Bemerkung:

Der folgende Abschnitt

„Boolesche Algebren“

ist (im WS 2010/11) nicht Teil des Prüfungsstoffs, soweit nicht Teile daraus in der Übung behandelt werden!

6. Boolesche Algebren

6.1 Definitionen

Eine Boolesche Algebra ist eine Algebra

$$\langle S, \oplus, \otimes, \sim, 0, 1 \rangle,$$

$\oplus, \otimes$ sind binäre, $\sim$ ist ein unärer Operator, 0 und 1 sind Konstanten. Es gilt:

1. $\oplus$ und $\otimes$ sind assoziativ und kommutativ.
2. 0 ist Einselement für $\oplus$, 1 ist Einselement für $\otimes$.
3. für $\sim$ gilt:
$$\begin{aligned} b \oplus \sim b &= 1 \\ b \otimes \sim b &= 0 \quad \forall b \in S. \end{aligned}$$
4. Distributivgesetz:
$$\begin{aligned} b \otimes (c \oplus d) &= (b \otimes c) \oplus (b \otimes d) \\ b \oplus (c \otimes d) &= (b \oplus c) \otimes (b \oplus d) \end{aligned}$$

Bemerkung:
Eine boolesche Algebra ist keine Gruppe, weder bezüglich $\oplus$ ($b \oplus \sim b = 1$) noch bezüglich $\otimes$.

Beispiel 108

- $\langle \mathbb{B}, \vee, \wedge, \neg, F, T \rangle$
- $\langle 2^U, \cup, \cap, ^-, \emptyset, U \rangle$
- $\langle \{1,2,3,6\}, \mathrm{kgV}, \mathrm{ggT}, x \mapsto \frac{6}{x}, 1, 6 \rangle$

George Boole (1815–1864)

George Boole

lived from 1815 to 1864

Boole approached logic in a new way reducing it to a simple algebra, incorporating logic into mathematics. He also worked on differential equations, the calculus of finite differences and general methods in probability.

Satz 109 (Eigenschaften Boolescher Algebren)

1. *Idempotenz:*

$$(\forall b \in S)\Big[b \oplus b = b \quad \wedge \quad b \otimes b = b\Big]$$

2. *Nullelement:*

$$(\forall b \in S)\Big[b \oplus 1 = 1 \quad \wedge \quad b \otimes 0 = 0\Big]$$

3. *Absorption:*

$$(\forall b, c \in S)\Big[b \oplus (b \otimes c) = b \quad \wedge \quad b \otimes (b \oplus c) = b\Big]$$

4. *Kürzungsregel:*

$$(\forall b, c, d \in S)\left[\begin{array}{l}(b \oplus c = b \oplus d) \wedge (\sim b \oplus c = \sim b \oplus d) \Leftrightarrow c = d \\ (b \otimes c = b \otimes d) \wedge (\sim b \otimes c = \sim b \otimes d) \Leftrightarrow c = d\end{array}\right]$$

Satz 109 (Forts.)

5. *eindeutiges Komplement:*

$$(\forall b, c \in S)\left[b \oplus c = 1 \ \wedge \ b \otimes c = 0 \iff c \ = \sim b\right]$$

6. *Involution:*

$$(\forall b \in S)\left[\sim (\sim b) = b\right]$$

7. *Konstanten:*

$$\sim 0 = 1 \qquad \sim 1 = 0$$

8. *De-Morgan-Regeln:*

$$(\forall b, c, d \in S)\begin{bmatrix} \sim (b \oplus c) = \sim b \otimes \sim c \\ \sim (b \otimes c) = \sim b \oplus \sim c \end{bmatrix}$$

Augustus de Morgan (1806–1871)

Wir zeigen zunächst die Teilbehauptung 7:

$$\sim 0 = 1 \qquad \sim 1 = 0$$

Beweis:
Mit $b = 0$ folgt aus den Eigenschaften 2 und 3 Boolescher Algebren sofort

$$\sim 0 = 1 \, ,$$

und ebenso mit $b = 1$

$$\sim 1 = 0 \, ,$$

womit wir Behauptung 7 gezeigt haben. □

Folgende Hilfsbehauptung ist sehr nützlich:

$$1 = 1 \oplus (0 \otimes 1) = (1 \oplus 0) \otimes (1 \oplus 1) = 1 \otimes (1 \oplus 1) = 1 \oplus 1 \; .$$

Beweis:

[Es werden nur Teile des Satzes bewiesen.]

