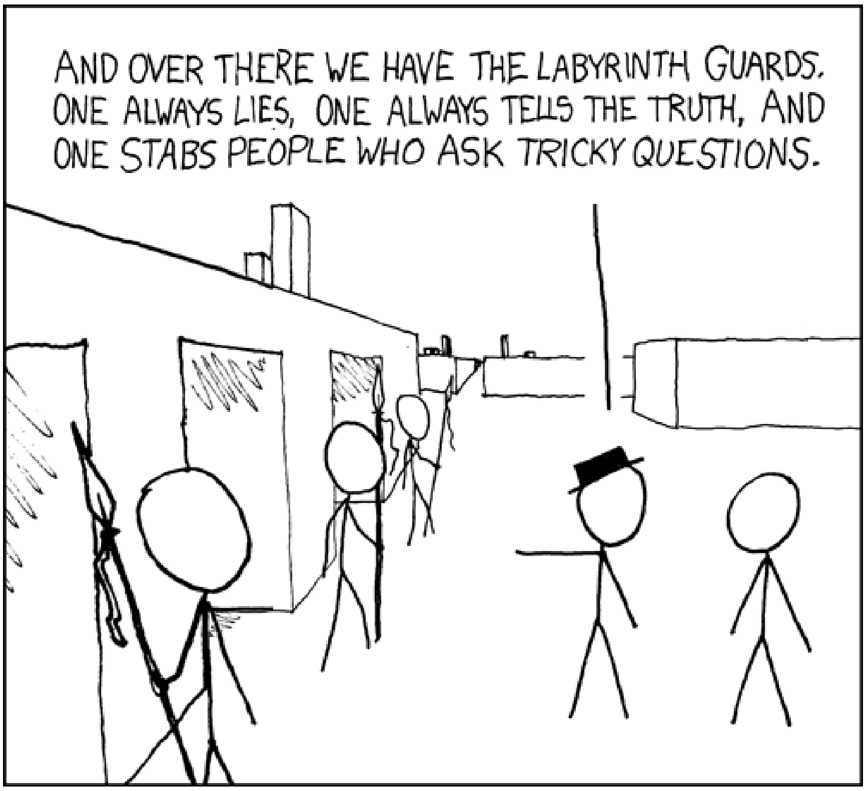
Mathematische Logik I

apl. Prof. Dr. rer. nat. habil. Dietlinde Lau

2007-08-01



And the whole setup is just a trap to capture escaping logicians. None of the doors actually lead out.
(http://xkcd.com/246/)

Inhalt

1 Boolesche Algebra

1.1 Definitionen, Beispiele, elementare Eigenschaften

Def.:

$$\underline{B} = (B; \vee, \wedge, {}^{-}, 0, 1)$$

Algebra des Typs $(2, 2, 1, 0, 0)$[1] heißt *Boolesche Algebra* $:\Leftrightarrow$

(B_1) $(B; \vee, \wedge)$ ist distributiver Verband, d. h. $\vee, \wedge$ sind kommutative, assoziative, distributive Operationen und es gilt:
$\forall x, y \in B$:
$x \vee x = x \wedge x = x$ („Idempotenz")
$x \vee (x \wedge y) = x$
$x \wedge (x \vee y) = x$ („Absorption")
(B_2) $\forall x \in B: x \wedge 0 = 0,\ x \vee 1 = 1$
(B_3) $\forall x \in B: x \wedge \bar{x} = 0,\ x \vee \bar{x} = 1$

Beispiele:

1) $B = \{0,1\}$

x	y	$x \vee y$	$x \wedge y$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

x	$\bar{x}$
0	1
1	0

2) X Menge mit $|X| \geq 1$

$$(\mathfrak{P}(X); \cup, \cap, {}^{-}, \emptyset, X)$$

$|\mathfrak{P}(X)| = 2^{|X|}$, falls X endliche Menge

3) $B \coloneqq \{(x_1, x_2, \dots, x_n) \mid \forall i \in \{1, \dots, n\}: x_i \in \{0,1\}\} = \{0,1\}^n,\ |B| = 2^n$

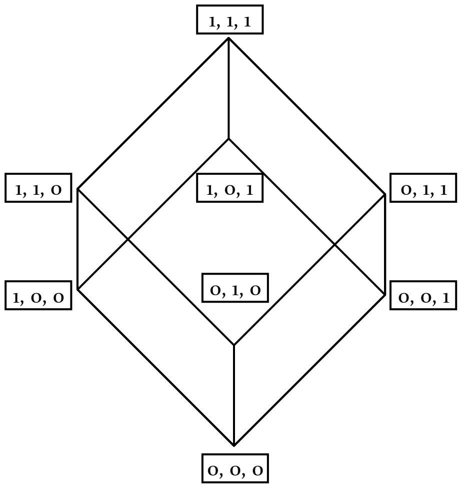
$$\forall \circ \in \{\vee, \wedge\}: (x_1, x_2, \dots, x_n) \circ (y_1, y_2, \dots, y_n) \coloneqq (x_1 \circ y_1, x_2 \circ y_2, \dots, x_n \circ y_n)$$

$$\overline{(x_1, x_2, \dots, x_n)} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$$

$$0 \coloneqq (0, 0, \dots, 0), \qquad 1 \coloneqq (1, 1, \dots, 1)$$

$$(x_1, x_2, \dots, x_n) \leq (y_1, y_2, \dots, y_n) :\Leftrightarrow \forall i: x_i \leq y_i,\ \text{wobei } 0 < 1$$

[1] Arität der Operatoren



4) Boolesche Algebren, die von obigen Beispielen verschieden sind, sind echte Unteralgebren von

$$(\mathfrak{P}(X); \cup, \cap, ^{-}, \emptyset, X),$$

falls X unendliche Menge.
(Sogenannte *Felder von Teilmengen von X*)
z. B.:

- $B := \{A \in \mathfrak{P}(X) \mid A \text{ endlich oder } \bar{A} \text{ endlich}\}$
  offenbar $\emptyset, X \in B$ und B ist bezüglich $\cap, \cup, ^{-}$ abgeschlossen, d. h., $(B; \cup, \cap, ^{-}, \emptyset, X)$ ist Unteralgebra von $(\mathfrak{P}(X); \cup, \cap, ^{-}, \emptyset, X)$ und ebenfalls Boolesche Algebra.

Satz 1

Sei $\underline{B}$ eine Boolesche Algebra und $\forall x, y \in B$:

(a) $x \vee 0 = x,\ \ x \wedge 1 = x$
(b) $\big((x \wedge y = 0) \wedge (x \vee y = 1)\big) \Rightarrow \bar{x} = y$
(c) $\bar{0} = 1,\ \ \bar{1} = 0$
(d) $\bar{\bar{x}} = x$
(e) $\overline{x \vee y} = \bar{x} \vee \bar{y},\ \ \overline{(x \vee y)} = \bar{x} \wedge \bar{y}$

Zur Erinnerung: In Verbänden gilt:

$$a \leq b :\Leftrightarrow a \vee b = b$$
$$(:\Leftrightarrow a \wedge b = a)$$

$\leq$ ist reflexive, teilweise Ordnung

(f) $x \leq y \Leftrightarrow \bar{y} \leq \bar{x}$
(g) $x \leq y \Leftrightarrow \bar{x} \vee y = 1$

Beweis

(a) $x \vee 0 \underset{(B_2)}{=} x \vee (x \wedge 0) \underset{\text{Abs.}}{=} x$
$x \wedge 1 \underset{(B_2)}{=} x \wedge (x \vee 1) \underset{\text{Abs.}}{=} x$
(b) Seien $x \wedge y = 0$ und $x \vee y = 1$
Zu zeigen: $\bar{x} = y$. Dies ist bewiesen, wenn man $\bar{x} \leq y$ und $y \leq \bar{x}$ gezeigt hat.
Es gilt:

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

und

$$\bar{x} \wedge y \underset{(a)}{=} (\bar{x} \wedge y) \vee 0 \underset{\text{Vor.}}{=} (\bar{x} \wedge y) \vee (x \wedge y)$$

$$\underset{\text{Distrib.}}{=} \underbrace{(\bar{x} \vee x)}_{(B_3)} \wedge y \underset{(a)}{=} y$$

$$\Rightarrow y \leq \bar{x}$$

$$\bar{x} \underset{(a)}{=} 1 \wedge \bar{x} \underset{\text{Vor.}}{=} (x \vee y) \wedge \bar{x} \underset{\text{Distrib.}}{=} \underbrace{(x \wedge \bar{x})}_{0\ (B_3)} \vee (y \wedge \bar{x})$$

$$\underset{(a)}{=} y \wedge \bar{x}$$

$$\Rightarrow \bar{x} \leq y$$

Also: $\bar{x} = y$

(c) Wählt man in (b) $x = 0$ und $y = 1$, so steht dort

$$\underbrace{0 \wedge 1 = 0 \text{ und } 0 \vee 1 = 1}_{\text{Offenbar nach Axiomen einer Booleschen Algebra erfüllt}}$$

$$\underset{(b)}{\Rightarrow} \bar{0} = 1$$

Analog zeigt man $\bar{1} = 0$ $(x \leftrightarrow y)$

(d) $\bar{\bar{x}} = x$ folgt aus (b), indem man x durch $\bar{x}$ und y durch x ersetzt und (B_3) benutzt.

(e) Beweisen nur $\overline{x \vee y} = \bar{x} \wedge \bar{y}$

(Der Beweis für $\overline{x \wedge y} = \bar{x} \vee \bar{y}$ verläuft analog)

Zeigen, dass Voraussetzung von (b) erfüllt ist (Dabei $x \to x \vee y$, $y \to \bar{x} \wedge \bar{y}$), d. h. wir zeigen:

$$(x \vee y) \wedge (\bar{x} \wedge \bar{y}) = 0 \qquad (*)$$

$$(x \vee y) \wedge (\bar{x} \wedge \bar{y}) = 1 \qquad (**)$$

Es gilt:

$$(x \vee y) \wedge (\bar{x} \wedge \bar{y}) \underset{\text{Distrib.}}{=} \big(x \wedge (\bar{x} \wedge \bar{y})\big) \vee \big(y \wedge (\bar{x} \wedge \bar{y})\big)$$

$$\underset{\text{Komm.}}{=} ((\underbrace{x \wedge \bar{x}}_{0\ (B_3)}) \wedge \bar{y}) \vee (x \wedge (\underbrace{y \wedge \bar{y}}_{0}))$$

$$\underset{(B_2)}{=} 0 \vee 0 \underset{\text{Idemp.}}{=} 0$$

Also gilt $(*)$.

