER STONESCHE DARSTELLUNGSSATZ

Sei B eine atomare Boolesche Algebra und A die Menge der Atome von B. Aus dem Beweis von 9.6 kann man herauslesen, daß die Abbildung $\psi: B \to \mathbb{P}(A)$ mit $\psi(b) = \{x \in A \mid x \leq b\}$ ein injektiver Homomorphismus von B in die Potenzmengenalgebra von A ist, denn nur zum Beweis der Surjektivität von ψ wurde dort die Vollständigkeit von B benötigt. Also ist B isomorph zu einer Unteralgebra von $\mathbb{P}(A)$.
Nun gibt es Boolesche Algebren ohne auch nur ein Atom (vgl. Beispiel 9.9). Einen Ersatz für die Atome findet man in dem Begriff des "Ultrafilters".

10.1 Definition: Sei B eine Boolesche Algebra und F eine nichtleere Teilmenge von B. F heißt Filter auf B, falls folgende Bedingungen erfüllt sind:

(i) Mit $x,y \in F$ ist auch $x \cdot y \in F$.

(ii) Ist $x \in F$ und $y \in B$ mit $y \geq x$, so folgt $y \in F$.

(iii) $0 \notin F$.

Anmerkung: Ein Ideal ist dual zu einem Filter definiert. Es ist leicht zu zeigen, daß $F \subseteq B$ genau dann ein Filter ist, wenn $\{x' \mid x \in F\}$ ein Ideal ist.

10.2 Beispiele:

a) Ist B Boolesche Algebra und $0 \neq a \in B$, so ist $[a) := \{x \in B \mid x \geq a\}$ ein Filter auf B. Solche Filter nennt man Hauptfilter.

b) $\{X \subseteq \mathbb{N} \mid \mathbb{N} \setminus X \text{ ist endlich}\}$ ist ein Filter auf $\mathbb{P}(\mathbb{N})$.

c) Ist F ein Filter auf der Booleschen Algebra B und $x \in B$ ein Element mit $x \notin F$ und $x' \notin F$, so gilt: der Filter $F_x := \{y \in B \mid y \geq a \cdot x$ für ein $a \in F\}$ ist der *kleinste* unter den Filtern G mit $F \subseteq G$ und $x \in G$.

Ist B eine Boolesche Algebra, so bezeichnen wir mit $F(B)$ die Menge aller Filter auf B. $F(B)$ wird mit der mengentheoretischen Inklusion "$\subseteq$" zu einer Halbordnung $(F(B), \subseteq)$.

10.3 Definition: Sei B eine Boolesche Algebra. Ein Ultrafilter auf B ist ein maximales Element von $F(B)$. (Dual dazu ist der Begriff des Primideals.)

Es ist unmittelbar einsichtig, daß für ein $a \in B$ der Filter $[a)$ genau dann ein Ultrafilter ist, wenn a ein Atom von B ist. Zum Beweis, daß es stets Ultrafilter gibt - auch wenn keine Atome zur Verfügung stehen -, wird das Auswahlaxiom benötigt, das wir in der Form des Zornschen Lemmas*) benutzen:

10.4 Lemma: Sei B eine Boolesche Algebra, $F \subseteq B$ ein Filter auf B. Dann existiert ein Ultrafilter U auf B mit $F \subseteq U$.

Beweis: Wir zeigen, daß die Menge

$$\mathcal{F} := \{G \subseteq B \mid G \text{ ist Filter auf } B \text{ und } F \subseteq G\},$$

die wegen $F \in \mathcal{F}$ offensichtlich nicht leer ist, induktiv geordnet ist. Sei also $\emptyset \neq \mathcal{k} \subseteq \mathcal{F}$ eine totalgeordnete Teilmenge von $\mathcal{F}$. Wir behaupten: $\bigcup \mathcal{k} \in \mathcal{F}$.

Zunächst muß gezeigt werden, daß $\bigcup \mathcal{k}$ ein Filter auf B ist. Seien $x,y \in \bigcup \mathcal{k}$. Es gibt $F_1, F_2 \in \mathcal{k}$ mit $x \in F_1$ und $y \in F_2$. Da $\mathcal{k}$ totalgeordnet ist, kann o.B.d.A. $F_1 \subseteq F_2$ angenommen werden. Es folgt $x,y \in F_2$ und $x \cdot y \in F_2 \subseteq \bigcup \mathcal{k}$.

Ist $x \in \bigcup \mathcal{k}$ und $y \in B$ mit $y \geq x$, so gibt es ein $F_1 \in \mathcal{k}$ mit $x \in F_1$, und man hat $y \in F_1 \subseteq \bigcup \mathcal{k}$.

Da schließlich offenbar auch $0 \notin \bigcup \mathcal{k}$ gilt, ist $\bigcup \mathcal{k}$ als Filter auf B nachgewiesen. Trivialerweise ist auch $F \subseteq \bigcup \mathcal{k}$.

Somit folgt $\bigcup \mathcal{k} \in \mathcal{F}$, und es ist bewiesen, daß $\mathcal{F}$ induktiv geordnet ist.

Nach dem Zornschen Lemma gibt es nun in $\mathcal{F}$ ein maximales Element U. Es ist klar, daß U ein Ultrafilter ist, der F enthält.

Für das Weitere wollen wir einige weitere charakterisierende Eigenschaften von Ultrafiltern bereitstellen:

10.5 Lemma: Sei F ein Filter auf der Booleschen Algebra B. Dann sind die folgenden Bedingungen äquivalent:

(i) F ist ein Ultrafilter.

(ii) Für jedes $x \in B$ ist $x \in F$ oder $x' \in F$.

(iii) Ist $x+y \in F$, so muß $x \in F$ oder $y \in F$ gelten.

---

*) Dieses setzen wir hier - zusammen mit den in ihm verwendeten Begriffen - als bekannt voraus.

Beweis:

(i) impliziert (ii) (siehe auch 10.2 c)): Hätte man ein x mit $x \notin F$ und $x' \notin F$, so wäre F_x ein F echt enthaltender Filter, F könnte somit kein Ultrafilter sein.

(ii) impliziert (iii): Sei $x+y \in F$, jedoch $x \notin F$ und $y \notin F$. Aufgrund der Voraussetzung folgt $x' \in F$ und $y' \in F$, also $x' \cdot y' = (x+y)' \in F$, was $(x+y) \cdot (x+y)' = 0 \in F$ und damit einen Widerspruch ergibt.

(iii) impliziert (i): Wäre F kein Ultrafilter, so gäbe es einen Filter G mit $F \subsetneq G$. Für $x \in G \setminus F$ folgte dann $x' \notin G$ und somit $x' \notin F$, jedoch $x+x' = 1 \in F$. Dies ergäbe einen Widerspruch zu (iii), wonach $x \in F$ oder $x' \in F$ sein müßte.

Wir kommen nun zu einem allgemeinen Darstellungssatz:

10.6 Satz: Sei B eine Boolesche Algebra, $UF(B)$ die Menge aller Ultrafilter auf B. Dann ist die Abbildung

$$\psi : B \to \mathbb{P}(UF(B))$$

mit $\quad \psi(b) := \{F \in UF(B) \mid b \in F\}$

ein injektiver Homomorphismus, also ein Isomorphismus von B auf die Unteralgebra $\psi(B)$ von $\mathbb{P}(UF(B))$.

Da Unteralgebren von Potenzmengenalgebren auch Mengenkörper genannt werden, kann man 10.6 verkürzt so ausdrücken:

Jede Boolesche Algebra ist isomorph zu einem Mengenkörper.

Beweis von 10.6: Zunächst muß gezeigt werden, daß ψ ein Homomorphismus ist. Angesichts von 10.5 ist dies sehr einfach: z.B. folgt mit (iii) sofort

$$\begin{aligned} \psi(b_1+b_2) &= \{F \in UF(B) \mid b_1+b_2 \in F\} \\ &= \{F \in UF(B) \mid b_1 \in F\} \cup \{F \in UF(B) \mid b_2 \in F\} \end{aligned}$$

und damit $\psi(b_1+b_2) = \psi(b_1) \cup \psi(b_2)$.

Ebenso können die anderen Bedingungen leicht nachgeprüft werden.

Es bleibt die Injektivität von ψ nachzuweisen.

Sei $b_1 \neq b_2$. Wir können o.B.d.A. $b_1 \not\leq b_2$ annehmen. Wir zeigen, daß es einen Ultrafilter in $\psi(b_1) \setminus \psi(b_2)$ gibt.

Zunächst folgt $b_1 \cdot b_2' \neq 0$, denn aus $b_1 \cdot b_2' = 0$ würde folgen $b_1 = b_1 \cdot (b_2+b_2') = b_1 b_2 + b_1 b_2' = b_1 b_2$ und $b_1 \leq b_2$, was ein Widerspruch wäre. Mit 10.4 erhalten wir nun die Existenz eines Ultrafilters U, der den Filter $[b_1 b_2')$ (siehe 10.2.a) enthält. Offenbar gilt $b_1 \in U$ und $b_2 \notin U$, d.h. $U \in \psi(b_1) \setminus \psi(b_2)$●

Anmerkung: Da in einer atomaren Booleschen Algebra für jedes Atom a der Hauptfilter $[a)$ der einzige Ultrafilter ist, der a enthält, ist 10.6 die präzise Verallgemeinerung von 9.6.