1. $$b \oplus b = (1 \otimes b) \oplus (1 \otimes b) = (1 \oplus 1) \otimes b = 1 \otimes b = b$$

2. $$b \oplus 1 = b \oplus \big(b \oplus (\sim b)\big) = (b \oplus b) \oplus (\sim b) = b \oplus (\sim b) = 1$$

3. $$b \oplus (b \otimes c) = (b \otimes 1) \oplus (b \otimes c) = b \otimes (1 \oplus c) = b \otimes 1 = b$$

□

Beobachtung:
Die Eigenschaften treten in Paaren auf, die durch Vertauschen von $\oplus$ und $\otimes$ und von 0 und 1 ineinander übergehen. Solche Eigenschaften heißen dual zueinander.

Da die Axiome unter Dualität abgeschlossen sind, folgt:

Das Duale eines Satzes ist wieder ein Satz.

Definition 110

Sei $A = \langle S, \oplus, \otimes, \sim, 0, 1 \rangle$ eine endliche Boolesche Algebra. Dann definiert man:

$$a \leq b \iff a \otimes b = a$$
$$a < b \iff a \leq b \ \wedge \ a \neq b$$

Satz 111

Durch $\leq$ ist auf A eine partielle Ordnung definiert, d. h. eine reflexive, antisymmetrische und transitive Relation.

Beweis:

(a) Reflexivität: Zu zeigen ist, dass für alle $a \in S$ gilt $a \leq a$, d. h. $a \otimes a = a$ (Idempotenzgesetz bzgl. $\otimes$)

(b) Antisymmetrie: Sei $a \leq b \ \wedge \ b \leq a$. Damit gilt: $a \otimes b = a$ und $b \otimes a = b$ nach Definition. Damit:

$$a = a \otimes b = b \otimes a = b$$

(c) Transitivität: Sei $a \leq b \ \wedge \ b \leq c$, dann gilt: $a \otimes b = a$ und $b \otimes c = b$. Es ist zu zeigen, dass $a \leq c$, d.h. $a \otimes c = a$.

$$a \otimes c = (a \otimes b) \otimes c = a \otimes (b \otimes c) = a \otimes b = a$$

□

6.2 Atome

Definition 112

Ein Element $a \in S$, $a \neq 0$ heißt ein Atom, i. Z. $\mathrm{atom}(a)$, falls

$$(\forall b \in S \setminus \{0\}) \Big[b \leq a \;\Rightarrow\; b = a \Big].$$

Satz 113

Es gilt:

1. $\mathrm{atom}(a) \;\Rightarrow\; (\forall b \in S) \quad [a \otimes b = a \;\vee\; a \otimes b = 0]$
2. $\mathrm{atom}(a) \wedge \mathrm{atom}(b) \wedge a \neq b \;\Rightarrow\; a \otimes b = 0$
3. *Falls gilt:* $(\forall a \in S)[\mathrm{atom}(a) \;\Rightarrow\; a \otimes b = 0]$, *dann* $b = 0$.