Analog zeigt man $(**) \Rightarrow$ (e)

(f) Behauptung: $x \leq y \Leftrightarrow \bar{y} \leq \bar{x}$

Beweis:

$$x \leq y \underset{\text{Def.}}{\Leftrightarrow} x \wedge y = x \underset{(e)}{\Leftrightarrow} \underbrace{\overline{x \wedge y}}_{\bar{x} \vee \bar{y}} = \bar{x}$$

$$\Leftrightarrow \bar{y} \leq \bar{x}$$

(g) Behauptung: $x \leq y \Leftrightarrow \bar{x} \vee y = 1$

Beweis:

Hinrichtung:

$$\bar{x} \vee y = 1 \Rightarrow \underbrace{x \wedge (\bar{x} \vee y)}_{\underbrace{(x \wedge \bar{x})}_{0} \vee (x \wedge y) = x} = x \wedge 1$$

$$\Rightarrow x \wedge y = x \Rightarrow x \leq y$$

Rückrichtung:

$$x \leq y \Rightarrow x \wedge y = x$$

$$\Rightarrow \bar{x} \vee (x \wedge y) = \underbrace{\bar{x} \vee x}_{1}$$

$$\underset{\text{Distrib.}}{\Longrightarrow} (\bar{x} \vee x) \wedge (\bar{x} \vee y) = 1$$

$$\underset{(a)}{\Rightarrow} \bar{x} \vee y = 1$$

Eigenschaft von Verbänden, die nachfolgend benötigt wird:

$(L; \wedge,\vee)$ Verband, $L \neq \emptyset$

$:\Leftrightarrow$ $\wedge,\vee$ kommutativ, assoziativ und
$\forall x \in L: x \vee x = x \wedge x = x$ (Idempotenz)
$\forall x, y \in L: x \vee (x \wedge y) = x$ und $x \wedge (x \vee y) = x$ (Absorptionsgesetze)
(1. Definition eines Verbandes)

2. Definition:

$(L; \leq)$ Verband, $L \neq \emptyset$

$:\Leftrightarrow$ $\leq$ ist reflexive, antisymmetrische und transitive Relation auf L (d. h., $\leq$ ist reflexive Halbordnung) und für beliebige $x, y \in L$ sind $\sup\{x, y\}$ [2] und $\inf\{x, y\}$ [3] eindeutig bestimmt.

Zusammenhang zwischen den obigen Definitionen:

- Falls $(L; \vee,\wedge)$ Verband nach 1. Definition, so ist $(L; \leq)$, wobei
$$x \leq y :\Leftrightarrow x \wedge y = x$$
$$(\Leftrightarrow x \vee y = y)$$
Verband nach 2. Definition
- Falls $(L; \leq)$ Verband nach 2. Definition, so ist $(L; \vee,\wedge)$ mit
$$x \vee y := \sup\{x, y\}$$
$$x \wedge y := \inf\{x, y\}$$
Verband nach 1. Definition.

1.2 Der Stonesche Darstellungssatz

Satz 2

Bis auf Isomorphie ist $\{0, 1\} := (\{0, 1\}; \vee, \wedge, \bar{}\,, 0, 1)$ die einzige Boolesche Algebra, die
(a) Direkt unzerlegbar (direkt irreduzibel)
(b) Subdirekt unzerlegbar (subdirekt irreduzibel)
ist.

Beweis:

Zur Erinnerung:

- Bis auf Isomorphie ist $\{0, 1\}$ die einzige Boolesche Algebra mit genau 2 Elementen, da

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

(wegen (B_2) und Kommutativität) (wegen Idempotenz)

x	$\bar{x}$
0	1

[2] Kleinstes Element $\in L$, das $\geq x$ und $\geq y$
[3] Größtes Element $\in L$, das $\leq x$ und $\leq y$

$\boxed{1}\boxed{0}$

(wegen (B_3) und oben)

- $\underline{A} = (A; F)$ direkt irreduzibel $:\Leftrightarrow$

$$\underline{A} \cong \underline{A}_1 \times \underline{A}_2 \Rightarrow |A_1| = 1 \text{ oder } |A_2| = 1$$

$$\underset{\text{Vorlesung Allgemeine Algebra}}{\Longleftrightarrow}$$

$$\forall \sigma, \tau \in \operatorname{Con} \underline{A}: \\ (\sigma \wedge \tau = \kappa_0 \text{ und} \\ \sigma \vee \tau = \kappa_1 \text{ und} \\ \sigma \square \tau = \tau \square \sigma) \\ \Rightarrow \{\sigma, \tau\} = \{\kappa_0, \kappa_1\}$$

- $\underline{A} = (A; F)$ subdirekt irreduzibel

  $:\Leftrightarrow \cdots$

$$\underset{\text{Vorlesung Allgemeine Algebra}}{\Longleftrightarrow}$$

$$\bigcap_{(x \in \operatorname{Con} \underline{A} | \{\kappa_0\})} \kappa \neq \kappa_0$$

Wegen $\sigma \cap \tau = \kappa_0, \sigma \neq \kappa_0, \tau \neq \kappa_0$, falls $a \in B | \{0, 1\}$ existiert, folgt mit Hilfe des obigen Kriteriums (b).

■

Eine Folgerung aus Satz 2 und den Sätzen der Allgemeinen Algebra

- Jede *endliche* Algebra ist isomorph zu einem direkten Produkt direkt irreduzibler Algebren.
- Jede Algebra ist isomorph zu einem subdirektem Produkt subdirekt irreduzibler Algebren

Ist der folgende Satz:

Satz 3 (Stonescher Darstellungssatz)

(a) Sei $\underline{B}$ *endliche* Boolesche Algebra mit $|B| \geq 2$. Dann existiert ein $n \in \mathbb{N}$ mit der Eigenschaft, dass $\underline{B}$ isomorph zur Algebra

$$\{0,1\}^n \coloneqq \left(\{(x_1, x_2, \dots, x_n) \middle| \forall i: x_i \in \{0,1\}\}; \vee, \wedge, ^{-}, (0, 0, \dots, 0), (1, 1, \dots, 1)\right)$$

Ist (siehe Beispiel 3 aus 1.1).

(b) *Jede* Boolesche Algebra ist isomorph zu einem Feld von Teilmengen einer gewissen Menge (siehe Beispiel 4 aus 1.1).

■

Bemerkung:

Isomorph zur Algebra $\{0,1\}^n$ ist die Algebra

$$(\mathfrak{P}(X); \cap, \cup, ^{-}, \emptyset, X)$$

mit $|X| = n$

O. B. d. A. $X \coloneqq \{1, 2, \dots, n\}$

Eine isomorphe Abbildung ist dann

$$\varphi: \mathfrak{P}(X) \to \{0,1\}^n, A \mapsto (x_1, x_2, \dots, x_n),$$

wobei

$$x_i := \begin{cases} 1 & \text{falls } i \in A \\ 0 & \text{falls } i \notin A \end{cases}$$

Z. B. $n = 5$

$$A = \{2, 3, 5\}, \qquad \varphi(A) = (0, 1, 1, 0, 1)$$

1.3 Boolescher Ring

Definition:

$\{R;\ +, \cdot, -, 0, 1)$ Ring mit neutralem Element 0 bzgl. $+$ und neutralem Element 1 bzgl. $\cdot$ heißt *Boolescher Ring* $:\Leftrightarrow$

$$\forall x \in R\colon \underbrace{x \cdot x}_{x^2} = x$$

Beispiel:

$\underline{R} = (\{0, 1\};\ \underbrace{+, \cdot}_{\text{mod } 2}\ , -, 0, 1)$ ist Boolescher Ring, da $0 \cdot 0 = 0, 1 \cdot 1 = 1 \pmod 2$

Lemma 4

$\underline{R}$ Boolescher Ring

$$\Rightarrow \forall x, y \in R\colon x + x = 0 \quad \text{und}$$
$$x \cdot y = y \cdot x$$

Beweis

Nach Definition:

$$\underbrace{(x + x) \cdot (x + x)}_{} = (x + x)$$
$$\underbrace{x \cdot x}_{x} + \underbrace{x \cdot x}_{x} + \underbrace{x \cdot x}_{x} + \underbrace{x \cdot x}_{x}$$

$\Rightarrow x + x = 0$ (man subtrahiere $x + x$ [d. h. $-x = x$])

$$\underbrace{(x + y) \cdot (x + y)}_{} = x + y$$
$$\underbrace{x \cdot x}_{x} + x \cdot y + y \cdot x + \underbrace{y \cdot y}_{y}$$
$$\xRightarrow[\text{Subtration von } x+y]{} x \cdot y + y \cdot x = 0$$
$$\Rightarrow \underbrace{-(x \cdot y)}_{=(x \cdot y)} = y \cdot x$$

∎

Satz 5

(1) $\underline{B} = (B; \vee, \wedge, \overline{\ }, 0, 1)$ Boolesche Algebra

$\Rightarrow \underline{B}^* := (B;\ +, \cdot, -, 0, 1)$ mit

$$x + y := (x \wedge \bar{y}) \vee (\bar{x} \wedge y)$$
$$x \cdot y := x \wedge y$$
$$-x := x$$

ist Boolescher Ring

Speziell:

$$B = \{0, 1\}$$

x	y	$x + y \pmod 2$	$x \wedge \bar{y}$	$\bar{x} \wedge y$
0	0	0	0	0

0	1	1	0	1
1	0	1	1	0
1	1	0	0	0

$$x + y = (x \wedge \bar{y}) \vee (\bar{x} \wedge y)$$

(2) $\underline{R} = (R;\ +,\cdot,-,0,1)$ Boolescher Ring

$\Rightarrow \underline{R}^* := (R; \vee,\wedge,^{-},0,1)$ mit

$$x \vee y := x + y + x \cdot y$$
$$x \wedge y := x \cdot y$$
$$\bar{x} := 1 + x$$

ist Boolesche Algebra.

Speziell: $B = \{0,1\}$

x	y	$x \vee y$	$x + y$	$x \cdot y$
0	0	0	0	0
0	1	1	1	0
1	0	1	1	0
1	1	1	0	1

$$x \vee y = x + y + x \cdot y$$

(3) $\left(\underline{B}^*\right)^* = \underline{B}$ und $\left(\underline{R}^*\right)^* = \underline{R}$ (Beweis: Nachrechnen [ÜA]).

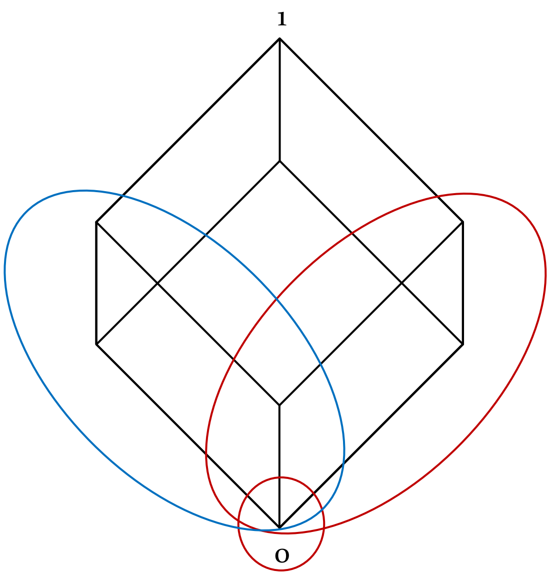
■

1.4 Filter und Ideale Boolescher Algebren

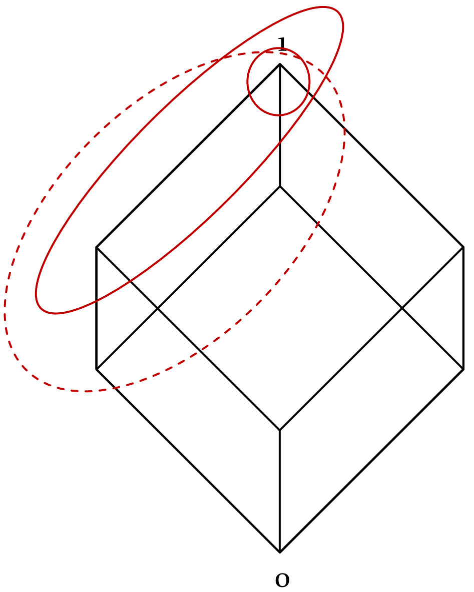
Definition: $\underline{B}$ Boolesche Algebra. $I, F \subseteq B$.