Wir geben uns mit 10.6 noch nicht zufrieden und wollen die zu der Booleschen Algebra B isomorphe Unteralgebra von $\mathbb{P}(UF(B))$ genauer beschreiben. Dazu bedienen wir uns der Sprache der Topologie.*)

Zunächst ist es eine leichte Übung, sich folgendes zu überlegen: Ist U ein Ultrafilter auf der Booleschen Algebra B, so ist die Abbildung $\phi_U : B \to \mathbf{2}$ mit

$$\phi_U(x) := \begin{cases} 1, & \text{falls } x \in U \\ 0, & \text{falls } x \notin U \end{cases}$$

ein Homomorphismus von B auf $\mathbf{2}$; ist umgekehrt ψ ein Homomorphismus von B auf $\mathbf{2}$, so ist $\psi^{-1}(\{1\})$ ein Ultrafilter auf B, und es gilt

$$\psi = \phi_{\psi^{-1}(\{1\})} .$$

Man kann folglich $UF(B)$ mit der Menge Hom $(B,\mathbf{2})$ der Homomorphismen von B auf $\mathbf{2}$ identifizieren.

Fassen wir nun $\mathbf{2} = \{0,1\}$ als topologischen Raum mit der diskreten Topologie auf, so ist $\mathbf{2}$ kompakt. Nach dem Satz von Tychonoff ist damit auch $\mathbf{2}^B$ kompakt.

In 10.7, 10.8 und 10.6* werden wir von einer gegebenen Booleschen Algebra B und der mit der diskreten Topologie versehenen zweielementigen Booleschen Algebra $\mathbf{2}$ ausgehen.

10.7 Lemma: Hom $(B,\mathbf{2})$ ist eine abgeschlossene Teilmenge von $\mathbf{2}^B$.

Beweis: Aufgrund elementarer Tatsachen bezüglich Produkttopologien folgt, daß die Mengen der Form $U_{(b,i)} := \{f \in \mathbf{2}^B \mid f(b) = i\}$ $(b \in B,\ i \in \mathbf{2})$ eine Subbasis von $\mathbf{2}^B$ bilden; die endlichen Durchschnitte solcher Mengen bil-

*) Die topologischen Grundbegriffe werden hier als bekannt vorausgesetzt.

den eine Basis. Wegen $2^B \setminus U_{(b,i)} = U_{(b,i')}$ hat man: die Elemente der Subbasis (und mithin auch der Basis) sind offen *und* abgeschlossen in 2^B; der Raum 2^B ist also total unzusammenhängend. Da der Durchschnitt von abgeschlossenen Mengen stets wieder abgeschlossen ist, brauchen wir zum Beweis von 10.7 nur zu zeigen, daß jeweils die Menge derjenigen Abbildungen $B \to 2$, die mit einer der Booleschen Grundoperationen verträglich sind, eine abgeschlossene Teilmenge von 2^B ist. Betrachten wir die Komplementierung:

$$\{f \in 2^B \mid f(b') = f(b)' \text{ für alle } b \in B\} \text{ ist nichts anderes als}$$

$$\bigcap \{(U_{(b,0)} \cap U_{(b',1)}) \cup (U_{(b,1)} \cap U_{(b',0)}) \mid b \in B\},$$

also abgeschlossen.
Entsprechend argumentiert man für die anderen Operationen.

Wir können nun auch schließen, daß die Mengen der Form

$$T_b := \{\phi \in \mathrm{Hom}\,(B,2) \mid \phi(b) = 1\} \quad (b \in B)$$

eine Subbasis des mit der Relativtopologie versehenen Raumes $\mathrm{Hom}\,(B,2)$ bilden (siehe Übungsaufgabe 37). Das System der Mengen T_b ist unter endlichen Durchschnitten abgeschlossen (dies ergibt sich aus der Homomorphieeigenschaft der Elemente von T_b) und bildet also eine Basis des - wegen 10.7 kompakten - Raumes $\mathrm{Hom}\,(B,2)$. Da jede der Mengen T_b offen und abgeschlossen ist, ist $\mathrm{Hom}\,(B,2)$ total unzusammenhängend.

10.8 <u>Lemma:</u> Sei $\Phi \subseteq \mathrm{Hom}\,(B,2)$. Φ ist genau dann offen-abgeschlossen, wenn es ein $b \in B$ mit $\Phi = T_b$ gibt.

<u>Beweis:</u> Sei $\Phi \subseteq \mathrm{Hom}\,(B,2)$ offen-abgeschlossen. Da Φ offen ist, ist Φ Vereinigung von Mengen der Form T_b. Da Φ abgeschlossen und somit kompakt ist, gibt es $b_1,\dots,b_n \in B$ mit $\Phi = T_{b_1} \cup \dots \cup T_{b_n}$. Es folgt $\Phi = T_{b_1+\dots+b_n}$.

Betrachtet man nun nochmals Satz 10.6 und benutzt die Entsprechung von Ultrafiltern auf B und Homomorphismen von B auf 2, so erhält man:

10.6* <u>Satz:</u> Die Abbildung $\psi: B \to \mathbf{P}(\mathrm{Hom}\,(B,2))$ mit

$$\psi(b) := \{\phi \in \mathrm{Hom}\,(B,2) \mid \phi(b) = 1\}$$

ist ein injektiver Homomorphismus. ψ ist ein Isomorphismus von B auf den Mengenkörper der offen-abgeschlossenen Teilmengen des kompakten total unzusammenhängenden topologischen Raumes Hom $(B,\mathbf{2})$.

Aufgrund obiger Tatsachen nennt man einen kompakten total unzusammenhängenden topologischen Raum auch Booleschen Raum.
Offensichtlich bilden die offen-abgeschlossenen Mengen eines Booleschen Raumes X stets eine Boolesche Algebra, die man mit B_X bezeichnet und die zu dem Booleschen Raum X duale Boolesche Algebra nennt. Entsprechend heißt der Boolesche Raum Hom $(B,\mathbf{2})$ der zu B duale Boolesche Raum.

10.9 Darstellungssatz von Stone:

a) Ist B eine Boolesche Algebra, so ist $B_{\mathrm{Hom}(B,\mathbf{2})} \cong B$, d.h. die duale Algebra zum dualen Booleschen Raum ist isomorph zu B; die Abbildung

$$\Gamma: B \to B_{\mathrm{Hom}(B,\mathbf{2})}$$
$$\text{mit} \quad \Gamma(b) := \{\phi \in \mathrm{Hom}\,(B,\mathbf{2}) \mid \phi(b) = 1\}$$

ist ein Isomorphismus.
b) Ist X ein Boolescher Raum, so ist Hom $(B_X,\mathbf{2}) \cong X$, d.h. der duale Boolesche Raum zur dualen Booleschen Algebra ist homöomorph zu X; die Abbildung

$$\Delta: X \to \mathrm{Hom}\,(B_X,\mathbf{2})$$
$$\text{mit} \quad \Delta(x)(A) := \begin{cases} 1, & \text{falls } x \in A \\ 0, & \text{falls } x \notin A \end{cases}$$

ist ein Homöomorphismus.

Es sei noch angemerkt, daß sich die in 10.9 beschriebene "Dualität" auch auf die Morphismen ausdehnen läßt: einem Homomorphismus zwischen Booleschen Algebren läßt sich auf natürliche Weise eine stetige Abbildung zwischen den entsprechenden Booleschen Räumen (allerdings "in umgekehrter Richtung") zuordnen - und umgekehrt. Man spricht in einem solchen Fall von einer Dualität zwischen der Kategorie der Booleschen Algebren und der Kategorie der Booleschen Räume.

Zu 10.9 bleibt anzumerken, daß wir nur a) gezeigt haben (mit 10.6*). Der Beweis von b) sei als (anspruchsvollere) Übung empfohlen.

Übungsaufgaben:

36. a) Sei $\phi\colon B \to C$ ein Homomorphismus zwischen Booleschen Algebren. Man zeige, daß $\phi^{-1}(\{0\})$ ein Ideal, $\phi^{-1}(\{1\})$ ein Filter auf B ist.

b) Zeige: Ist F ein Filter auf der Booleschen Algebra B, so gibt es eine Kongruenz Θ auf B mit $F = [1]\Theta$.

37. Sei B eine Boolesche Algebra, $b \in B$ und $i \in \mathbf{2}$. Man setzt $T_{(b,i)} := \{\phi \in \mathrm{Hom}\,(B,\mathbf{2}) \mid \phi(b) = i\}$. Zeige, daß es zu $b_1, b_2 \in B$ und $i,j \in \mathbf{2}$ stets ein $b \in B$ gibt mit $T_{(b_1,i)} \cap T_{(b_2,j)} = T_{(b,1)}$.

§ 11. FREIE BOOLESCHE ALGEBREN

Wir betrachten nochmals die Boolesche Algebra 2^{2^n} der Schaltfunktionen. Dabei sei die natürliche Zahl n beliebig vorgegeben. Mit π_i $(i = 1,\dots,n)$ haben wir die i-te Projektion $x_i^2: 2^n \to 2$ bezeichnet. Nach 4.2 gilt für ein beliebiges $f \in 2^{2^n}$

$$f = \sum_{(\alpha_1,\dots,\alpha_n)\in T(f)} \pi_1^{\alpha_1} \cdot \dots \cdot \pi_n^{\alpha_n} .$$

Wie an früherer Stelle bereits erwähnt, besagt dies unter anderem, daß 2^{2^n} von der Menge $\{\pi_1,\dots,\pi_n\}$ erzeugt wird. Wir zeigen als nächstes, daß 2^{2^n} *die größte* Boolesche Algebra ist, die von einer n-elementigen Teilmenge erzeugt wird.