Beweis:

[Wir zeigen nur die erste Teilbehauptung]

1. Sei a ein Atom. Nach Voraussetzung gilt (mit $a \otimes b$ statt b):

$$a \otimes b \neq 0 \quad \Longrightarrow \quad \big(a \otimes b \leq a \;\Rightarrow\; a \otimes b = a\big)$$

Da aber $a \otimes b \leq a$ ist (Übungsaufgabe!), folgt

$$(a \otimes b = 0) \vee (a \otimes b = a).$$

□

Satz 114 (Darstellungssatz)

Jedes Element x einer endlichen Booleschen Algebra $\langle S, \oplus, \otimes, \sim, 0, 1\rangle$ lässt sich in eindeutiger Weise als $\oplus$-Summe von Atomen schreiben:

$$x = \bigoplus_{\substack{a \in S \\ \mathrm{atom}(a) \\ a \otimes x \neq 0}} a$$

Beweis:

Es gilt:

$$x \otimes \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a \overset{\text{D–G.}}{=} \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} (x \otimes a) \overset{\text{Satz113}}{=} \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a$$

Setze

$$y := \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a \,.$$

Beweis (Forts.):

Wir haben gezeigt:

$$x \otimes y = y$$

Ebenso gilt:

$$x \otimes (\sim y) = 0 \quad \text{(Übungsaufgabe!)}$$

Zusammen:

$$\begin{aligned} x &= x \otimes \big(y \oplus (\sim y)\big) \\ &\overset{\text{D-G.}}{=} \big(x \otimes y\big) \oplus \big(x \otimes (\sim y)\big) \\ &= y \oplus 0 = y \end{aligned}$$

Beweis (Forts.):

Zur Eindeutigkeit: Sei (Widerspruchsannahme)

$$0 \neq x = \bigoplus_{a \in S_1} a = \bigoplus_{a \in S_2} a,$$

wobei $S_1, S_2 \subseteq S$, $S_1 \neq S_2$ zwei verschiedene Teilmengen von Atomen aus S sind.
O. B. d. A. gelte $S_1 \cap S_2 = \emptyset$ — wenn nicht, dann bilde die Schnittmenge mit $\left(\overline{S_1 \cap S_2}\right)$.

Beweis (Forts.):

Dann gilt:

$$
\begin{aligned}
x \quad &= \quad x \otimes x = \Big(\bigoplus_{a \in S_1} a\Big) \otimes \Big(\bigoplus_{a \in S_2} a\Big) \\
&= \bigoplus_{\substack{a \in S_1 \\ a' \in S_2}} \underbrace{a \otimes a'}_{=0} \\
&\overset{\text{Satz113(2)}}{=} \bigoplus_{\substack{a \in S_1 \\ a' \in S_2}} 0 = 0,
\end{aligned}
$$

was ein Widerspruch zur Annahme ist. □

Korollar 115

Jede endliche Boolesche Algebra mit n Atomen enthält genau 2^n Elemente.

Korollar 116

Jede endliche Boolesche Algebra $A = \langle S, \oplus, \otimes, \sim, 0, 1\rangle$ mit n Atomen ist isomorph zur Potenzmengenalgebra

$$\mathcal{P}_n := \langle 2^{\{1,\ldots,n\}}, \cap, \cup, ^-, \emptyset, \{1,\ldots,n\}\rangle$$

Beweis:

Seien $a_1, \ldots, a_n$ die Atome von A. Definiere die Abbildung

$$h : S \ni \bigoplus_{i\in I} a_i \mapsto I \in 2^{\{1,\ldots,n\}}$$

Diese Abbildung ist ein Isomorphismus (leicht nachzurechnen). □

Kapitel III Ringe und Körper

1. Definitionen und Beispiele

Definition 117

Eine Algebra $A = \langle S, \oplus, \odot, 0, 1\rangle$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heißt ein Ring, falls

R1. $\langle S, \oplus, 0\rangle$ eine abelsche Gruppe mit neutralem Element $0 \in S$ ist,

R2. $\langle S, \odot, 1\rangle$ ein Monoid mit neutralem Element $1 \in S$ ist und

R3. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ für alle $a, b, c \in S$,
$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$ für alle $a, b, c \in S$,
(man sagt: $\oplus$ und $\odot$ sind distributiv).