- I heißt *Ideal von $\underline{B}$* $:\Leftrightarrow$
  - (I_1) $0 \in I$
  - (I_2) $x, y \in I \Rightarrow x \vee y \in I$
  - (I_3) $(x \in I \text{ und } y \leq x) \Rightarrow y \in I$
- F heißt Filter von $\underline{B}$ $:\Leftrightarrow$
  - (F_1) $1 \in F$
  - (F_2) $x, y \in F \Rightarrow x \wedge y \in F$
  - (F_3) $(x \in F \text{ und } x \leq y) \Rightarrow y \in F$

Beispiele:



|| Idea-



Satz 6:

$\underline{B} = (B; \vee, \wedge, \bar{}, 0, 1)$ Boolesche Algebra
$\underline{B}^* = (B;\ +, \cdot, -, 0, 1)$ Boolescher Ring

$$x + y := (x \wedge \bar{y}) \vee (\bar{x} \wedge y)$$
$$x \cdot y := x \wedge y$$
$$-x := x$$

Sei $I \in B$. Dann gilt:

I Ideal von $B \Leftrightarrow I$ Ideal von B^*

Beweis:

- $\Leftarrow$
  Sei I Ideal des Booleschen Ringes, d. h. es gilt:
  (IR_1) $0 \in I \subseteq B$
  (IR_2) $\forall x, y \in I: x - y \in I$
  (IR_3) $\forall i \in I: \forall x \in B: i \cdot x \in I$
  Hieraus folgt:
  (I_1) $0 \in I$ (wegen (IR_1))
  (I_2) $\forall x, y \in I: x \vee y \in I$, da $x \vee y \underset{\text{S. 5}}{=} x + y + x \cdot y \in I$
  (I_3) $\forall x, y \in B: (x \in I$ und $y \leq x) \Rightarrow y \in I$ da $y \leq x \in I \underset{\text{Def.}}{\Longrightarrow} \underbrace{x \wedge y}_{y \cdot x} = y \in I$

- $\Rightarrow$
  Sei I Ideal der Booleschen Algebra $\underline{B}$, d. h. es gilt:
  (I_1) $0 \in I$
  (I_2) $\forall x, y \in I: x \vee y \in I$
  (I_3) $\forall x, y \in B: (x \in I$ und $y \leq x) \Rightarrow y \in I$
  Dann gilt:
  (IR_1) $0 \in I$ (wegen (I_1))
  (IR_2) $\forall a, b \in I; a + b \in I$, da $a + b \underset{\text{S. 5}}{=} \underbrace{(a \wedge \bar{b})}_{\leq a} \vee \underbrace{(\bar{a} \wedge b)}_{\leq b} \in I$ (wegen (I_2) und (I_3))
  (IR_3) $\forall i \in I: \forall x \in B: i \cdot x \in I$, da $i \cdot x = i \wedge x \leq i \underset{(I_3)}{\Longrightarrow} i \cdot x \in I$

∎

Satz 7:

$\underline{B}$ Boolesche Algebra.
$X \subseteq B,\ \bar{X} := \{\bar{x} | x \in X\}$
Dann gilt:

(a) I Ideal von $\underline{B} \Leftrightarrow \bar{I}$ Filter von $\underline{B}$
(b) F Filter von $\underline{B} \Leftrightarrow \bar{F}$ Ideal von $\underline{B}$

Beweis:

Es genügt, (a) zu beweisen.

- $\Rightarrow$
  Zu zeigen: $\bar{I}$ erfüllt die Bedingungen:
  (F_1) $1 \in \bar{I}$
  (F_2) $\forall x, y \in \bar{I}: x \wedge y \in \bar{I}$
  (F_3) $\forall x \in \bar{I}: \forall y \in B: x \leq y \Rightarrow y \in \bar{I}$
  (F_1) gilt wegen (I_1): $0 \in I$ und S. 1, (c)
  (F_2): Seien $x, y \in \bar{I}$
  $$\Rightarrow \bar{x}, \bar{y} \in I \underset{(I_2)}{\Longrightarrow} \bar{x} \vee \bar{y} \in I$$
  $$\Rightarrow \underbrace{\overline{\bar{x} \vee \bar{y}}}_{x \wedge y} \in \bar{I} \Rightarrow x \wedge y \in \bar{I}$$
  (F_3): Seien $x \in \bar{I}$ und $y \in B$ mit $x \leq y$
  $\Rightarrow \bar{x} \in I$ und $x \wedge y = x$
  $\Rightarrow \bar{x} \in I$ und $\bar{y} \leq \bar{x}$
  $$\underset{(I_3)}{\Longrightarrow} y \in \bar{I}$$
  Also ist $\bar{I}$ Filter.

- $\Leftarrow$
  Sei $\bar{I}$ Filter von $\underline{B}$, d. h. $\bar{I}$ erfüllt $(F_1), (F_2), (F_3)$
  Zu zeigen: I ist Ideal von $\underline{B}$, d. h. I erfüllt $(I_1), (I_2), (I_3)$
  (I_1) gilt wegen (F_1)
  (I_2): Seien $x, y \in I$
  $$\Rightarrow \bar{x}, \bar{y} \in \bar{I} \underset{(F_2)}{\Longrightarrow} \bar{x} \wedge \bar{y} \in \bar{I}$$
  $$\Rightarrow \overline{\bar{x} \wedge \bar{y}} = x \vee y \in I$$
  (I_3): Seien $x \in I, y \in B, y \leq x$
  $$\Rightarrow \bar{x} \in \bar{I} \text{ und } x \wedge y = y$$
  $$\Rightarrow \bar{x} \in \bar{I} \text{ und } \underbrace{\overline{x \wedge y}}_{\bar{x} \vee \bar{y}} = \bar{y}$$
  $$\Rightarrow \bar{x} \in \bar{I} \text{ und } \bar{x} \leq \bar{y}$$
  $$\underset{(F_3)}{\Longrightarrow} \bar{y} \in \bar{I} \Rightarrow y \in I$$

■

1.5 Kongruenzen auf Booleschen Algebren

Bekanntlich:

Seien $\underline{A} = (A; F), \underline{B} = (B; F)$ Algebren desselben Typs,
$\varphi: A \to B$ homomorphe Abbildung, d. h.
$\forall f^{(n)} \in F: \forall a_1, \dots, a_n \in A$:

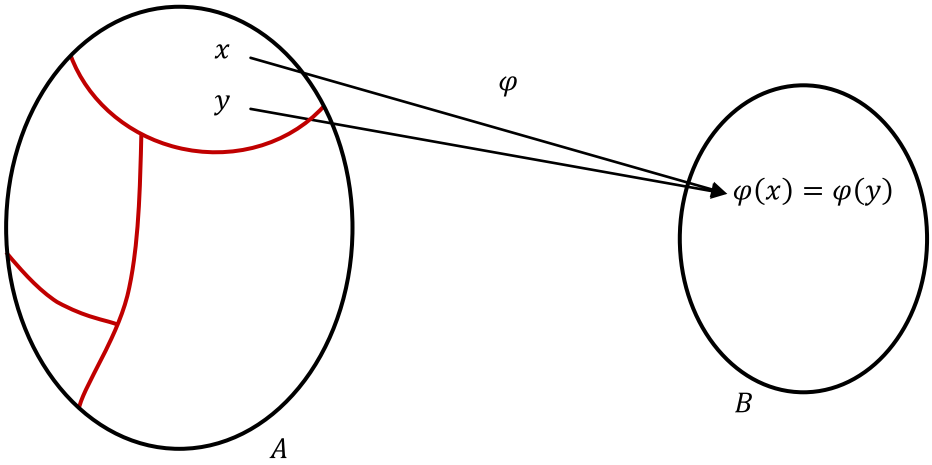
$\varphi(f(a_1, \dots, a_n)) = f(\varphi(a_1), \dots, \varphi(a_n))$ falls $n \geq 1$,
$\varphi(\underbrace{f_{\underline{A}}}_{\substack{\uparrow \\ A}}) = \underbrace{f_{\underline{B}}}_{\substack{\uparrow \\ B}}$ falls $n = 0$

Dann ist

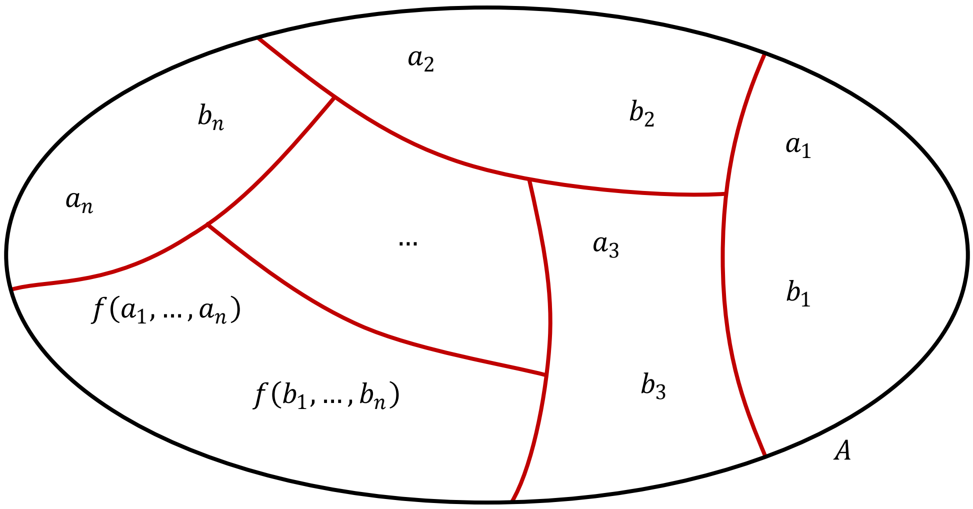
$$\kappa_\varphi \coloneqq \{(x, y) \in A^2 | \varphi(x) = \varphi(y)\}$$

Eine *Kongruenz(relation)* auf A, d. h. eine Äquivalenzrelation auf A, die mit den Operationen $\in F$ verträglich ist, d. h.

$\forall f^{(n)} \in F\ (n \geq 1): \forall a_1, \dots, a_n, b_1, \dots, b_n \in A:$
$(a_1, b_1), (a_2, b_2), \dots, (a_n, b_n) \in \kappa_\varphi \Rightarrow (f(a_1, a_2, \dots, a_n), f(b_1, b_2, \dots, b_n)) \in \kappa_\varphi$



Zerlegung von A, die durch φ bestimmt ist. Dies führt zur Äquivalenzrelation κ_φ:



Satz 8

$\underline{B}$ Boolesche Algebra
I Ideal von $\underline{B}$
Für beliebige $a, b \in B$ sind folgende Aussagen äquivalent:
(a) $\exists x, y \in I: a \vee x = b \vee y$

(b) $a \wedge \overline{b} \in I$ und $\overline{a} \wedge b \in I$

(c) $a + b \coloneqq (\overline{a} \wedge b) \vee \left(a \wedge \overline{b}\right) \in I$

Beweis:

Zeigen: (a) ⇒ (b) ⇒ (c) ⇒ (a)

(a) ⇒ (b)

$a, b \in B; \quad x, y \in I$

$a \vee x = b \vee y$

$$\Rightarrow a \wedge \bar{b} \underset{\text{Idemp., K., Abs.}}{=} \overbrace{(a \wedge \bar{b} \wedge a)}^{= a \wedge \bar{b}} \vee (a \wedge \bar{b} \wedge x)$$

$$\underset{\text{Distr.}}{=} (a \wedge \bar{b}) \wedge \underbrace{(a \vee x)}_{b \vee y}$$

$$\underset{\text{Distr.}}{=} \underbrace{(a \wedge \bar{b} \wedge b)}_{0} \vee (a \wedge \bar{b} \wedge y)$$

$$\Rightarrow a \wedge \bar{b} = (a \wedge \bar{b}) \wedge y$$

$$\Rightarrow a \wedge \bar{b} \leq y \xRightarrow[\substack{y \in I \\ I \text{ Ideal}}]{} a \wedge \bar{b} \in I$$

Analog zeigt man $\bar{a} \wedge b \in I$:

$$\bar{a} \wedge b = (\bar{a} \wedge b) \wedge (b \vee y) \underset{\text{Vor.}}{=} (\bar{a} \wedge b) \wedge (a \vee x)$$

$$= (\bar{a} \wedge b) \wedge x$$

$$\Rightarrow \bar{a} \wedge b \leq x \xRightarrow[\substack{x \in I \\ I \text{ Ideal}}]{} \bar{a} \wedge b \in I$$

Also gilt (a) ⇒ (b)

(b) ⇒ (c)

Klar, da I bzgl. $\vee$ abgeschlossen.