11.1 Satz: Sei B eine Boolesche Algebra, $b_1,\dots,b_n$ seien Elemente von B. Dann gibt es genau einen Homomorphismus $\phi: 2^{2^n} \to B$ mit $\phi(\pi_i) = b_i$ für $i = 1,\dots,n$, nämlich

$$\phi(f) = \sum_{(\alpha_1,\dots,\alpha_n)\in T(f)} b_1^{\alpha_1} \cdot \dots \cdot b_n^{\alpha_n} \quad \text{für alle } f \in 2^{2^n} .$$

Beweis: Wenn ψ ein Homomorphismus von 2^{2^n} in B mit $\psi(\pi_i) = b_i$ $(i = 1,\dots,n)$ ist, dann gilt

$$\begin{aligned}\psi(f) &= \psi\Big(\sum_{(\alpha_1,\dots,\alpha_n)\in T(f)} \pi_1^{\alpha_1} \cdot \dots \cdot \pi_n^{\alpha_n}\Big) \\ &= \sum_{(\alpha_1,\dots,\alpha_n)\in T(f)} \psi(\pi_1)^{\alpha_1} \cdot \dots \cdot \psi(\pi_n)^{\alpha_n} \\ &= \sum_{(\alpha_1,\dots,\alpha_n)\in T(f)} b_1^{\alpha_1} \cdot \dots \cdot b_n^{\alpha_n} ,\end{aligned}$$

d.h. wenn es überhaupt einen Homomorphismus $\psi: 2^{2^n} \to B$ mit $\psi(\pi_i) = b_i$ $(i = 1,\dots,n)$ gibt, dann muß dieser wie im Satz angegeben definiert werden und ist damit eindeutig bzw. gleich ϕ. Daß die oben definierte Funktion ϕ tatsächlich ein Homomorphismus ist, kann leicht nachgerechnet werden: z.B. folgt wegen $T(f+g) = T(f) \cup T(g)$

$$\phi(f+g) = \sum_{(\alpha_1,\ldots,\alpha_n)\in T(f+g)} b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}$$

$$= \sum_{(\alpha_1,\ldots,\alpha_n)\in T(f)} b_1^{\alpha_1}\cdot\ldots\cdot b_n^{\alpha_n} + \sum_{(\alpha_1,\ldots,\alpha_n)\in T(g)} b_1^{\alpha_1}\cdot\ldots\cdot b_n^{\alpha_n}$$

$$= \phi(f) + \phi(g).$$

11.2 <u>Folgerung:</u> Sei B eine Boolesche Algebra, $b_1,\ldots,b_n \in B$. Dann besteht die in B von $\{b_1,\ldots,b_n\}$ erzeugte Unteralgebra aus allen Elementen der Form

$$\sum_{(\alpha_1,\ldots,\alpha_n)\in S} b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n} ,$$

wobei S die Teilmengen von $\mathbf{2}^n$ durchläuft.

<u>Beweis:</u> Man braucht sich nur klarzumachen, daß $\langle\{b_1,\ldots,b_n\}\rangle_B$ gerade das Bild $\phi(\mathbf{2}^{\mathbf{2}^n})$ des in 11.1 angegebenen Homomorphismus ist.

Wir können hier festhalten, daß 11.2 ein einfacheres Verfahren zur Berechnung der von $\{b_1,\ldots,b_n\}$ erzeugten Booleschen Unteralgebra liefert als das in 2.10 angegebene.

Der in 11.1 angegebene Homomorphismus $\phi\colon \mathbf{2}^{\mathbf{2}^n} \to B$ ist offenbar genau dann surjektiv, wenn $\{b_1,\ldots,b_n\}$ ein Erzeugendensystem von B ist. Damit ist klar, daß eine von n Elementen erzeugte Boolesche Algebra höchstens 2^{2^n} viele Elemente haben kann.

11.3 <u>Definition:</u> Sei B eine Boolesche Algebra, $b_1,\ldots,b_n \in B$. $\{b_1,\ldots,b_n\}$ heißt ein <u>freies Erzeugendensystem</u> von B, falls die Abbildung $\phi\colon \mathbf{2}^{\mathbf{2}^n} \to B$ aus 11.1 bijektiv ist, d.h. falls sich jedes Element $a\in B$ auf genau eine Weise in der Form

$$a = \sum_{(\alpha_1,\ldots,\alpha_n)\in S} b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}$$

darstellen läßt. Eine Boolesche Algebra heißt <u>frei</u>, wenn sie ein freies Erzeugendensystem besitzt.

$\{\pi_1,\dots,\pi_n\}$ ist ein freies Erzeugendensystem von $\mathbf{2}^{\mathbf{2}^n}$. Aus 11.1 und 11.2 erhält man:

11.4 <u>Folgerung:</u> Eine endliche Boolesche Algebra ist genau dann frei, wenn sie für ein gewisses n isomorph zu $\mathbf{2}^{\mathbf{2}^n}$ ist.

Da eine endliche Boolesche Algebra bis auf Isomorphie schon durch die Anzahl ihrer Elemente bzw. durch die Anzahl ihrer Atome festgelegt ist (siehe Übungsaufgaben 34 und 35), können wir auch schließen, daß die Eigenschaft, frei zu sein, gleichbedeutend ist damit, 2^{2^n} viele Elemente bzw. 2^n Atome (für ein gewisses n) zu haben.

Es soll nun ein einfaches Kriterium dafür angegeben werden, daß eine Menge $\{b_1,\dots,b_n\}$ von Elementen einer Booleschen Algebra B ein freies Erzeugendensystem der von ihr erzeugten Unteralgebra ist:

11.5 <u>Satz:</u> Für eine Boolesche Algebra B und $b_1,\dots,b_n \in B$ ist $\{b_1,\dots,b_n\}$ genau dann ein freies Erzeugendensystem von $\langle\{b_1,\dots,b_n\}\rangle_B$, wenn für alle $(\alpha_1,\dots,\alpha_n) \in \mathbf{2}^n$ gilt $b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n} \neq 0$.

<u>Beweis:</u> Ist $\{b_1,\dots,b_n\}$ freies Erzeugendensystem von $\{b_1,\dots,b_n\}_B$, so muß wegen der Isomorphie dieser Unteralgebra zu $\mathbf{2}^{\mathbf{2}^n}$ stets $b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n} \neq 0$ sein. Für die Umkehrung zeigen wir, daß unter der Voraussetzung $b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n} \neq 0$ (für beliebiges $(\alpha_1,\dots,\alpha_n) \in \mathbf{2}^n$) der in 11.1 angegebene Homomorphismus $\phi\colon \mathbf{2}^{\mathbf{2}^n} \to B$ injektiv ist, womit dann die Behauptung folgt. Seien $f,g \in \mathbf{2}^{\mathbf{2}^n}$ mit $f \neq g$. O.B.d.A. können wir ein $(\gamma_1,\dots,\gamma_n) \in T(f) \setminus T(g)$ nehmen. Wäre nun $\phi(f) = \phi(g)$, so würde folgen

$$\begin{aligned}
b_1^{\gamma_1}\cdot\ldots\cdot b_n^{\gamma_n} &= b_1^{\gamma_1}\cdot\ldots\cdot b_n^{\gamma_n} \cdot \sum_{(\alpha_1,\dots,\alpha_n)\in T(f)} b_1^{\alpha_1}\cdot\ldots\cdot b_n^{\alpha_n} \\
&= b_1^{\gamma_1}\cdot\ldots\cdot b_n^{\gamma_n} \cdot \sum_{(\alpha_1,\dots,\alpha_n)\in T(g)} b_1^{\alpha_1}\cdot\ldots\cdot b_n^{\alpha_n} \\
&= \sum_{(\alpha_1,\dots,\alpha_n)\in T(g)} (b_1^{\alpha_1}\cdot\ldots\cdot b_n^{\alpha_n})\cdot(b_1^{\gamma_1}\cdot\ldots\cdot b_n^{\gamma_n}) \\
&= 0 \quad \text{wegen } (\gamma_1,\dots,\gamma_n) \notin T(g).
\end{aligned}$$

<u>Anmerkung:</u> Es ist leicht zu sehen, daß unter den Voraussetzungen von 11.5 die Elemente der Form $b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}$ $((\alpha_1,\ldots,\alpha_n) \in \mathbf{2}^n)$ die Atome der Unteralgebra $\langle\{b_1,\ldots,b_n\}\rangle_B$ sind; selbstverständlich müssen diese nicht notwendigerweise Atome von B sein.

11.6 <u>Beispiel:</u> Wir betrachten die Potenzmengenalgebra $\mathbf{P}(\{1,2,3,4,5\})$. $B_1 = \{1,2\}$ und $B_2 = \{2,3,4,5\}$ bilden kein freies Erzeugendensystem der von ihnen erzeugten Mengenalgebra, denn es ist $\overline{B}_1 \cap \overline{B}_2 = \{3,4,5\} \cap \{1\} = \emptyset$. Dagegen ist die von $C_1 = \{1,2,3\}$ und $C_2 = \{2,3,5\}$ erzeugte Unteralgebra frei, denn es gilt: $C_1 \cap C_2 = \{2,3\}$, $C_1 \cap \overline{C}_2 = \{1\}$, $\overline{C}_1 \cap C_2 = \{5\}$, $\overline{C}_1 \cap \overline{C}_2 = \{4\}$ - keiner dieser zu betrachtenden Durchschnitte ist leer.