Definition 118

Eine Algebra $A = \langle S, \oplus, \odot, 0, 1\rangle$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heißt Körper (engl. field), falls

K1. $\langle S, \oplus, 0\rangle$ eine abelsche Gruppe mit neutralem Element $0 \in S$ ist,

K2. $\langle S \setminus \{0\}, \odot, 1\rangle$ eine abelsche Gruppe mit neutralem Element $1 \in S$ ist und

K3. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ für alle $a, b, c \in S$.

Beispiele 119

- Die Algebra der ganzen Zahlen $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ ist ein kommutativer Ring.
- Für $n \in \mathbb{N}$, $n > 1$, ist die Algebra der Restklassen bzgl. Division durch n, also $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$ ein kommutativer Ring.
- Die Menge der $n \times n$-Matrizen ($n \geq 1$) mit Einträgen aus $\mathbb{Z}$ ist ein im Allgemeinen nicht kommutativer Ring.

Beispiele 120

- $\mathbb{Q}$ (die Menge der rationalen Zahlen) ist ein Körper.
- Ebenso $\mathbb{R}$ und $\mathbb{C}$.
- Die Restklassenalgebra $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$ ist für alle n, die prim sind, ein Körper.

2. Eigenschaften von Körpern

Satz 121

In jedem Körper K gilt:

$$a \cdot 0 = 0 \cdot a = 0 \qquad \textit{für alle } a \in K\,.$$

Beweis:

Es sei a ein beliebiges Element aus K. Dann folgt aus den Axiomen:

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + a \cdot 0 - a \cdot 0 = a \cdot (0+0) - a \cdot 0 \\ &= a \cdot 0 - a \cdot 0 = 0\,. \end{aligned}$$

□

Bemerkung: Satz 121 gilt sogar in Ringen.

Definition 122

Sei R kommutativ. Ein $a \in R$, $a \neq 0$, heißt Nullteiler, falls es ein $b \in R$ gibt, $b \neq 0$, so dass $ab = 0$.

Satz 123

In jedem Körper K gilt für alle $a, b \in K$:

$$ab = 0 \quad \Longrightarrow \quad a = 0 \quad \textit{oder} \quad b = 0\,.$$

(Man sagt: Körper sind nullteilerfrei.)

Beweis:

Angenommen $ab = 0$. Falls $a \neq 0$, so existiert ein multiplikatives Inverses a^{-1} von a. Unter Verwendung von Satz 121 folgt damit:

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0\,.$$

□

2.1 Größter gemeinsamer Teiler (ggT)

Definition 124

- Seien $a, b \in \mathbb{N}$. Dann heißt $d \in \mathbb{N}$ der größte gemeinsame Teiler ($\mathrm{ggT}(a, b)$), falls gilt:
  1. $d|a$ und $d|b$;
  2. falls $d' \in \mathbb{N}$, $d'|a$ und $d'|b$, dann gilt $d'|d$.
- Sind $a_1, \ldots, a_n \in \mathbb{N}$, $n \geq 3$, dann definieren wir

$$\mathrm{ggT}(a_1, \ldots, a_n) := \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n)\,.$$

Satz 125

Seien $a, b \in \mathbb{N}$. Dann gibt es $c, d \in \mathbb{Z}$, so dass

$$c \cdot a + d \cdot b = \mathrm{ggT}(a, b)\,.$$

Beweis:

Sei o.B.d.A. $a > b$. Der Euklidische Algorithmus (fortgesetzte ganzzahlige Division mit Rest) (Euklid von Alexandria, ca. 325–265 v. Chr.) liefert eine Folge

$$
\begin{aligned}
r_0 := a &= q_2 \cdot b + r_2 && \text{, mit } 0 < r_2 < b, q_2, r_2 \in \mathbb{N}_0 \\
r_1 := b &= q_3 \cdot r_2 + r_3 && \text{, mit } 0 < r_3 < r_2, q_3, r_3 \in \mathbb{N}_0 \\
r_2 &= q_4 \cdot r_3 + r_4 && \text{, mit } 0 < r_4 < r_3, q_4, r_4 \in \mathbb{N}_0 \\
&\vdots \\
r_{m-3} &= q_{m-1} \cdot r_{m-2} + r_{m-1} && \text{, mit } 0 < r_{m-1} < r_{m-2} \qquad (*) \\
r_{m-2} &= q_m \cdot r_{m-1} + r_m && \text{, mit } 0 = r_m < r_{m-1}
\end{aligned}
$$