(c) ⇒ (a)

Sei $(\bar{a} \wedge b) \vee (a \wedge \bar{b}) \in I$

Wähle $x \coloneqq \bar{a} \wedge b, y \coloneqq a \wedge \bar{b}$

$$\Rightarrow a \vee x = a \vee (\bar{a} \wedge b) \underset{\text{Distr.}}{=} \underbrace{(a \vee \bar{a})}_{1} \wedge (a \vee b)$$

$$= a \vee b$$

Und

$$b \vee y = b \vee (a \wedge \bar{b}) \underset{\text{Distr.}}{=} (b \vee a) \wedge \underbrace{(b \vee \bar{b})}_{1}$$

$$= a \vee b$$

$$\Rightarrow a \vee x = b \vee y$$

Noch zu zeigen:

$x = \bar{a} \wedge b \in I$ und $y = a \wedge \bar{b} \in I$

Laut Voraussetzung:

$$\underbrace{(\bar{a} \wedge b)}_{x} \vee \underbrace{(a \wedge \bar{b})}_{y} \in I$$

$\Rightarrow \bar{a} \wedge b \leq x \vee y$ und $a \wedge \bar{b} \leq x \vee y$

$$\xRightarrow[\substack{\text{Def. eines} \\ \text{Ideals}}]{} \bar{a} \wedge b, a \wedge \bar{b} \in I$$

■

Satz 9

Sei $\underline{B} = (B; \vee, \wedge, \bar{\ }, 0, 1)$ Boolesche Algebra. Dann gilt:

(a) ∀ Ideale $I \subseteq B$:

$$\boxed{R(I) \coloneqq \{(a, b) \in B^2 \mid \exists x, y \in I : a \vee x = b \vee y\}}$$

ist Kongruenz auf $\underline{B}$.

(b) $\forall$ Kongruenzen R auf B:

$$I(R) \coloneqq \{a \in B | (a,0) \in R\}$$
$$(= [0]_R = 0/R)$$

ist Ideal von $\underline{B}$.

(c) $I(R(I)) = I,\ R(I(R)) = R$

Beweis:

(a)

Sei I Ideal von B.

$R(I) \coloneqq \{(a,b) \in B^2 | \exists x, y \in I: a \vee x = b \vee y\}$ ist dann

- Reflexiv, da
$$\forall a \in B: a \vee 0 = a \vee 0 \text{ und } 0 \in I$$
$$\Rightarrow (a,a) \in R(I)$$
- Symmetrisch, da
$$(a,b) \in R(I) \Rightarrow \exists x, y \in I: a \vee x = b \vee y$$
$$\Rightarrow \exists x, y \in I: b \vee y = a \vee x \Rightarrow (b,a) \in R(I)$$
- Transitiv, da
$(a,b) \in R(I)$ und $(b, c \in R(I)$
$$\Rightarrow \quad \exists x,y,u,v \in I: \quad a \vee x = b \vee y \text{ und } b \vee u = c \vee v$$
$$\Rightarrow \quad \exists x,y,u,v \in I: (a \vee x) \vee u = (b \vee y) \vee u \quad (b \vee u) \vee y = (c \vee v) \vee y$$
$$\Rightarrow \quad \exists x,y,u,v \in I: a \vee \underbrace{(x \vee u)}_{\in I} = c \vee \underbrace{(v \vee y)}_{\in I}$$
$$\xRightarrow[\substack{\text{Def. von} \\ R(I)}]{} (a,c) \in R(I)$$
Also ist $R(I)$ eine Äquivalenzrelation
- $R(I)$ ist verträglich mit $\overline{}$, da
$$(a,b) \in R(I) \Rightarrow \exists x, y \in I: a \wedge x = b \vee y$$
$$\Rightarrow \bar{a} \wedge \bar{x} = \bar{b} \wedge \bar{y}$$
$$\Rightarrow (\bar{a} \wedge \bar{x}) \vee (x \vee y) = (\bar{b} \wedge \bar{y}) \vee (x \vee y)$$
$$\Rightarrow \underbrace{((\bar{a} \wedge \bar{x}) \vee x)}_{(\bar{a} \vee x)} \vee y = \underbrace{((\bar{b} \wedge \bar{y}) \vee y)}_{(\bar{b} \vee y)} \vee x$$
(Distributivgesetz...)
$$\Rightarrow \bar{a} \vee \underbrace{(x \vee y)}_{\in I} = \bar{b} \vee \underbrace{(x \vee y)}_{\in I}$$
$$\Rightarrow (\bar{a}, \bar{b}) \in R(I)$$
- $R(I)$ ist verträglich mit $\vee$, da
$(a,b) \in R(I)$ und $(c,d) \in R(I)$
$$\Rightarrow \exists x,y,u,v \in I: a \vee x = b \vee y \text{ und } c \vee u = d \vee v$$
$$\Rightarrow (a \vee x) \vee (c \vee u) = (b \vee y) \vee (d \vee v)$$
$$\Rightarrow (a \vee c) \vee \underbrace{(x \vee u)}_{\in I} = (b \vee d) \vee \underbrace{(y \vee v)}_{\in I}$$
$$\Rightarrow (a \vee c, b \vee d) \in R(I)$$

- $R(I)$ ist verträglich mit $\wedge$, wegen dem oben Gezeigten und $x \wedge y = \overline{\bar{x} \vee \bar{y}}$

Folglich gilt (a)

(b)

Sei R eine Kongruenz auf B, d. h. R ist eine mit $\vee, \wedge, ^{-}$ verträgliche Äquivalenzrelation auf B
Zu zeigen:
$$I(R) := \{a \in B | (a, 0) \in R\} \text{ ist Ideal von } B.$$
Es gilt:

- $0 \in I(R)$, da $(0,0) \in R$ ($\leftarrow$ reflexiv)
- $\forall a, b \in I(R)$:
  $(a, 0) \in R$ und $(b, 0) \in R$
  $$\xRightarrow[\text{Verträgl.}]{} \left(a \vee b, \underbrace{0}_{0 \vee 0}\right) \in R \Rightarrow a \vee b \in I(R)$$
  $\forall a, b \in B$: $a \in I(R)$ und $b \leq a$
  $\Rightarrow (a, 0) \in R$ und $b \wedge a = b$
  $$\xRightarrow[\substack{R \text{ ist} \\ \text{Kongr.} \\ (\text{Speziell } (b,b) \in R)}]{} (\underbrace{a \wedge b}_{b}, \underbrace{a \wedge b}_{0}) \in R \underset{\text{Def.}}{\Rightarrow} b \in I(R)$$

Folglich gilt (b).

(c)

$I\big(R(I)\big) = I$ folgt aus
$$\begin{aligned} a \in I\big(R(I)\big) &\underset{\text{Def.}}{\Leftrightarrow} (a, 0) \in R(I) \\ &\underset{\text{Def.}}{\Leftrightarrow} \exists x, y \in I: a \vee x = 0 \vee y \\ &\underset{\text{S. 8}}{\Leftrightarrow} [XXX: gnaaah!] \end{aligned}$$
Es gilt nun

- $R \subseteq R\big(I(R)\big)$, da
  $(a, b) \in R \xRightarrow[R \text{ Kongr.}]{} (a \wedge \bar{b}, \underbrace{b \wedge \bar{b}}_{0}) \in R$ und $(\underbrace{a \wedge \bar{a}}_{0}, b \wedge \bar{a}) \in R$
  $\Rightarrow a \wedge \bar{b} \in I(R)$ und $b \wedge \bar{a} \in I(R)$
  $$\underset{(*)}{\Rightarrow} (a, b) \in R\big(I(R)\big)$$
- $R\big(I(R)\big) \subseteq R$, da
  $$\begin{aligned} (a, b) \in R\big(I(R)\big) &\underset{(*)}{\Rightarrow} \big(a \wedge \bar{b}\big) \vee (\bar{a} \wedge b) \in I(R) \\ &\Rightarrow \Big(\big(a \wedge \bar{b}\big) \vee (\bar{a} \wedge b), 0\Big) \in R \\ &\xRightarrow[R \text{ Kongr.}]{} (\underbrace{\big(a \wedge \bar{b}\big) \vee (\bar{a} \wedge b) \vee a}_{a \vee b}, \underbrace{0 \vee a}_{b}) \in R \\ &\xRightarrow[\substack{R \text{ symm.,} \\ \text{trans.}}]{} (a, b) \in R \end{aligned}$$

Also: $R\big(I(R)\big) = R$

■

Neue Bezeichnungen:

Anstelle von $B_{/R} := \{[x]_R | x \in B\}$, wobei R Kongruenz der Booleschen Algebra, schreiben wir

$$B/I,$$

falls R und I wie in Satz 9 zusammenhängen.

$$B/I = \{I, a+I, b+I, \dots\} \qquad a \in B \setminus I, b \in B \setminus \big(I \cup (a+I)\big), \dots$$

Eine Folgerung aus Satz 9 und dem allgemeinen Homomorphiesatz (siehe Vorlesung „Allgemeine Algebra“) ist der folgende Satz:

Satz 10

(1) $\underline{B}, \underline{C}$ Boolesche Algebra
$\varphi: B \to C$ homomorphe Abbildung

$$\Rightarrow \exists \text{ Ideal } I \text{ von } B:$$
$$\underline{\varphi(B)} \cong \underline{B/I}$$

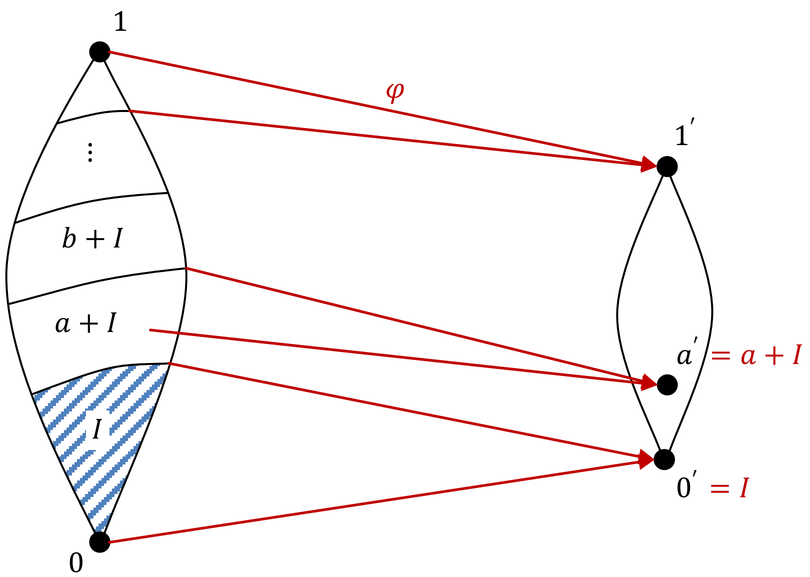
Und $\underline{B/I}$ ist ebenfalls Boolesche Algebra

(2) $\underline{B}$ Boolesche Algebra, I Ideal von $\underline{B}$.

$$\Rightarrow \varphi: B \to B/I, b \mapsto \underbrace{b/R(I)}_{\{x \in B | (b,x) \in R(I)\}}$$

ist homomorphe Abbildung, die sogenannte *kanonische homomorphe Abbildung* bzw. *natürlicher Homomorphismus*.