Die Nützlichkeit freier Algebren liegt vor allem darin, daß die allgemeine Gültigkeit von Gleichungen an ihnen getestet werden kann. Als Vorbereitung formulieren wir die folgende Konsequenz von 11.1 und 11.4:

11.7 <u>Folgerung:</u> Ist $\{b_1,\ldots,b_n\}$ ein freies Erzeugendensystem der Booleschen Algebra B und sind $c_1,\ldots,c_n$ Elemente einer Booleschen Algebra C, so gibt es genau einen Homomorphismus $\psi\colon B \to C$ mit $\psi(b_i) = c_i$ für $i = 1,\ldots,n$.

11.8 <u>Satz:</u> Sei $\{b_1,\ldots,b_n\}$ ein freies Erzeugendensystem der Booleschen Algebra B, $p(x_1,\ldots,x_n)$ und $q(x_1,\ldots,x_n)$ seien Boolesche Terme. Ist $p^B(b_1,\ldots,b_n) = q^B(b_1,\ldots,b_n)$, so folgt $p \equiv q$, d.h. $p^C(c_1,\ldots,c_n) = q^C(c_1,\ldots,c_n)$ für beliebige Elemente $c_1,\ldots,c_n$ einer Booleschen Algebra C.

<u>Beweis:</u> Für gegebene $c_1,\ldots,c_n$ in einer Booleschen Algebra C betrachten wir den aufgrund von 11.7 existierenden Homomorphismus $\psi\colon B \to C$ mit $\psi(b_i) = c_i$ für $i = 1,\ldots,n$. Es folgt

$$\begin{aligned} p^C(c_1,\ldots,c_n) &= p^C(\psi(b_1),\ldots,\psi(b_n)) = \psi(p^B(b_1,\ldots,b_n)) \\ &= \psi(q^B(b_1,\ldots,b_n)) = q^C(\psi(b_1),\ldots,\psi(b_n)) = q^C(c_1,\ldots,c_n). \end{aligned}$$

Wir wollen noch einmal zu dem Problem zurückkehren, für zwei vorgelegte Boolesche Terme $p(x_1,\ldots,x_n)$ und $q(x_1,\ldots,x_n)$ zu entscheiden, ob die Gleichung "$p = q$" in allen Booleschen Algebren gilt. Wir wissen aus 4.11, und es folgt nochmals aus dem Stoneschen Darstellungssatz, daß man nur nachzuprüfen braucht, ob die Gleichung in der Booleschen Algebra $\mathbf{2}$ gilt.

Mit Hilfe von 11.8 können wir nun nachweisen, daß man die Gültigkeit von "$p = q$" auch mit Hilfe der bekannten Venn-Diagramme nachprüfen kann:*)

11.9 Zur Beweiskraft von Venn-Diagrammen:

Sei X das Innere eines Quadrats in der euklidischen Ebene. Wir betrachten Teilmengen $B_1,\dots,B_n$ von X, die sich darstellen lassen als Innengebiete von doppelpunktfreien, geschlossenen, glatten Kurven in X. Seien $p(x_1,\dots,x_n)$ und $q(x_1,\dots,x_n)$ Boolesche Terme.
Um nachzuprüfen, ob

$$p^C(c_1,\dots,c_n) = q^C(c_1,\dots,c_n)$$

für beliebige Elemente $c_1,\dots,c_n$ einer Booleschen Algebra C gilt, genügt es nach 11.8, ein Venn-Diagramm zu betrachten, in dem die Mengen $B_1,\dots,B_n$ ein freies Erzeugendensystem der von ihnen erzeugten Unteralgebra von $\mathbb{P}(X)$ bilden, und nachzusehen, ob in diesem Beispiel

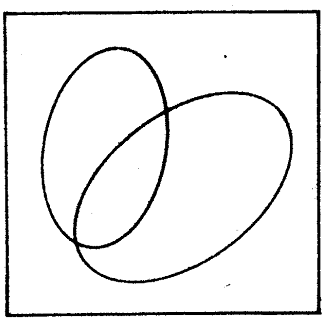
$$p^{\mathbb{P}(X)}(B_1,\dots,B_n) = q^{\mathbb{P}(X)}(B_1,\dots,B_n)$$

gilt.
Nach 11.5 ist ein Venn-Diagramm (in diesem Sinne) genau dann beweiskräftig, wenn

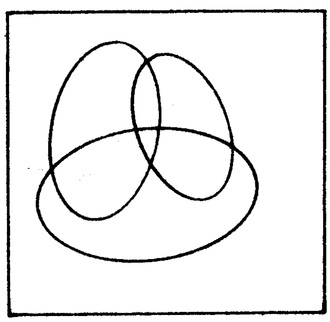
$$B_1^{\alpha_1} \cap \dots \cap B_n^{\alpha_n} \neq \emptyset$$

ist für alle $(\alpha_1,\dots,\alpha_n) \in \mathbf{2}^n$.

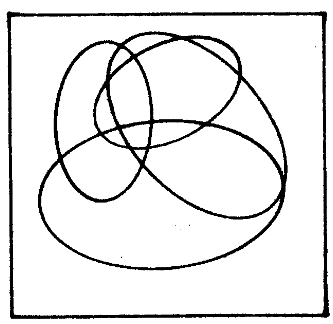
Beispiele beweiskräftiger Venn-Diagramme:



n=2



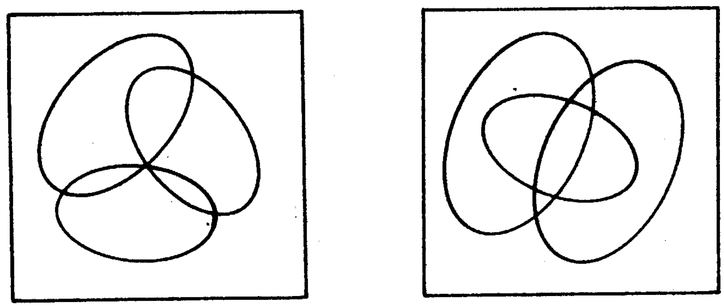
n=3



n=4

*) Eine ausführliche Behandlung dieser Thematik findet man in dem Aufsatz von A. Kirsch: Venn-Diagramme und freie Boolesche Verbände; in: Der Mathematikunterricht 18/2 (1972), 15-33.

Beispiele nicht-beweiskräftiger Venn-Diagramme (n=3):



Wie man sieht, zeigen die oberen (beweiskräftigen) Diagramme jeweils Mengen "in allgemeinster Lage", während in den beiden unteren Diagrammen spezielle Beziehungen zwischen den dargestellten Mengen bestehen.

Übungsaufgaben:

38. Sei B eine von $\{b_1,\dots,b_n\}$ erzeugte Boolesche Algebra, $(\alpha_1,\dots,\alpha_n) \in \mathbf{2}^n$. Man beweise, daß das Element $b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}$ entweder gleich 0 oder ein Atom von B ist.

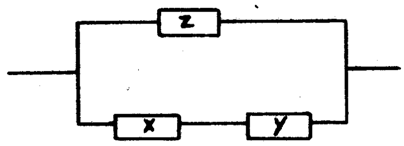
39. Begründe, daß die Boolesche Algebra $\mathbb{P}(\{1,2,3,4\})$ frei ist, und gib ein freies Erzeugendensystem an.

LÖSUNGSVORSCHLÄGE ZU DEN ÜBUNGSAUFGABEN

1. a) $z + ((x+y')\cdot((x'\cdot y)+y))$

   b) $z + ((x+y')\cdot((x'\cdot y)+y)) \equiv z + ((x+y')\cdot y)$
   $\equiv z + (x\cdot y) + (y'\cdot y)$
   $\equiv z + (x\cdot y);$

   vereinfachter Schaltkreis:



2. a) $u' + (u')' \equiv 1$ nach (8) und
   $u' \cdot (u')' \equiv 0$ nach $(\overline{8})$,
   also ist $(u')'$ ein Komplement von u'. Da andererseits auch u ein Komplement von u' ist und Komplemente eindeutig sind (siehe Seite 9), folgt $(u')' \equiv u$.

   b) $(u\cdot(v+w))' \equiv u' + (v+w)' \equiv u' + (v'\cdot w')$ folgt nach den De Morganschen Regeln.

3. Für Teilmengen A, B von X ist $(A \Rightarrow B) = \overline{A}\cup B$. Es ist $(A \Rightarrow B) = X$ bzw. $\overline{A}\cup B = X$ offenbar genau dann der Fall, wenn $A \subseteq B$ gilt.

4. Daß die Menge $\{0,b,b',1\}$ abgeschlossen ist, kann leicht nachgerechnet werden.
   Es ist $\langle\emptyset\rangle_B = \{0,1\}$, da $\{0,1\}$ die kleinste abgeschlossene Menge ist.

5. Sei k die kleinste Mächtigkeit eines Erzeugendensystems von T_{30}. Offensichtlich gilt $k \geq 2$, da jede von einem Element erzeugte Unteralgebra einer Booleschen Algebra nach 4. höchstens vier Elemente haben kann. Andererseits gilt aber $\langle\{2,3\}\rangle_{T_{30}} = T_{30}$, wie man mit Satz 2.10 nachprüft. Folglich ist $k = 2$.