Dann gilt $r_{m-1} | a$ und $r_{m-1} | b$ sowie $\mathrm{ggT}(a,b) | r_{m-1}$.
Also $r_{m-1} = \mathrm{ggT}(a,b)$.
Rückwärtiges iteratives Ersetzen von $r_{m-2}, r_{m-3}, \ldots$ in Gleichung (*) entsprechend den vorhergehenden Gleichungen liefert die gewünschte Darstellung. $\square$

Satz 126

Bezeichnet man mit $+_n$ und $\cdot_n$ die Addition bzw. Multiplikation modulo n, so gilt:

$$\langle \mathbb{Z}_n, +_n, \cdot_n \rangle \text{ ist ein Körper} \quad \Longleftrightarrow \quad n \text{ ist Primzahl .}$$

Beweis:

Die Axiome K1 und K3 sind durch die Addition und Multiplikation modulo n offensichtlich erfüllt. Wir haben bereits gesehen, dass a modulo n genau dann ein multiplikatives Inverses hat, wenn a und n teilerfremd sind, also

$$\mathrm{ggT}(a, n) = 1 \; .$$

Falls n prim ist, gilt dies für alle a, $1 \leq a < n$.
Umgekehrt kann $\mathrm{ggT}(a, n) = 1$ für alle a, $1 \leq a < n$ nur gelten, falls n prim ist. □

2.2 Multiplikative Gruppe endlicher Körper

Satz 127

In jedem endlichen Körper K ist die multiplikative Gruppe $K^* = K \setminus \{0\}$ zyklisch, d.h. es gibt ein Element $g \in K^*$ mit $K^* = \{1, g, g^2, \ldots, g^{|K|-2}\}$.

Beweis:

Es gilt: $\mathrm{ord}(a) < \infty$ für alle $a \in K^*$. Sei a ein Element in K^* mit maximaler Ordnung:

$$\max\{\mathrm{ord}(b) \mid b \in K^*\} = \mathrm{ord}(a) \ .$$

Es ist zu zeigen, dass $\mathrm{ord}(a) = |K| - 1$. Dazu betrachten wir das Polynom $x^{\mathrm{ord}(a)} - 1$, das Grad $\mathrm{ord}(a)$ hat.
Für jedes $b \in K^*$ gilt, dass $\mathrm{ord}(b) \mid \mathrm{ord}(a)$ (da sonst ab größere Ordnung als a hätte). Also ist jedes Element von K^* eine Nullstelle des obigen Polynoms. Da ein Polynom vom Grad k höchstens k verschiedene Nullstellen haben kann (warum? Siehe dazu später Satz 139), folgt daraus $\mathrm{ord}(a) \geq |K^*| = |K| - 1$. □

2.3 Primitive Elemente

Definition 128

Sei K ein endlicher Körper. Ein Element a, das die multiplikative Gruppe $K^* = K \setminus \{0\}$ erzeugt, nennt man primitives Element.

Beispiel 129

In $\mathbb{Z}_5^*$ sind sowohl 2 als auch 3 primitive Elemente:

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 3 \\ (2^4 &= 1 \end{aligned} \qquad \begin{aligned} 3^0 &= 1 \\ 3^1 &= 3 \\ 3^2 &= 4 \\ 3^3 &= 2 \\ 3^4 &= 1) \end{aligned}$$

Bemerkung: $\langle \mathbb{Z}_4, +_4, \cdot_4, 0, 1 \rangle$ ist kein Körper!

Beispiel 130

Setzt man $K = \{0, 1, a, b\}$ und definiert eine Addition und Multiplikation wie folgt:

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

so bildet $\langle K, \oplus, \odot, 0, 1 \rangle$ einen Körper (Übung!).