■

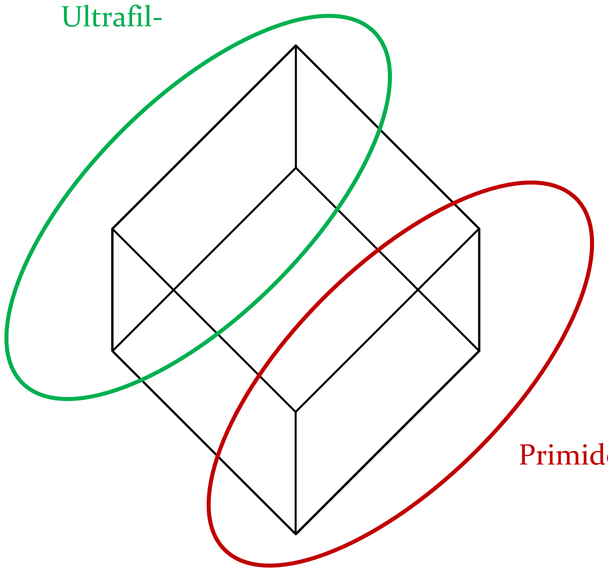


1.6 Primideale und Ultrafilter, Hilfssätze für die Aussagen- und Prädikatenlogik

Definitionen:

- I heißt Ideal der Booleschen Algebra $\underline{B}$
  I heißt *Primideal von $\underline{B}$* $:\Leftrightarrow I \neq B$ und ($\nexists$ Ideal $I' : I \subset I' \subset B$)
- F Filter der Booleschen Algebra $\underline{B}$
  F heißt Ultrafilter von $\underline{B}$ $:\Leftrightarrow F \neq B$ und ($\nexists$ Filter $F' : F \subset F' \subset B$)

Beispiel:



Satz 11

Für beliebige Ideale I ($\neq B$) der Booleschen Algebra $\underline{B}$ sind folgende Aussagen äquivalent:

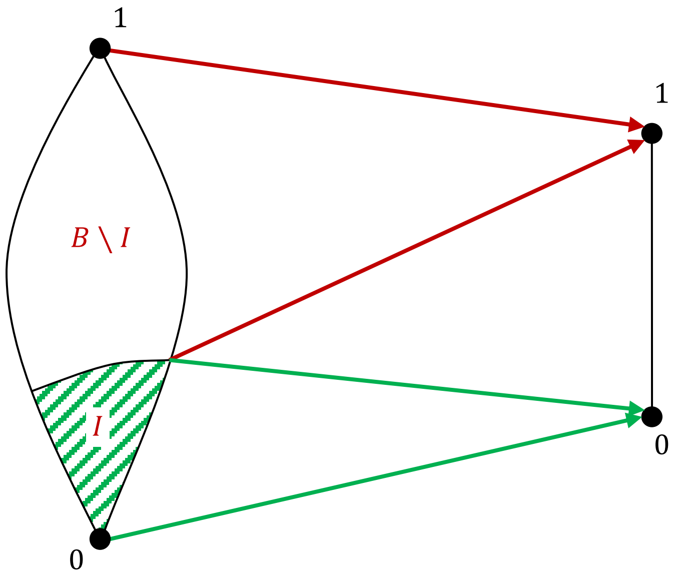
(a) I ist Primideal von $\underline{B}$

(b) $\forall a \in B$: (entweder $a \in I$ oder $\bar{a} \in I$)

(c) $\forall a, b \in B$: $\big(a \wedge b \in I \Rightarrow (a \in I$ oder $b \in I)\big)$

(d) $\exists$ homomorphe Abbildung φ von $\underline{B}$ auf die Boolesche Algebra $\underline{\{0,1\}}$ mit

$$I = \operatorname{kern} \varphi := \{x \in B | \varphi(x) = 0\}$$



Beweis

(a) $\Rightarrow$ (b)

Sei I ein Primideal von $\underline{B}$.

Zu zeigen: (α) $\nexists a \in B: \{a, \bar{a}\} \subseteq I$

(β) $\forall a \in B: a \notin I \Rightarrow \bar{a} \in I$

Zu (α):

Angenommen, es existiert ein $a \in B$ mit

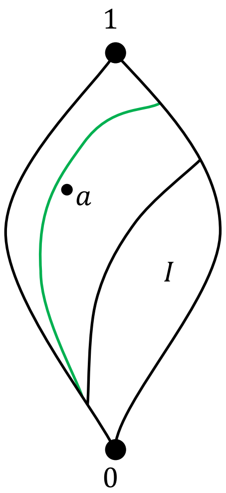
$$\{a, \bar{a}\} \subseteq I$$

$$\underset{\substack{\text{Def.}\\ \text{eines}\\ \text{Ideals}}}{\Longrightarrow} a \vee \bar{a} = 1 \in I \text{ (Widerspruch zu } I \neq B\text{)}$$

Zu (β):

Sei $a \in B$ und $a \notin I$.

Falls für alle $x \in I$: $a \vee x \neq 1$ gilt, ist I kein Primideal



$\{a \vee x | x \in I\} \cup \{y | \exists x \in I: y \leq a \vee x\}$ Ideal

Also existiert ein $x \in I$ mit $a \vee x = 1$

$$\underset{\substack{\text{S. 1, (g)}\\ (x \leq y \Leftrightarrow x \vee y = 1)}}{\Longrightarrow} \bar{a} \leq x \in I \Rightarrow \bar{a} \in I$$

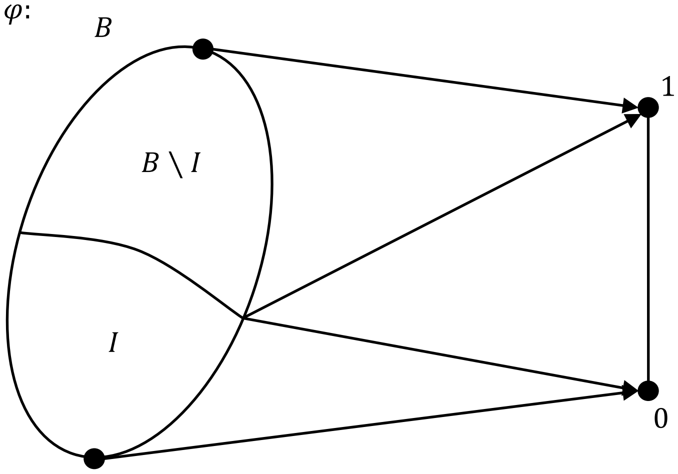
(b) ⇒ (c)

Angenommen, (c) ist falsch.

$$\Rightarrow \exists a, b \in B: a \wedge b \in I \text{ und } a \notin I \; und \; b \notin I$$
$$\underset{\text{Vor. }(b)}{\Longrightarrow} \{\bar{a}, \bar{b}\} \subseteq I$$
$$\underset{(I_2)}{\Longrightarrow} \bar{a} \vee \bar{b} \underset{\text{Satz 1}}{=} \overline{a \wedge b} \in I \underset{\text{Vor. }(b)}{\Longrightarrow} a \wedge b \notin I \text{ (Widerspruch)}$$

(c) $\Rightarrow$ (d)

φ:

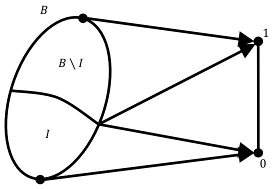


φ ist Homomorphismus, da für beliebige $x, y \in B$ gilt:

- $\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$, da
  1. Fall $x \wedge y \in I$
  $$\xRightarrow[\text{Vor. }(c)]{} x \in I \text{ oder } y \in I$$
  $$\Rightarrow \underbrace{\varphi(x \wedge y)}_{0} = \underbrace{\varphi(x) \wedge \varphi(y)}_{\text{Mindestens einer dieser Werte ist0}}$$
  2. Fall $x \wedge y \in B \setminus I$
  Wegen $x \wedge y \leq x$ und $x \wedge y \leq y$ gilt
  $x \notin I$ und $y \notin I$
  $$\Rightarrow \underbrace{\varphi(x \wedge y)}_{1} = \underbrace{\varphi(x)}_{1} \wedge \underbrace{\varphi(y)}_{1}$$
- $\varphi(\bar{x}) = \overline{\varphi(x)}$, da
  1. Fall $\bar{x} \notin I$ (d. h., $\varphi(\bar{x}) = 1$)
  Wegen $x \wedge \bar{x} = 0$ und Vor. (c) gilt dann $x \in I$ (d. h., $\varphi(x) = 0$).
  Damit:
  $$\underbrace{\varphi(\bar{x})}_{1} = \bar{0} = \overline{\varphi(x)}$$
  2. Fall $\bar{x} \in I$
  $$\xRightarrow[\substack{\text{Wegen } I \neq B \\ \text{und } x \vee \bar{x} = 1}]{} x \notin I$$
  $$\Rightarrow \varphi(\bar{x}) = 0 = \bar{1} = \overline{(\varphi(x))}$$
- $\varphi(x \vee y) = \varphi(x) \vee \varphi(y)$
  Folge aus obigen Überlegungen und Morganschen Gesetzen ($a \vee y = \overline{\bar{x} \wedge \bar{y}}$)

(d) ⇒ (a)

Voraussetzung: $\varphi: B \to \{0,1\}$ mit



ist homomorphe Abbildung

Zu zeigen: I ist Primideal

Angenommen, I ist kein Primideal

$$\Rightarrow \exists \text{ Ideal } I' : I \subset I' \subset B$$

Sei $x \in I' \setminus I$

$$\begin{aligned}
&\underset{(d)}{\Longrightarrow} \varphi(x) = 1 \Rightarrow \overline{\varphi(x)} = \varphi(\bar{x}) = 0 \\
&\underset{(d)}{\Longrightarrow} \bar{x} \in I \Rightarrow \bar{x} \in I' \\
&\Rightarrow \{x, \bar{x}\} \subseteq I' \Rightarrow x \vee \bar{x} = 1 \in I' \\
&\Rightarrow I' = B \text{ (Widerspruch)}
\end{aligned}$$

■

Satz 12 („Primidealtheorem“)

$\underline{B}$ Boolesche Algebra

Für beliebiges Ideal $I \subset B$ existiert Primideal I' mit $I \subseteq I'$

Beweis

Behauptung klar für endliche Boolesche Algebren. Sei als nächstes B abzählbar unendlich, d. h.

$$B = \{b_1, b_2, b_3, \dots\}, \qquad |B| = \aleph_0 = |\mathbb{N}|$$

Konstruktion eines Primideals I' mit $I \subseteq I'$ ist wie folgt möglich:

$$I_1 := I$$

$$I_{n+1} := \begin{cases} I_n, & \text{falls } \exists a \in I_n : a \vee b_n = 1 \\ \underbrace{[I_n \cup \{b_n\}]_{\vee,\leq}}_{\substack{\text{kleinstes Ideal, das } I_n \cup \{b_n\} \\ \text{enthält, bzw.} \\ \text{Abschluß bzgl. } \vee \text{ und } \leq}}, & \text{sonst} \end{cases}$$

$I' := \bigcup_{n \in \mathbb{N}} I_n$ ist Primideal, das I enthält.

Abschließend sei B eine Menge beliebiger Mächtigkeit.