6. Es ist die Abgeschlossenheit von $C = \{bx \mid x \in B\} \cup \{b'+x \mid x \in B\}$ nachzuprüfen. Wegen $0 = b \cdot 0$ und $1 = b'+1$ folgt sofort $0, 1 \in C$. Wir zeigen nur die Abgeschlossenheit unter der Multiplikation, für $+$ und $'$ verlaufen die Beweise ähnlich. Abkürzend wird $C_1 = \{bx \mid x \in B\}$ und $C_2 = \{b'+x \mid x \in B\}$ gesetzt. Seien $a_1, a_2 \in C$.
1. Fall: $a_1, a_2 \in C_1$. Es existieren $x_1, x_2 \in B$ mit $a_1 = bx_1$ und $a_2 = bx_2$. Daraus folgt $a_1a_2 = (bx_1)\cdot(bx_2) = b\cdot(x_1x_2)$ und somit $a_1a_2 \in C_1 \subseteq C$.
2. Fall: $a_1 \in C_1$, $a_2 \in C_2$. Es existieren $x_1, x_2 \in B$ mit $a_1 = bx_1$ und $a_2 = b'+x_2$. Man erhält $a_1a_2 = bx_1\cdot(b'+x_2) = b\cdot(x_1x_2)$ und wieder $a_1a_2 \in C_1 \subseteq C$.
3. Fall: $a_1, a_2 \in C_2$. Hier ist $a_1 = b'+x_1$ und $a_2 = b'+x_2$, also $a_1a_2 = (b'+x_1)\cdot(b'+x_2) = b' + x_1x_2$ und damit $a_1a_2 \in C_2 \subseteq C$.

7. Nehmen wir an, $(\mathbb{E}(\mathbb{N}); \cup, \cap, \overline{}, \emptyset, \mathbb{N})$ sei von den endlich vielen Teilmengen $S_1, \ldots, S_n$ erzeugt. Darunter seien o.B.d.A. $S_1, \ldots, S_k$ endlich und $S_{k+1}, \ldots, S_n$ "koendlich" (d.h. ihr Komplement ist endlich). Dann ist $\mathbb{E}(\mathbb{N})$ auch von den *endlichen* Mengen $S_1, \ldots, S_k, \overline{S_{k+1}}, \ldots, \overline{S_n}$ erzeugt. Deswegen können wir o.B.d.A. von vornherein annehmen, daß $S_1, \ldots, S_n$ allesamt endliche Mengen sind. Mit $B := S_1 \cup \ldots \cup S_n$ und Übungsaufgabe 6 haben wir nun, daß $C = C_1 \cup C_2$ mit $C_1 = \{B \cap X \mid X \in \mathbb{E}(\mathbb{N})\}$ und $C_2 = \{\overline{B} \cup X \mid X \in \mathbb{E}(\mathbb{N})\}$ eine Unteralgebra ist, die die Elemente $S_1, \ldots, S_n$ (die in C_1 liegen) enthält, folglich

$$\langle\{S_1, \ldots, S_n\}\rangle_{\mathbb{E}(\mathbb{N})} \subseteq C.$$

Ein Widerspruch ergibt sich nun daraus, daß wir $C \neq \mathbb{E}(\mathbb{N})$ zeigen können: Ist b ein beliebiges Element von $\mathbb{N}\setminus B$, so ist zwar $B \cup \{b\} \in \mathbb{E}(\mathbb{N})$, jedoch gilt $B \cup \{b\} \notin C_1$ (wegen $B \cup \{b\} \nsubseteq B$) und $B \cup \{b\} \notin C_2$ (da jedes Element von C_2 koendlich ist).

8. a) $\operatorname{Ker} \phi = \{(S_1, S_2) \mid c \in S_1 \cap S_2\} \cup \{(S_1, S_2) \mid c \in \overline{S}_1 \cap \overline{S}_2\}$

b) $\operatorname{Ker} \phi = \{(r,s) \mid 5 \text{ teilt } r \text{ und } s\} \cup$
$\cup \{(r,s) \mid 5 \text{ teilt weder } r \text{ noch } s\}$

c) $\operatorname{Ker} \phi = \{(r,s) \mid r = s\} = \{(r,r) \mid r \in T_{30}\}$
(triviale Kongruenz).

9. Es gibt nur eine Abbildung einer nichtleeren Menge B in eine einelementige Menge; diese ist offensichtlich ein Homomorphismus. Ihr Kern ist $B\times B$.

10. a) $(A_1,B_1) \in \Theta$ und $(A_2,B_2) \in \Theta$ heißt:

A_1 und B_1 unterscheiden sich in höchstens endlich vielen Elem.
und
A_2 und B_2 " " " " " " "
Dann gilt:
$A_1\cup A_2$ und $B_1\cup B_2$ " " " " " " "
sowie
$A_1\cap A_2$ und $B_1\cap B_2$ " " " " " " "
und
A_1' und B_1' " " " " " " "

b) $[\emptyset]\Theta$ ist die Menge aller endlichen Teilmengen von X.

11. Man kann die Kongruenzeigenschaften für Θ_F nachweisen wie in 10. Man kann aber auch Satz 2.23 ausnutzen, denn man hat (mit Θ wie in 10) $(A_1,B_1) \in \Theta$ genau dann, wenn $(\psi(A_1), \psi(B_1)) \in \Theta_F$ gilt. Das heißt, daß unter ψ die Kongruenz Θ auf die Relation Θ_F in $\mathbf{2}^M$ abgebildet wird. Da ψ ein Isomorphismus ist, führt er auch Kongruenzrelationen in Kongruenzrelationen über.

12. $A\subseteq B$ heißt: $A\cap B = A$. Ist ϕ ein Homomorphismus mit $\phi(B) = 0$, so hat man: $\phi(A) = \phi(A\cap B) = \phi(A)\cdot\phi(B) = \phi(A)\cdot 0 = 0$.

13. $\underline{f(x_1,x_2,x_3) = (x_1'\cdot x_2'\cdot x_3 + x_1'x_2x_3' + x_1x_2'x_3')^{\mathbf{2}}}$,

$\underline{g(x_1,x_2,x_3) = (x_1'x_2'x_3 + x_1x_2'x_3' + x_1x_2'x_3 + x_1x_2x_3)^{\mathbf{2}}}$.

14. Schaltfunktion:

x_1	x_2	x_3	$h(x_1,x_2,x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$\underline{h(x_1,x_2,x_3) = (x_1'x_2x_3 + x_1x_2'x_3 + x_1x_2x_3' + x_1x_2x_3)^{\mathbf{2}}}$.

15. Schaltfunktion:

x_1	x_2	x_3	$p^2(x_1,x_2,x_3)$	$p_1(x_1x_2x_3)'$
0	0	0	0	1
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

Da $T(p^2(x_1,x_2,x_3))$ so groß ist, stellen wir $p^2(x_1,x_2,x_3)'$ dar und komplementieren anschließend.
Man erhält $p^2(x_1,x_2,x_3)' = (x_1'x_2'x_3')^2$ und damit

$$\underline{p^2(x_1,x_2,x_3) = (x_1'x_2'x_3')'^2 = (x_1 + x_2 + x_3)^2.}$$

16. Sei $p = (x_1+x_2x_3)(x_1'x_2+x_4)'$. Dann gilt

$$\begin{aligned}
p &\equiv (x_1+x_2x_3)((x_1'x_2)'\cdot x_4') \equiv (x_1+x_2x_3)\cdot(x_1+x_2')\cdot x_4' \\
&\equiv (x_1x_1 + x_1x_2' + x_2x_3x_1 + x_2x_3x_2')\cdot x_4' \\
&\equiv x_1x_4' + x_1x_2'x_4' + x_1x_2x_3x_4' \\
&\equiv x_1(x_2+x_2')(x_3+x_3')x_4' + x_1x_2'(x_3+x_3')x_4' + x_1x_2x_3x_4' \\
&\equiv x_1x_2x_3x_4' + x_1x_2'x_3x_4' + x_1x_2x_3'x_4' + x_1x_2'x_3'x_4' + \\
&\quad + x_1x_2'x_3x_4' + x_1x_2'x_3'x_4' + x_1x_2x_3x_4' \\
&\equiv \underline{x_1x_2x_3x_4' + x_1x_2'x_3x_4' + x_1x_2x_3'x_4' + x_1x_2'x_3'x_4'}\ .
\end{aligned}$$

Andere Methode:

x_1	x_2	x_3	x_4	$x_1+x_2x_3$	$(x_1'x_2+x_4)'$	p
0	0	0	0	0	1	0
0	0	0	1	0	0	0
0	0	1	0	0	1	0
0	0	1	1	1	0	0
0	1	0	0	0	0	0
0	1	0	1	0	0	0
0	1	1	0	0	0	0
0	1	1	1	1	0	0
1	0	0	0	1	1	1
1	0	0	1	1	0	0
1	0	1	0	1	1	1
1	0	1	1	1	0	0
1	1	0	0	1	1	1
1	1	0	1	1	0	0
1	1	1	0	1	1	1
1	1	1	1	1	0	0

Also $\underline{p \equiv x_1x_2'x_3'x_4' + x_1x_2'x_3x_4' + x_1x_2x_3'x_4' + x_1x_2x_3x_4'}$.

Konjunktive Normalform:

$$\begin{aligned} p \equiv\ & (x_1+x_2+x_3+x_4)(x_1+x_2+x_3+x_4')(x_1+x_2+x_3'+x_4)(x_1+x_2+x_3'+x_4') \cdot \\ & \cdot (x_1+x_2'+x_3+x_4)(x_1+x_2'+x_3+x_4')(x_1+x_2'+x_3'+x_4)(x_1+x_2'+x_3'+x_4') \cdot \\ & \cdot (x_1'+x_2+x_3+x_4')(x_1'+x_2+x_3'+x_4')(x_1'+x_2'+x_3+x_4')(x_1'+x_2'+x_3'+x_4'). \end{aligned}$$

17. Sei $p = xy' + x'y + yz' + y'z$ und $q = xy' + x'z + yz'$.
Dann hat man:

x	y	z	$p^{\mathbf{2}}$	$q^{\mathbf{2}}$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	0	0

Es folgt $p^{\mathbf{2}} = q^{\mathbf{2}}$,
also $p \underset{\mathbf{2}}{\equiv} q$ und somit
$p \equiv q$ mit Folgerung 4.11.

18. $p \hookrightarrow q$ ist gleichbedeutend mit $p \cdot q \equiv p$ (vgl. 5.7).
Aus $p \cdot q \equiv p$ folgt $p+q \equiv p \cdot q + q \equiv q$.
Umgekehrt hat man auch, daß aus $p+q = q$ folgt: $p \cdot q \equiv p \cdot (p+q) \equiv p$.

19. a) $p \hookrightarrow q$ bedeutet $p+q \equiv q$ (siehe Übungsaufgabe 18).
Damit hat man auch $p + (q+r) \equiv (q+r)$, also $p \hookrightarrow q+r$.
b) Aus $p \hookrightarrow q$ und $p \hookrightarrow r$ folgt $p \cdot q \equiv p$ und $p \cdot r \equiv p$. Man hat dann $p \cdot q \cdot r \equiv p$, also $p \hookrightarrow q \cdot r$.
Dual zu b):
c) $p \hookrightarrow q$ und $r \hookrightarrow q$ heißt $p+q \equiv q$ und $r+q \equiv q$. Also ist $p+q+r \equiv q$, somit $p+r+q \equiv q$ und $p+r \hookrightarrow q$.

20. $p \hookrightarrow q$ heißt $T(p^{\mathbf{2}}) \subseteq T(q^{\mathbf{2}})$.
Wegen $T(p^{\mathbf{2}}) = T(p^{\mathbf{2}})$ hat man $p \hookrightarrow p$ (Reflexivität).
Aus $p \hookrightarrow q$ und $q \hookrightarrow r$ hat man $T(p^{\mathbf{2}}) \subseteq T(q^{\mathbf{2}}) \subseteq T(r^{\mathbf{2}})$, also $T(p^{\mathbf{2}}) \subseteq T(r^{\mathbf{2}})$, was gleichbedeutend ist mit $p \hookrightarrow r$ (Transitivität).

21. p_1 und p_2 sind Produktterme. Ist p_2 ein Teilterm von p_1, so gibt es einen Term r mit $p_1 \equiv p_2 \cdot r$.
Es folgt $p_1 + p_2 + \ldots + p_k \equiv p_2 r + p_2 + p_3 + \ldots + p_k \equiv p_2 + p_3 + \ldots + p_k$.

22. a) $x_1'x_2x_3x_4' + x_1x_2x_3 + x_1'x_3'x_4 + x_1'x_3x_4 \equiv$

$\equiv x_1'x_2x_3x_4' + x_1x_2x_3 + x_1'x_3'x_4 + x_1'x_3x_4 + x_2x_3x_4' + x_1'x_4 \equiv$

$\equiv x_1x_2x_3 + x_2x_3x_4' + x_1'x_4 \equiv$

$\equiv x_1x_2x_3 + x_2x_3x_4' + x_1'x_4 + x_2x_3x_4 + x_2x_3 \equiv$

$\equiv \underline{x_1'x_4 + x_2x_3}\,.$

b) $x_1x_2x_3x_4 + x_1x_2x_3'x_4x_5 + x_1x_2'x_3x_4x_5 + x_1x_2'x_3x_4'x_5 +$

$+ x_1x_3'x_4'x_5 + x_1'x_2'x_3x_4x_5 + x_1'x_2x_3'x_4x_5' + x_1x_2'x_3'x_4' \equiv$

$\equiv x_1x_2x_3x_4 + x_1x_2x_3'x_4x_5 + x_1x_2'x_3x_4x_5 + x_1x_2'x_3x_4'x_5 + x_1x_3'x_4'x_5 +$

$+ x_1'x_2'x_3x_4x_5 + x_1'x_2x_3'x_4x_5' + x_1x_2'x_3'x_4' + x_1x_2x_4x_5 + x_1x_2'x_3x_5 \equiv$

$\equiv x_1x_2x_3x_4 + x_1x_3'x_4'x_5 + x_1'x_2'x_3x_4x_5 + x_1'x_2x_3'x_4x_5' +$

$+ x_1x_2'x_3'x_4' + x_1x_2x_4x_5 + x_1x_2'x_3x_5 + x_2'x_3x_4x_5 \equiv$

$\equiv \underline{x_1x_2x_3x_4 + x_1x_3'x_4'x_5 + x_1'x_2x_3'x_4x_5' + x_1x_2'x_3'x_4' + x_1x_2x_4x_5 +}$

$+ \underline{x_1x_2'x_3x_5 + x_2'x_3x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_3'x_5 + x_1x_2'x_4'x_5}\,.$

23. Der in Teil a) der vorigen Aufgabe gefundene Term $x_1'x_4 + x_2x_3$ ist bereits minimal, denn kein Summand ist überflüssig. Für den Term in Teil b) erstellen wir eine Tabelle:

	ϕ_1 $x_1x_2x_3x_4$	ϕ_2 $x_1x_3'x_4'x_5$	ϕ_3 $x_1'x_2x_3'x_4x_5'$	ϕ_4 $x_1x_2'x_3'x_4'$	ϕ_5 $x_1x_2x_4x_5$	ϕ_6 $x_1x_2'x_3x_5$	ϕ_7 $x_2'x_3x_4x_5$	ϕ_8 $x_1x_3x_4x_5$	ϕ_9 $x_1x_2x_3'x_5$	ϕ_{10} $x_1x_2'x_4'x_5$	
ϕ_1		0	0	0	α_5	0	0	α_5	0	0	
ϕ_2	0			α_2'	0	0	0	0	α_2	α_2'	ü
ϕ_3	0	0		0	0	0	0	0	0	0	
ϕ_4	0	α_5	0		0	0	0	0	0	α_5	
ϕ_5	α_3	0	0	0		0	0	α_3	α_3'	0	ü
ϕ_6	0	0	0	0	0		α_4	α_4	0	α_4'	ü
ϕ_7	0	0	0	0	0	α_1		α_1	0	0	
ϕ_8	α_2	0	0	0	α_2	α_2'	α_2'		0	0	ü
ϕ_9	0	α_4'	0	0	α_4	0	0	0		0	ü
ϕ_{10}	0	α_3'	0	α_3'	0	α_3	0	0	0		ü

Man kann z.B. ϕ_2, ϕ_5, ϕ_6 und ϕ_8 weglassen und erhält:

$$\underline{p \equiv x_1x_2x_3x_4 + x_1'x_2x_3'x_4x_5' + x_1x_2'x_3'x_4' + x_2'x_3x_4x_5 + x_1x_2x_3'x_5 + x_1x_2'x_4'x_5}$$

Ließe man ϕ_9 weg, so müßte man ϕ_2 beibehalten. Ließe man ϕ_{10} weg, so müßte man ϕ_6 beibehalten. Da alle diese Summanden vier Variablen haben, folgt, daß der angegebene Term sicher minimal ist. Es gibt aber noch mehr minimale!

24. x_1 stehe für den Präsidenten.

$x_1x_2x_3x_4$	$f(x_1,x_2,x_3,x_4)$
0 0 0 0	0
0 0 0 1	0
0 0 1 0	0
0 0 1 1	0
0 1 0 0	0
0 1 0 1	0
0 1 1 0	0
0 1 1 1	1
1 0 0 0	0
1 0 0 1	1
1 0 1 0	1
1 0 1 1	1
1 1 0 0	1
1 1 0 1	1
1 1 1 0	1
1 1 1 1	1

$$\begin{aligned}
p = {} & x_1'x_2x_3x_4 + x_1x_2'x_3'x_4 + x_1x_2'x_3x_4' + x_1x_2'x_3x_4 + x_1x_2x_3'x_4' + \\
& x_1x_2x_3'x_4 + x_1x_2x_3x_4' + x_1x_2x_3x_4 \\
\equiv {} & x_1'x_2x_3x_4 + x_1x_2'x_3'x_4 + x_1x_2'x_3x_4' + x_1x_2'x_3x_4 + x_1x_2x_3'x_4' + x_1x_2x_3'x_4 + \\
& x_1x_2x_3x_4' + x_1x_2x_3x_4 + x_1x_2'x_4 + x_1x_3x_4' + x_1x_2x_3' + x_2x_3x_4 \\
\equiv {} & x_1x_2'x_4 + x_1x_3x_4' + x_1x_2x_3' + x_2x_3x_4 + x_1x_2'x_3 + x_1x_2x_4' + x_1x_3'x_4 + \\
& x_1x_2x_3 + x_1x_3x_4 + x_1x_2x_4 + x_1x_4 + x_1x_3 + x_1x_2 \\
\equiv {} & \underline{x_2x_3x_4 + x_1x_4 + x_1x_3 + x_1x_2}
\end{aligned}$$

Da keine Variable komplementiert vorkommt, kann kein Term überflüssig sein. Der Term ist also minimal.