Sei $J := \{I' \subseteq B \mid I' \text{ Ideal}, I' \neq B\}$

$$I \in J \Rightarrow J \neq \emptyset$$

Offenbar $(J;\ \subseteq)$ Poset. Diese Poset erfüllt die Voraussetzung des

Zornschen Lemmas:

$(P; \leq)$ Poset

$\forall$ total geordneten Teilmengen von P existiert eine obere Schranke

$\Rightarrow \exists$ maximales Element von P

da:
Sei K eine beliebig total geordnete Teilmenge von J, d. h., es gilt: $\forall I_1, I_2 \in K: I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$. Offenbar $\bigcup_{I' \in K} I' \in J$ und $\bigcup_{I' \in K} I'$ ist obere Schranke von K.
Folglich: J besitzt maximales Element M, d. h. $\nexists N \in J: M \subset N$. M ist das gesuchte Primideal.

■

Problem:

Gegeben:

- $\underline{B}$ Boolesche Algebra
- $M_n \subseteq B,\ (n \in \mathbb{N})$

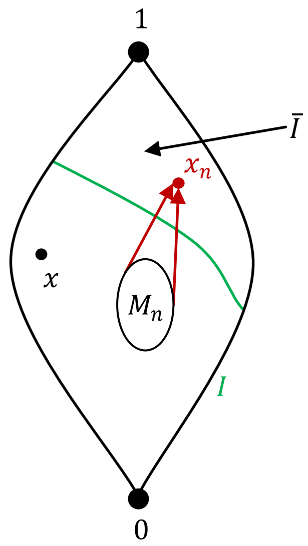
  Für jedes M_n existiert das Supremum $x_n \in B$, d. h.

$$\text{Bez.: } V\ M_n = x_n \begin{cases} \forall m \in M_n: m \leq x\_n \\ \forall y \in B: \\ \quad (\forall m \in M_n: m \leq y) \\ \quad \Rightarrow x_n \leq y \end{cases}$$

- $x \in B \setminus \{1\}$

Gesucht:

Primideal I mit $x \in I$ und der Eigenschaft, dass für beliebige $n \in \mathbb{N}$ die folgende Situation *nicht* auftritt:



D. h. der zu I gehörende kanonische Homomorphismus π:

$$B \to \{0,1\}$$
$$x \in I \Rightarrow \pi(x) = 0$$
$$x \in \bar{I} \Rightarrow \pi(x) = 1$$

hat die Eigenschaften

- $\forall n \in \mathbb{N} \exists \bigvee\{\pi(n) | m \in M_n\}$
- $\forall n \in \mathbb{N} \exists \pi(x) = \bigvee\{\pi(n) | m \in M_n\}$

Sprechweise für obige Situation:

„I bewahrt die Suprema von $G \coloneqq \{M_n | n \in \mathbb{N}\}$"

Antwort auf obiges Problem gibt das folgende

Lemma 13 (Rasiowa-Sikorski-Tarski-Lemma)

Es sei:
$\underline{B}$ Boolesche Algebra
$\forall n \in \mathbb{N}: M_n \subseteq B$ und $x_n \coloneqq \bigvee M_n \in B$ (siehe oben)
$G \coloneqq \{M_n | n \in \mathbb{N}\}$
Dann gilt:
$\forall x \in B \setminus \{1\}: \exists$ Primideal I:
$x \in I$ und I bewahrt die Suprema von G.

Beweis:

Sei $x \in B \setminus \{1\}$ beliebig gewählt. Zeigen zunächst durch vollständige Induktion, dass eine Folge

$$a_n \in M_n, \qquad (n \in \mathbb{N})$$

mit der Eigenschaft

$$\forall n \in \mathbb{N}: x \vee (x_1 \wedge \bar{a}_1) \vee (x_2 \wedge \bar{a}_2) \vee \dots \vee (x_n \wedge \bar{a}_n) \neq 1$$

existiert:

(1) $n = 1$

Angenommen, für alle $a \in M_1$:

$$\underbrace{x \vee (x_1 \wedge \bar{a})}_{(x \vee x_1) \wedge (x \vee \bar{a})} = 1$$

$\Rightarrow x \vee x_1 = 1$ und $x \vee \bar{a} = 1$ für alle $a \in M_1$

$\xRightarrow[\text{Satz 1, (g)}]{} a \leq x$ für alle $a \in M_1 \Rightarrow x_1 \leq x$

$\xRightarrow[\text{Def. von} \leq]{} x_1 \vee x = x = 1$ (Widerspruch!)

(2) $n \to n + 1$

Angenommen, es existiert

$a_n \in M_1, a_2 \in M_2, \dots, a_n \in M_n$ mit

$$x \vee (x_1 \wedge \bar{a}_1) \vee (x_2 \wedge \bar{a}_2) \vee \dots \vee (x_n \wedge \bar{a}_n) \neq 1$$

Zu zeigen:

Es existiert $a_{n+1} \in M_{n+1}$ mit

$$x \vee (x_1 \wedge \bar{a}_1) \vee \dots \vee (x_{n+1} \wedge \bar{a}_{n+1}) \neq 1$$

Angenommen, für jedes $a \in M_{n+1}$ gilt:

$$\underbrace{x \vee (x_1 \wedge \bar{a}_1) \vee \dots \vee (x_n \wedge \bar{a}_n)}_{=: y} \vee (x_{n+1} \wedge \bar{a}_{n+1}) \neq 1$$

Es gilt dann:

$$\underbrace{y}_{\neq 1} \vee (x_{n+1} \wedge \bar{a}_{n+1}) = 1$$

$$\underset{(D)}{=} \underbrace{(y \vee x_{n+1})}_{=1} \wedge \underbrace{(y \vee \bar{a})}_{=1} = 1$$

$\xRightarrow[\text{S. 1, (g)}]{} \quad a \leq y$ für alle $a \in M_{n+1}$

$\xRightarrow[x_{n+1} := \bigvee M_{n+1}]{} \quad x_{n+1} \leq y$

$\Rightarrow \quad \underbrace{x_{n+1} \vee y}_{=1,\text{ s. oben}} = y$

Widerspruch zur Induktionsannahme.

∎

Die Menge

$$\{x\} \cup \{x_n \wedge \bar{a}_n | n \in \mathbb{N}\}$$

erzeugt ein eigentliches Ideal I_1 von B, da

[XXX: Bild]

$\xRightarrow[\text{Satz 12}]{} \exists$ Primideal $I: I_1 \subseteq I$

Betrachten von Homomorphismus

$$\pi: B \to \{0,1\}$$
$$\forall x \in I: \pi(x) = 0$$
$$\forall x \in \bar{I}: \pi(x) = 1$$

für das gilt:

- $\pi(\underbrace{x_k \wedge \bar{a}_k}_{\in I}) = \pi(x_k) \wedge \overline{\pi(a_k)} = \overline{\overline{\pi(x_k)} \vee \pi(a_k)} = 0$

$$\Rightarrow \overline{(\pi(x_k))} \vee \pi(a_k) = 1$$

$$\xRightarrow[\text{Satz 1, (g)}]{} \pi(x_k) \leq \underbrace{\pi(a_k)}_{\leq \bigvee\{\pi(a) | a \in M_k\}}$$

$$\Rightarrow \pi(x_k) \leq \bigvee\{\pi(a) | a \in M_k\}$$

- Nach Definition: $\forall a \in M_n : a \leq x_k$

$$\Rightarrow a \vee x_k = x_k$$

$$\xRightarrow[\text{Hom.}]{\pi} \pi(a) \vee \pi(x_k) = \pi(x_k)$$

$$\Rightarrow \pi(a) \leq \pi(x_k) \text{ für alle } a \in M_k$$

Folglich

$$\bigvee\{\pi(a) | a \in M_k\} \leq \pi(x_k)$$

Zusammenfassend erhalten wir damit

$$\bigvee\{\pi(a) | a \in M_k\} = \pi(x_k)$$

für jedes $k \in \mathbb{N}$, d. h., I bewahrt die Suprema von G.

■

2 Aussagenlogik

2.1 Aussagen, Aussagenverknüpfung

Definition: Eine *Aussage* in der Aussagenlogik ist ein sprachliches „Gebilde" (meist in der Form eines Satzes der natürlichen Sprache), von dem es sinnvoll ist, zu fragen, ob er *wahr* oder *falsch* ist.

Bezeichnungen für Aussagen: $A, B, \dots, p, q, \dots, p_i, q_i, \dots$

$$A \begin{cases} \text{wahr} & 1 \\ \text{falsch} & 0 \end{cases}$$

Beispiele:

1. 5 ist eine Primzahl 1
2. $2 + 3 = 9$ 0
3. Im Weltall gibt es außerirdische Lebewesen. ?

Keine Aussagen sind z. B.:

4. Seid leise!
5. Alles, was ich sage, ist falsch.
6. Heute ist ein schöner Tag.
7. Zwei Hühner auf dem Weg nach vorgestern.

Sprachlich kann man Aussagen durch gewisse Bindewörter wie z. B. und, oder, wenn-dann, … verknüpfen und man erhält wieder eine Aussage. Außerdem kann man durch Verneinung (Negation) einer Aussage wieder eine Aussage gewinnen. Bei der mathematischen Modellierung dieses Sachverhaltes lassen wir uns von folgendem Prinzip leiten:

Der Wahrheitswert einer zusammengesetzten Aussage ist nur von den Wahrheitswerten der Einzelaussagen und der verwendeten Bindewörter abhängig.

Eine wahre Aussage ist damit z. B.:

Wenn die Rose Stacheln hat, dann kann man in Rostock Informatik studieren.

Da wir vom Inhalt der Aussagen abstrahieren, Aussagen nur die Werte 0 oder 1 annehmen und nach obigem Prinzip, sind Aussagenverbindungen Abbildungen der Art

$$\underbrace{\{0,1\} \times \{0,1\} \times \ldots \times \{0,1\}}_{n \text{ mal}} \to \{0,1\}, \qquad (n \in \mathbb{N})$$

die sogenannten *n-stelligen Booleschen Funktionen*.

Für unsere Zwecke genügen die folgenden ein- und zweistelligen Booleschen Funktionen bzw. *Aussagenverbindungen*:

- *Negation* ($\neg$ oder $\overline{}$)
  Die Aussage $\neg p$ (oder $\bar{p}$) sei genau dann wahr, wenn p falsch ist.

p	$\neg p$
0	1
1	0

- Disjunktion ($\vee$)
  $p \vee q$ ist genau dann falsch, wenn p und q falsch sind.
  [XXX: Wertetabelle]
- Konjunktion ($\wedge$)
  $p \wedge q$ ist genau dann wahr, wenn p und q wahr sind.
  [XXX: Wertetabelle]
- Kontravalenz ($+$ oder $\oplus$)
  $p + q$ ist genau dann wahr, wenn entweder p oder q wahr ist.
  [XXX: Wertetabelle]
- Äquivalenz ($\Leftrightarrow$ oder $\leftrightarrow$)
  $p \Leftrightarrow q$ ist genau dann wahr, wenn p und q den gleichen Wert haben.
  [XXX: Wertetabelle]
- Implikation ($\Rightarrow$ oder $\rightarrow$)
  $p \Rightarrow q$ ist genau dann falsch, wenn p wahr und q falsch.
  [XXX: Wertetabelle]

Vorteil obiger Beschreibung von Aussagenverknüpfungen mittels Boolescher Funktionen:

- Exakte Beschreibung (im Gegensatz zum sprachlichen Gebrauch, z. B. von „oder“)
- Durch formale Behandlung von Booleschen Funktionen kann man sich Umformulierungen von Aussagenverbindungen leicht verschaffen
- ...