25. $$\begin{aligned}
(\neg x \Rightarrow \neg y) \Rightarrow (y \Rightarrow x) & \equiv (x \vee \neg y) \Rightarrow (\neg y \vee x) \\
& \equiv \neg(x \vee \neg y) \vee (\neg y \vee x) \\
& \equiv (\neg x \wedge y) \vee (\neg y \vee x) \\
& \equiv (\neg x \vee \neg y \vee x) \wedge (y \vee \neg y \vee x) \\
& \equiv \quad 1 \quad \wedge \quad 1 \equiv 1
\end{aligned}$$

26. a) Sind p_1,p_2,p_3 die Aussageformen in M_1, so gilt etwa $(0,1,1) \in T(p_1^1) \cap T(p_2^1) \cap T(p_3^1)$.
Folglich ist M_1 konsistent.

b) $T(\neg(y \Rightarrow z)) = \{(0,1,0),(1,1,0)\}$. Beide Elemente sind nicht in $T(p_1^1) \cap T(p_2^1) \cap T(p_3^1)$. Es folgt, daß $M_1 \cup \{\neg(y \Rightarrow z)\}$ widersprüchlich ist.

c) $M_1 \cup \{y \Rightarrow z\}$ ist konsistent. Zum Beispiel ist $(0,1,1)$ wieder in $T(y \Rightarrow z) \cap T((p_1 \wedge p_2 \wedge p_3)^1)$.

27. Es stehe

x_1 für: Weißer Niederschlag fällt,

x_2 für: Natrium vorhanden,

x_3 für: Ammoniak vorhanden,

x_4 für: Eisen vorhanden.

Wir haben folgende Aussageformen:

$p_1 := x_1 \Rightarrow (x_2 \vee x_3)$, $p_2 := \neg x_2 \Rightarrow x_4$, $p_3 := (x_4 \wedge x_1) \Rightarrow \neg x_3$ und $p_4 := x_1$ (denn wir wissen, daß ein weißer Niederschlag fällt).

Wir bestimmen den Träger von $p_1 \wedge p_2 \wedge p_3 \wedge p_4$ (dabei verkürzt sich die Tafel, da $x_1 = 1$ sein muß):

x_1	x_2	x_3	x_4	$\neg x_1 \vee x_2 \vee x_3$	$x_2 \vee x_4$	$\neg x_4 \vee \neg x_1 \vee \neg x_3$	$p_1 \wedge p_2 \wedge p_3 \wedge p_4$
1	0	0	0	0	0	1	0
1	0	0	1	0	1	1	0
1	0	1	0	1	0	1	0
1	0	1	1	1	1	0	0
1	1	0	0	1	1	1	1
1	1	0	1	1	1	1	1
1	1	1	0	1	1	1	1
1	1	1	1	1	1	0	0

Mit Folgerung 4.8 ergibt sich

$$p_1 \wedge p_2 \wedge p_3 \wedge p_4 \equiv x_1 \wedge x_2 \wedge ((\neg x_3 \wedge \neg x_4) \vee (\neg x_3 \wedge x_4) \vee (x_3 \wedge \neg x_4))$$
$$\equiv x_1 \wedge x_2 \wedge \neg(x_3 \wedge x_4).$$

Auf jeden Fall ist also Natrium vorhanden, aber nicht gleichzeitig Ammoniak und Eisen.

28. Man findet z.B. für die zusammengesetzten Operationen $d(x,0,y)$ und $d(0,x,1)$ die Tafeln

x	y	d(x,0,y)
0	0	0
0	1	1
1	0	1
1	1	1

und

x	d(0,x,1)
0	1
1	0

Somit gilt für alle $x,y \in \{0,1\}$, daß $d(x,0,y) = x+y$ und $d(0,x,1) = x'$ ist. $\{+,'\}$ ist aber eine adäquate Menge von Operationen, demnach also auch $\{d,0,1\}$.

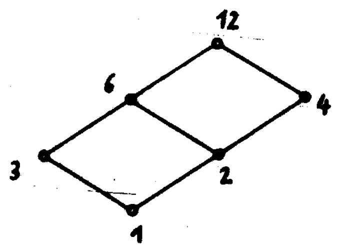
$\{d,0\}$ ist nicht adäquat, da z.B. für jede aus diesen zusammengesetzte Operation $f(x_1,\dots,x_n)$ gilt: $f(0,\dots,0) = 0$.

29. Ist R ein Boolescher Ring, dann ist $(R,+)$ eine abelsche Gruppe, auf der der Körper $GF(2)$ (bestehend aus den Elementen 0 und 1) operiert vermöge $0\cdot x = 0$ und $1\cdot x = x$. Die Vektorraumaxiome prüft man leicht nach. Ist R endlich, so hat R als Vektorraum endliche Dimension k, und folglich gilt: $|R| = 2^k$.

30. Für $a,b \in T_n$ gilt offenbar $\sup\{a,b\} = \text{kgV}(a,b)$ und $\inf\{a,b\} = \text{ggT}(a,b)$. Damit verifiziert man leicht, daß $(T_n;\ \text{kgV}, \text{ggT})$ ein distributiver Verband ist. Ist $p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot \ldots \cdot p_k^{\alpha_k}$ die Primzahlzerlegung von n, so gilt: T_n ist genau dann Boolesch, wenn n quadratfrei ist, wenn also $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 1$ ist.

<u>Beweis:</u> Ist n quadratfrei, so ist offenbar $\frac{n}{x}$ ein Komplement von x in T_n. Ist n nicht quadratfrei, also $n = p_i^2\cdot r$, so hat $p_i\cdot r$ kein Komplement in T_n; denn wäre x ein Komplement von $p_i r$, so müßte $p_i^2 | x$ gelten wegen $\text{kgV}(p_i r, x) = n$. Andererseits hätte dies aber $\text{ggT}(p_i r, x) \neq 1$ zur Folge.

<u>Beispiel:</u> $n = 12$, $T_n = \{1,2,3,4,6,12\}$



ist keine Boolesche Algebra, denn $2^2 = 4 | 12$.

31. Aus $x(y+z) = xy + xz$ folgt:

$$\begin{aligned}(x+y)(x+z) &= (x+y)x + (x+y)z = x(x+y) + z(x+y)\\ &= x + zx + zy\\ &= x + zy\\ &= x + yz.\end{aligned}$$

Die Umkehrung ist dual.

32. a) Sei $M = \{x_1,\ldots,x_n\}$ und $a := x_1 + x_2 + \ldots + x_n$.
Wir behaupten: $a = \sup M$.
Offensichtlich gilt $x_i \le a$ für alle i, also ist a eine obere Schranke.
Sei b eine beliebige obere Schranke von M. Wir erhalten $b \ge x_1,\ldots,b \ge x_n$, also $b \ge x_1 + \ldots + x_n = a$; somit ist a die kleinste obere Schranke.
Dual hat man $x_1 \cdot \ldots \cdot x_n = \inf M$.

b) Da der Verband endlich ist, ist 1 das Supremum und 0 das Infimum aller seiner Elemente. Beide existieren nach Teil a).

33. Sei $x \in V$ und $x \neq 0$. Wir suchen ein Atom $a \le x$. Ist x schon ein Atom, so sind wir fertig. Ansonsten gibt es ein Element x_1 mit $0 < x_1 < x$. (Wir schreiben $u<v$, falls $u \le v$ und $u \neq v$ ist.) Ist x_1 ein Atom, so sind wir fertig. Ansonsten gibt es ein x_2 mit $0 < x_2 < x_1 < x$. Ist x_2 kein Atom, so suchen wir uns ein x_3 ... usw. Dies kann nicht unendlich lange weitergehen, da V endlich ist. Also müssen wir irgendwann bei einem Atom x_n angelangt sein. Selbstverständlich ist $x_n \le x$.

34. Ist B eine endliche Boolesche Algebra, so gilt nach 9.8, daß $B \cong \mathbf{2}^n$ ist. Damit genügt es, die Atome von $\mathbf{2}^n$ zu zählen (Isomorphismen bilden Atome auf Atome ab). Die Atome von $\mathbf{2}^n$ sind aber genau die n-tupel $(\alpha_1,\alpha_2,\ldots,\alpha_n)$, für die genau ein $\alpha_i = 1$ und alle anderen $\alpha_j = 0$ sind. Es gibt genau n solche Tupel.

35. Dies folgt unmittelbar aus 9.8, denn beide sind isomorph zu $\mathbf{2}^n$ für dasselbe n.

36. a) (i) Sind $b_1, b_2 \in \phi^{-1}(\{0\})$, so gilt $\phi(b_1) = \phi(b_2) = 0$, also auch $\phi(b_1+b_2) = \phi(b_1) + \phi(b_2) = 0$ und $b_1+b_2 \in \phi^{-1}(\{0\})$.

(ii) Ist $b_1 \geq b_2$ und $b_1 \in \phi^{-1}(\{0\})$, so folgt $\phi(b_2) = \phi(b_1 \cdot b_2) = \phi(b_1) \cdot \phi(b_2) = 0 \cdot \phi(b_2) = 0$ und somit auch $b_2 \in \phi^{-1}(\{0\})$.

(iii) Wegen $\phi(1) = 1$ ist $1 \notin \phi^{-1}(\{0\})$.