Zunächst aber: Übersetzen eines umgangssprachlichen Satzes in einen aussagenlogischen Ausdruck durch

- Zerlegung des Satzes in nicht weiter zerlegbare Einzelsätze
- Auffinden der aussagenlogischen Verknüpfungen zwischen den Einzelsätzen und die Art der Verklammerung der Teilausdrücke

Beispiele:

1. Sonntags besuchen wir unsere Freunde und, sofern es nicht gerade regnet, machen wir eine Wanderung oder eine Radpartie.

   Diese Aussage A lässt sich wie folgt in folgende Einzelaussagen zerlegen:
   B: es ist Sonntag
   C: wir besuchen unsere Freunde
   D: es regnet
   E: wir machen eine Wanderung
   F: wir machen eine Radpartie
   Logisch präzise (aber stilistisch schlecht) lautet dann A:
   Wenn es Sonntag ist, *dann*
   1. besuchen wir unsere Freunde *und*
   2. wenn es nicht regnet, dann
   3. [XXX: ergänzen]

2.2 Erster Abschnitt zur Aussagenlogik

Sprachliche Hilfsmittel:

$$At \coloneqq \{A, B, C, \dots, A_1, B_1, C_2, \dots, A_n, B_n, C_n, \dots\}$$

Menge der atomaren Aussagen *(Aussagenvariable).*

$$J \coloneqq \{\wedge, \vee, \neg, \Rightarrow\}$$

Menge der logischen Symbole *(Junktoren).*

$$K \coloneqq \{(,)\}$$

Menge der Klammersymbole.

$$F_0' \coloneqq \{(X) | X \in At\}$$

Menge der „Atomformeln“

$$F_{n+1}' \coloneqq \left\{(X \circ Y) \middle| X, Y \in F_n', \circ \in \{\wedge, \vee, \Rightarrow\}\right\} \cup \{(\neg X) | X \in F_n'\} \cup F_n', \qquad (n \in \mathbb{N}_0)$$

$F \coloneqq \bigcup_{n=0}^{\infty} F_n'$ „Menge der Formeln“ bzw. „Menge der syntaktisch richtigen Ausdrücke“

$$F_0 \coloneqq F_0', \qquad F_{n+1} \coloneqq F_{n+1}' \setminus F_n'$$

Um Schreibarbeit zu sparen, verzichten wir in Beispielen auf die Außenklammern und auf Klammern, die durch Festlegungen wie *„$\wedge$ bindet stärker als $\vee$“* überflüssig sind.

Beispiele:

1. $f = \left(\left((A) \wedge (B)\right) \vee (C)\right) \in F_2$
   Wir setzen: $f = A \wedge B \vee C$
2. $g = \left(\left((A) \vee (B)\right) \vee (C)\right)$
   Wir setzen: $g = A \vee B \vee C$ (möglich wegen der Assoziativität von $\vee$)

Eine solche Vereinbarung ist natürlich nur dann sinnvoll, wenn man – bei Kenntnis der Werte von A, B, C ($\in \{0, 1\}$) – den Wert von $\left(\left((A) \wedge (B)\right) \vee (C)\right)$ ausrechnen möchte!

Durch Induktion über dem Formelaufbau beweist man den

Satz 14

$\forall \varphi \in F$:
1. φ ist Atomformel ($\Leftrightarrow \varphi \in F_0$)

Oder

2. $\varphi \in F_n$ für gewisses $n \in \mathbb{N}$ und es existiert $\varphi_1, \varphi_2 \in F_{n+1}$ mit $\varphi = (\varphi_1 \circ \varphi_2)$ für gewisses $\circ \in \{\wedge, \vee, \Rightarrow\}$ oder $\varphi = (\neg \varphi_1)$

■

Wir wollen nun den Formeln aus F einen Inhalt geben. Dazu benutzen wir sogenannte Bewertungsfunktionen:

Def.:

Seien $\vee, \wedge, \Rightarrow, \neg$ auf $\{0, 1\}$ wie im Abschnitt Aussagen, Aussagenverknüpfung definiert.
Eine Abbildung

$$u: F \to \{0, 1\}$$

Heißt *Bewertungsfunktion* (kurz: *Bewertung*), genau dann wenn

$$u(\neg f) = \neg u(f)$$
$$u(g \vee h) = u(g) \vee u(h)$$
$$u(g \wedge h) = u(g) \wedge u(h)$$
$$u(g \Rightarrow h) = u(g) \Rightarrow u(h)$$

Für beliebige $f, g, h \in F$

Beispiel:

Sei $A \in At$ und $u: F \to \{0, 1\}$
Setzen $u\big((A)\big) := 0$ und $u\big((X)\big) := 1$ für alle $X \in At \setminus \{A\}$
Dann muss gelten:

$$u\big(\neg (A)\big) = \neg u\big((A)\big) = 1$$
$$u\big(\neg (X)\big) = \neg u\big((X)\big) = 0$$
$$u\left(\left((A) \vee (B)\right)\right) = u\big((A)\big) \vee u\big((B)\big) = 1$$
$$\vdots$$

Def.:

$\varphi \in F, u$ Bewertung

- φ ist *falsch* unter u genau dann, wenn $u(\varphi) = 0$

- φ ist *wahr* unter u genau dann, wenn $u(\varphi) = 1$
- φ heißt *Tautologie* genau dann, wenn $u(\varphi) = 1$ für alle Bewertungen u
- φ heißt *erfüllbar* genau dann, wenn eine Bewertung u existiert mit $u(\varphi) = 1$
- φ heißt *widerspruchsvoll* genau dann, wenn $u(\varphi) = 0$ für alle Bewertungen u

[XXX: Bild]

Beispiele:

A	B	$A \wedge B$	$A \wedge (\neg A)$	$A \vee (\neg A)$
0	0	0	0	1
0	1	0	0	1
1	0	0	0	1
1	1	1	0	1

Satz 15 („Fortsetzungssatz“)

Jede Abbildung $u_0: F_0 \to \{0, 1\}$ lässt sich auf *genau eine Weise* zu einer Bewertungsfunktion

$$u: F \to \{0, 1\}$$

fortsetzen.

Beweis:

Klar nach Definition einer Bewertung.

■

Bemerkungen:

Obige Definitionen sind Spezialfälle gewisser Definitionen der Allgemeinen Algebra. Legt man als Typ von Algebren

$$(\vee, 2), (\wedge, 2), (\Rightarrow, 2), (\neg, 1)$$

fest, so ist

$$F = \underbrace{T(At)}_{\substack{\text{Trägermenge der Termalgebra} \\ \text{über dem Alphabet } X := At}} .$$

Eine Bewertung ist eine homomorphe Abbildung von der Termalgebra

$$(T(At); \vee, \wedge, \Rightarrow, \neg)$$

in die Algebra

$$(\{0, 1\}; \vee, \wedge, \Rightarrow, \neg).$$

Obiger Fortsetzungssatz ergibt sich damit aus einem entsprechenden Satz über homomorphe Abbildungen:

$\underline{A} := (A; F)$ Algebra mit Erzeugungssystem $B \subseteq A$
$\underline{C} := (C; F)$ Algebra
$u_0: B \to C$
Dann gibt es genau eine homomorphe Abbildung u, die auf B mit u_0 übereinstimmt und die Algebra $\underline{A}$ in $\underline{C}$ homomorph abbildet.

Von den Problemen der Aussagenlogik (später Prädikatenlogik) wollen wir zunächst das sogenannte *„Vollständigkeitsproblem“* behandeln.

Grob gesagt, geht es um die Beantwortung folgender Fragen:

- Wie kann man feststellen, ob eine Formel eine Tautologie ist?
  (Methode: Aufstellen einer Tabelle ist nur für Formeln mit wenigen Aussagenvariablen praktikabel!)
- Wie erhält man alle Tautologien (die gewisse logische Zeichen erhalten), d. h., alle „Gesetze der Aussagenlogik“?
- Wie erhält man alle zu einer Formel φ äquivalenten Formeln ψ, d. h., für welche ψ ist $\varphi \Leftrightarrow \psi$ eine Tautologie?

Unser Weg: Wir führen 2 Folgerungsbegriffe (Operatoren) ein:

- $\vDash$ *„semantischer Folgerungsoperator“ (kurz: Folgerungs-Op.)*
  $\emptyset \vDash \varphi$ genau dann, wenn φ ist Tautologie
- $\vdash$ *„syntaktischer Folgerungsoperator“ (kurz: Ableitungs-Op.)*

$\emptyset \vdash \varphi$ genau dann, wenn φ ist mittels gewisser Regeln aus den gegebenen 13 Tautologien ableitbar.

2.3 Semantischer Folgerungsbegriff

$$\Sigma \subseteq F, \qquad \varphi \in F$$

- $\emptyset \vDash \varphi$ genau dann, wenn φ Tautologie
  (kurz: $\vDash \varphi$)
- $\Sigma \neq \emptyset$
  $\Sigma \vDash \varphi$ genau dann, wenn:
  Für alle Bewertungen $u\colon F \to \{0,1\}$ gilt:
  Wenn für alle $\alpha \in \Sigma\colon u(\alpha) = 1$, so auch $u(\varphi) = 1$
  Falls $\Sigma = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, schreiben wir auch
  $$\alpha_1, \alpha_2, \dots, \alpha_n \vDash \varphi$$
- $\mathrm{Cons}(\Sigma) \coloneqq \{\varphi | \Sigma \vDash \varphi\}$ „Folgerungen aus Σ“

Beispiel:

$$\Sigma = \{(A \vee B), \big((\neg A) \wedge B\big) \vee \big(A \wedge (\neg B)\big)\}$$

A	B	$A \vee B$	$(\neg A \wedge B) \vee (A \wedge \neg B)$	…
0	0	0	0	(beliebig)
0	1	1	1	1
1	0	1	1	1
1	1	1	0	(beliebig)

$\underbrace{\qquad\qquad}_{\in \mathrm{Cons}\,(\Sigma)}$

Auch Elemente von $\mathrm{Cons}(\Sigma)$ sind:

$$\big((A \vee B) \vee C\big), \dots$$

und alle Tautologien

Offenbar gilt

Satz 16

$\mathrm{Cons}\colon \mathfrak{P}(F) \to \mathfrak{P}(F)$ ist Hüllenoperator, d. h.,

- $\Sigma \subseteq \mathrm{Cons}(\Sigma)$
- $\Sigma_1 \subseteq \Sigma_2$, dann $\mathrm{Cons}(\Sigma) \subseteq \mathrm{Cons}(\Sigma_2)$
- $\mathrm{Cons}(\mathrm{Cons}(\Sigma)) = \mathrm{Cons}(\Sigma)$

für beliebige $\Sigma, \Sigma_1, \Sigma\_2 \in \mathfrak{P}(F)$

2.4 Der syntaktische Folgerungsoperator (Ableitungsoperator)

Zunächst:

Der *Hilberttypkalkül* für die klassische Aussagenlogik besteht aus folgenden Axiomen und einer Regel:

(I) Axiome
Für beliebige $\alpha, \beta, \gamma \in F$ gilt:

[XXX: viiieeele tolle Axiome, stehen bei ihr im Netz]

(II) Regel: *„Modus ponens"*

$$\frac{\sigma,\ \sigma \Rightarrow \tau}{\tau}$$

(d. h., falls $\sigma, \sigma \Rightarrow \tau$ mittels Kalkül abgeleitet oder Axiome sind, ergibt sich hieraus mittels M. p. die Formel τ.)