Mit (i) - (iii) ist $\phi^{-1}(\{0\})$ als Ideal nachgewiesen. Dual zeigt man, daß $\phi^{-1}(\{1\})$ ein Filter ist.

b) Die Relation Θ auf B definieren wir durch die Festsetzung: für $x, y \in B$ sei genau dann $x\Theta y$, wenn $(x'+y)(x+y') \in F$ ist. Wir behaupten, daß Θ eine Kongruenzrelation mit $F = [1]\Theta$ ist.

1. Θ ist eine Äquivalenzrelation:

Reflexivität und Symmetrie sind sofort klar.

Sei nun $x\Theta y$ und $y\Theta z$, also $(x'+y)(x+y') \in F$ und $(y'+z)(y+z') \in F$. Es folgt $(x'+y)(x+y')(y'+z)(y+z') \in F$. Wegen $(x'+y)(x+y')(y'+z)(y+z') = xyz + x'y'z'$ und $xz + x'z' \geq xyz + x'y'z'$ hat man $xz + x'z' = (x'+z)(x+z') \in F$ und $x\Theta z$. Damit ist auch die Transitivität gezeigt.

2. Θ ist eine Kongruenzrelation:

Sei $x\Theta y$, also $(x'+y)(x+y') \in F$.

Wegen $(x'+y)(x+y') = (x''+y')(x'+y'') \in F$ hat man $x'\Theta y'$.

Seien $x\Theta y$ und $u\Theta v$, d.h. $(x'+y)(x+y') \in F$ und $(u'+v)(u+v') \in F$, also

$$a := (x'+y)(x+y')(u'+v)(u+v') = (xy+x'y')(uv+u'v') =$$
$$xyuv + xyu'v' + x'y'uv + x'y'u'v' \in F.$$

Andererseits hat man

$$b := ((x+u)' + (y+v))((x+u) + (y+v)')$$
$$= (x'u'+y+v)(x+u+y'v')$$
$$= x'y'u'v' + xy + yu + xv + uv \geq a,$$

also $b \in F$, was gerade $x+u \,\Theta\, y+v$ bedeutet.

Entsprechend hat man

$$c := ((x \cdot u)' + y \cdot v) \cdot (x \cdot u + (y \cdot v)')$$
$$= (x'+u' + yv)(x \cdot u + y'+v')$$
$$= x'y' + x'v' + y'u' + u'v' + xuyv \geq a,$$

also $c \in F$; und das bedeutet $x \cdot u \,\Theta\, y \cdot v$.

Θ ist also eine Kongruenzrelation.

3. $[1]\Theta = F$: Dies ergibt sich daraus, daß $x \in [1]\Theta$ bzw. $x\Theta 1$ gleichbedeutend ist mit $(x'+1) \cdot (x+1') \in F$, also mit $x \in F$.

37. Weil die ϕ Homomorphismen sind, gilt offenbar $T_{(b,0)} = T_{(b',1)}$ für beliebiges $b \in B$.
Also kann man für $i,j \in \mathbb{Z}$ immer $\overline{b}_1, \overline{b}_2$ finden mit

$$T_{(b_1,i)} \cap T_{(b_2,j)} = T_{(\overline{b}_1,1)} \cap T_{(\overline{b}_2,1)}.$$

Wir behaupten:

$$\underline{T_{(\overline{b}_1,1)} \cap T_{(\overline{b}_2,1)} = T_{(\overline{b}_1 \cdot \overline{b}_2,1)}} \ .$$

Ist nämlich $\phi \in T_{(\overline{b}_1,1)} \cap T_{(\overline{b}_2,1)}$, so gilt $\phi(\overline{b}_1) = 1$ und $\phi(\overline{b}_2) = 1$, also $\phi(\overline{b}_1 \cdot \overline{b}_2) = 1$, mithin $\phi \in T_{(\overline{b}_1 \cdot \overline{b}_2,1)}$.
Umgekehrt, wenn $\phi \in T_{(\overline{b}_1 \cdot \overline{b}_2,1)}$ ist, so folgt
$1 = \phi(\overline{b}_1 \cdot \overline{b}_2) = \phi(\overline{b}_1) \cdot \phi(\overline{b}_2)$. Deswegen muß gelten $\phi(\overline{b}_1) = 1$ und $\phi(\overline{b}_2) = 1$, also $\phi \in T_{(\overline{b}_1,1)} \cap T_{(\overline{b}_2,1)}$.

38. Wir nehmen an, es sei $b_1^{\alpha_1} \cdot \ldots b_n^{\alpha_n} > 0$, und dieses Element sei auch kein Atom. Dann gibt es ein $x \in B$ mit $0 < x < b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}$.
Nach Folgerung 11.2 gibt es eine Teilmenge $S \subseteq \mathbb{Z}^n$ mit

$$x = \sum_{(\gamma_1,\ldots,\gamma_n) \in S} b_1^{\gamma_1} \cdot \ldots \cdot b_n^{\gamma_n}.$$

Offenbar gilt $(\alpha_1,\ldots,\alpha_n) \notin S$, denn sonst müßte $b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n} \leq x$ sein. Man erhält nun

$$\begin{aligned} x &= x \cdot (b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}) \\ &= \sum_{(\gamma_1,\ldots,\gamma_n) \in S} (b_1^{\gamma_1} \cdot \ldots \cdot b_n^{\gamma_n}) \cdot (b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}) \\ &= 0 \end{aligned}$$

und dies ist ein Widerspruch.

39. Nach 11.4 und den anschließenden Bemerkungen ist $\mathbb{P}(\{1,2,3,4\})$ isomorph zu $\mathbb{Z}^{\mathbb{Z}^2}$ und frei.
Für $B_1 := \{1,2\}$ und $B_2 := \{2,3\}$ gilt $B_1 \cap B_2 = \{2\}$, $\overline{B}_1 \cap B_2 = \{3\}$, $B_1 \cap \overline{B}_2 = \{1\}$, $\overline{B}_1 \cap \overline{B}_2 = \{4\}$. Mit 11.5 kann daraus geschlossen werden, daß $\{B_1, B_2\}$ ein freies Erzeugendensystem von $\mathbb{P}(\{1,2,3,4\})$ ist.
(Es gibt zwölf verschiedene solche Erzeugendensysteme.)

LITERATUR

(Die mit * gekennzeichnete Literatur ist als mathematisch weiterführend zu verstehen.)

*G. Birkhoff: Lattice theory. Providence: AMS Coll. Publ., 3rd ed., 1967.

U. Bong: Boolesche Algebra. Freiburg: Herder 1977.

G. Boole: An investigation of the laws of thought. Dover Publ. (Nachdruck der Erstausgabe von 1854).

G. Braunss - H.J. Zubrod: Einführung in die Booleschen Algebren. Frankfurt: Akad. Verlagsges. 1974.

*P. Dwinger: Introduction to Boolean algebras. Würzburg: Physica-Verlag, 1961.

*G. Grätzer: Lattice theory. San Francisco: Freeman 1971.

*P.R. Halmos: Lectures on Boolean algebras. Princeton: Van Nostrand 1967.

E. Mendelson: Boolean algebras and switching circuits. Schaum's Outline Series, 1970.

*R. Sikorski: Boolean algebras. Berlin: Springer 1969.

G.F. South: Boolean algebra and its uses. London: Van Nostrand 1974.

J.E. Whitesitt: Boolesche Algebra und ihre Anwendungen. Braunschweig: Vieweg 1964.

SACHVERZEICHNIS

VERWENDETE SYMBOLE

(In dieser Aufstellung bezeichne X eine Menge, B eine Boolesche Algebra, T einen topologischen Raum, Θ eine Kongruenzrelation auf B, ϕ eine Abbildung, f eine Schaltfunktion, p einen Term, a ein Element aus B, $\alpha_i \in \{0,1\}$.)

A. Boolesche Algebren

B. Andere Strukturen

C. Spezialle Relationen und Teilmengen

D. Spezielle Abbildungen

E. Verknüpfungen

Heinz-Peter Gumm

Geboren am 16. Oktober 1951 in Ohlweiler auf dem Hunsrück. Studierte Mathematik und Physik an der Technischen Hochschule Darmstadt. 1975 Dipl.-Mathematiker, anschließend Auslandsstudium in Winnipeg, Kanada. 1977 Promotion zum Dr. rer. nat. in Darmstadt. Von 1977 bis 1980 Wissenschaftlicher Mitarbeiter am Fachbereich Mathematik der Technischen Hochschule Darmstadt. Frühjahr 1980 Gastforscher in Thunder Bay, Kanada. 1980/81 Gastprofessor an der University of Hawaii in Honolulu, Hawaii.

Werner Poguntke

Geboren 16. September 1949 in Homberg am Niederrhein. Nach dem Abitur 1968 Studium der Mathematik und Physik in Bonn und Darmstadt, 1972 Dipl.-Mathematiker, 1974 Promotion zum Dr. rer. nat. in Darmstadt. Von 1974 bis 1980 Wissenschaftlicher Mitarbeiter, seit 1980 Hochschulassistent im Fachbereich Mathematik der Technischen Hochschule Darmstadt. 1978/79 als Gastforscher an den Universitäten in Hamilton und Thunder Bay, Kanada. 1981 Habilitation und Privatdozent in Darmstadt.

Dieses Buch stellt eine Einführung in Theorie und Anwendung Boolescher Algebren dar. Es richtet sich an Studierende der Mathematik, der Informatik, der Natur- und Ingenieurwissenschaften.

ISBN 3-411-00604-8