Def.:

Seien $\Sigma \subseteq F,\ \varphi \in F$

$\Sigma \vdash \varphi$ (d. h. „φ ist aus Σ abgeleitet" bzw. „φ ist eine *Ableitung* aus Σ")

genau dann wenn

es existiert eine *endliche* Folge

$$(\varphi_1, \varphi_2, \dots, \varphi_n)$$

So dass für jedes $i \in \{1, 2, \dots, n\}$ gilt:

φ_i ist ein Axiom oder $\varphi\_i \in \Sigma$ oder φ_i ergibt sich mittels M. p. aus φ_u, φ_v mit $u, v < i$

Bezeichnung:

$\Sigma \subseteq F$

$$\mathrm{cons}(\Sigma) \coloneqq \{\varphi \in F | \Sigma \vdash \varphi\}$$

Beispiele:

1.

$\varphi_1 = \alpha \Rightarrow \alpha$	(A1)
$\varphi_2 = (\alpha \Rightarrow \alpha) \Rightarrow (\alpha \vee \neg\alpha)$	(A13)
$\varphi_3 = \alpha \vee \neg\alpha$	M. p. (φ_1, φ_2)
$\varphi_4 = (\alpha \vee \neg\alpha) \Rightarrow \big((\beta \vee \gamma) \Rightarrow (\alpha \vee \neg\alpha)\big)$	(A2)
$\varphi_5 = (\beta \vee \gamma) \Rightarrow (\alpha \vee \neg\alpha)$	M. p. (φ_3, φ_4)

Also: $0 \vdash \varphi_5$

2. $\Sigma = \{A, B, C\}$

$\varphi_1 = A \wedge B$	
$\varphi_2 = (A \wedge B) \Rightarrow \big((A \wedge B) \vee C\big)$	(A5)
$\varphi_3 = (A \wedge B) \vee C$	M. p. (φ_1, φ_2)
$\varphi_4 = \big((A \wedge B) \vee C\big) \Rightarrow \big((A \vee C) \wedge (B \vee C)\big)$	(A9)
$\varphi_5 = (A \vee C) \wedge (B\ or\ C)$	M. p. (φ_1, φ_4)

Also: $\Sigma \vdash \varphi_5$

Satz 17 (Vollständigkeitssatz der Aussagenlogik)

Für beliebige $\Sigma \subseteq F$ gilt

$$\mathrm{cons}(\Sigma) = \mathrm{Cons}(\Sigma)$$

d. h. $\vdash = \vDash$

Beweis:

Zeigen:

$$\mathrm{cons}(\Sigma) \subseteq \mathrm{Cons}(\Sigma)$$

und

$$\mathrm{cons}(\Sigma) \supseteq \mathrm{Cons}(\Sigma).$$

Zu $\mathrm{cons}(\Sigma) \subseteq \mathrm{Cons}(\Sigma)$:

Behauptung: Falls $\Sigma \vdash \varphi$, dann $\Sigma \vDash \varphi$ (Nachweis der *„Korrektheit von ⊢“*)

Man rechnet leicht nach, dass die Formeln (A1)–(A13) Tautologien sind.

Noch zu zeigen: Modus ponens arbeitet korrekt, d. h. falls

$$\Sigma \vDash \alpha \text{ und } \Sigma \vDash \alpha \Rightarrow \beta$$

dann auch

$$\Sigma \vDash \beta$$

Seien $\Sigma \vDash \alpha$ und $\Sigma \vDash \alpha \Rightarrow \beta$, d. h. für alle Belegungen u mit $u(\varphi) = 1$ für alle $\varphi \in \Sigma$ gilt:

$$u(\alpha) = 1 \qquad \text{und}$$
$$u(\alpha \Rightarrow \beta) = 1.$$

Damit:

$$1 = u(\alpha \Rightarrow \beta) = \underbrace{u(\alpha)}_{1} \Rightarrow u(\beta)$$

Daraus folgt: $u(\beta) = 1$

Also: $\Sigma \vDash \beta$

Zu $\mathrm{Cons}(\Sigma) \subseteq \mathrm{cons}(\Sigma)$:

Beweisidee:

Definieren auf F eine Äquivalenzrelation $\approx_\Sigma$ wie folgt:

$$\alpha \approx_\Sigma \beta \text{ :gdw } \Sigma \vdash \alpha \Rightarrow \beta \quad \text{und}$$
$$\Sigma \vdash \beta \Rightarrow \alpha$$

Zeigen, dass $\approx_\Sigma$ verträglich mit $\vee, \wedge, \neg, \Rightarrow$

(Damit ist $\approx_\Sigma$ Kongruenz der Algebra $F; \vee, \wedge, \neg, \Rightarrow$), wobei $\alpha \vee \beta := \alpha \vee \beta, \dots$ $(\alpha, \beta \in F)$)

Zeigen außerdem, dass

$$(F/{\approx_\Sigma}; \vee, \wedge, \neg, \underbrace{[\alpha \wedge (\neg\alpha)]_{\approx_\Sigma}}_{„0“}, \underbrace{\{\varphi | \Sigma \vdash \varphi\}}_{„1“})$$

mit

$$[\alpha]_{\approx_\Sigma} \vee [\beta]_{\approx_\Sigma} := [\alpha \vee \beta]_{\approx_\Sigma}$$
$$\dots \wedge \dots := [\dots \wedge \dots]_{\approx_\Sigma}$$
$$\neg\{\alpha\}_{\approx_\Sigma} := [\neg\alpha]_{\approx_\Sigma}$$

Boolesche Algebra

Falls obiges gezeigt ist, lässt sich $\mathrm{Cons}(\Sigma) \subseteq \mathrm{cons}(\Sigma)$ leicht indirekt beweisen:

Angenommen, $\mathrm{cons}(\Sigma) \underset{\neq}{\subset} \mathrm{Cons}(\Sigma)$

Dann existiert $\varphi \in F$ mit

$$\Sigma \vDash \varphi \text{ und } \Sigma \nvdash \varphi$$

Folglich:

[XXX: Bild]

Nach Abschnitt über Boolesche Algebren existiert ein Primideal I mit

[XXX: Bild]

Folglich existiert eine homomorphe Abbildung $u: F \to \{0, 1\}$ mit $u(\varphi) = 0$ und $u(\alpha) = 1$ für alle $\alpha \in \Sigma$. → Widerspruch.

[XXX: Bild]

Ausführlich:

Def.:

$$\alpha \approx_\Sigma \beta \text{ :gdw } \Sigma \vdash \alpha \Rightarrow \beta \quad \text{und}$$
$$\Sigma \vdash \beta \Rightarrow \alpha$$

d. h.

$At \rightarrow A\ B\ C\ \dots$	$\alpha \Rightarrow \beta$	$\beta \Rightarrow \alpha$
Alle Tupel auf denen alle $\varphi \in \Sigma$ gleich 1 sind.	1	1

Und es gibt eine „Ableitung“ von $\alpha \Rightarrow \beta$ und $\beta \Rightarrow \alpha$, die obige Eigenschaft beweist.

1. Behauptung:

$\approx_\Sigma$ ist eine Äquivalenzrelation auf F, d. h. es gilt

- $\forall \varphi \in F{:}\ \varphi \approx_\Sigma \varphi$
- $\forall \alpha, \beta \in F$: wenn $\alpha \approx_\Sigma \beta$, dann $\beta \approx_\Sigma \alpha$
- $\forall \alpha, \beta, \gamma \in F$: Wenn $\alpha \approx_\Sigma \beta$ und $\beta \approx_\Sigma \gamma$, dann auch $\alpha \approx_\Sigma \gamma$

Beweis:

Vereinbarung: Schreiben $\approx$ anstelle von $\approx_\Sigma$.

- Nach Definition: $\varphi \approx \varphi$:gdw $\Sigma \vdash \alpha \Rightarrow \beta$ und $\Sigma \vdash \beta \Rightarrow \alpha$
  Dies gilt jedoch wegen
  $$(\mathrm{A1}) \quad \alpha \Rightarrow \alpha$$
- Sei $\alpha \approx \beta$ (d. h. $\Sigma \vdash \alpha \Rightarrow \beta$ und $\Sigma \vdash \beta \Rightarrow \alpha$)
  Offenbar folgt hieraus: $\beta \approx \alpha$
- Seien $\alpha \approx \beta$ und $\beta \approx \gamma$, d. h.,
  $$\Sigma \vdash \alpha \Rightarrow \beta$$
  $$\Sigma \vdash \beta \Rightarrow \alpha$$
  $$\Sigma \vdash \beta \Rightarrow \gamma$$
  $$\Sigma \vdash \gamma \Rightarrow \beta$$

$$(\mathrm{A3}) \qquad (\alpha \Rightarrow \beta) \Rightarrow \big((\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma)\big)$$

Modus ponens:

$$\frac{\sigma, \sigma \Rightarrow \tau}{\tau}$$

Wähle oben $\sigma = \alpha \Rightarrow \beta, \tau = (\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma)$

Damit erhält man aus (A3) und dem M. p.

$$\Sigma \vdash (\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma)$$

Nochmals Anwendung des M. p. liefert:

$$\Sigma \vdash \alpha \Rightarrow \gamma$$

Analog zeigt man: $\Sigma \vdash \gamma \Rightarrow \alpha$

Also: $\alpha \approx \gamma$

■

2. Behauptung:

$\approx_\Sigma$ ist eine Kongruenz der Algebra

$$(F; \wedge, \vee, \Rightarrow, \neg),$$

wobei für beliebige $\alpha, \beta \in F$ gilt:

$$\alpha \wedge \beta \coloneqq (\alpha \wedge \beta)$$
$$\alpha \vee \beta \coloneqq (\alpha \vee \beta)$$
$$\alpha \Rightarrow \beta \coloneqq (\alpha \Rightarrow \beta)$$
$$\neg\alpha \coloneqq (\neg\alpha)$$

d. h. $\approx_\Sigma$ ist verträglich (kompatibel) mit den Operationen $\wedge, \vee, \Rightarrow, \neg$.

Beweis:

Eine Operation $\circ \in \{\wedge, \vee, \Rightarrow\}$ ist verträglich mit $\approx_\Sigma$ genau dann, wenn für beliebige $\alpha, \beta, \gamma, \delta \in F$ gilt: Wenn $\alpha \approx_\Sigma \beta$ und $\gamma \approx_\Sigma \delta$, dass auch

$$\alpha \circ \gamma \approx_\Sigma \beta \circ \delta$$

$\neg$ ist verträglich mit $\approx_\Sigma$ genau dann, wenn für beliebige $\alpha \in F$ gilt: Wenn $\alpha \approx_\Sigma \beta$, dann auch $\neg\alpha \approx_\Sigma \neg\beta$

Vereinbarung: Schreiben $\approx$ statt $\approx_\Sigma$.

$\neg$:

Sei $\alpha \approx \beta$, d. h. $\Sigma \vdash \alpha \Rightarrow \beta$ und $\Sigma \vdash \beta \Rightarrow \alpha$

(A11) $\quad (\alpha \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$

Mittels (A11) und M. p. erhält man:

$$\Sigma \vdash \neg\beta \Rightarrow \neg\alpha$$
$$\Sigma \vdash \neg\alpha \Rightarrow \neg\beta$$

Also gilt: $\neg\alpha \approx \neg\beta$

$\Rightarrow$:

Seien $\alpha \approx \beta$ und $\gamma \approx \delta$, d. h.,

$$\Sigma \vdash \alpha \Rightarrow \beta$$
$$\Sigma \vdash \beta \Rightarrow \alpha$$
$$\Sigma \vdash \gamma \Rightarrow \delta$$
$$\Sigma \vdash \delta \Rightarrow \gamma$$

(A2) $\quad \varphi \Rightarrow (\psi = \varphi)$

Wähle $\varphi \coloneqq \gamma \Rightarrow \delta$ und $\psi \coloneqq \alpha$

$$(\gamma \Rightarrow \delta) \Rightarrow \big(\alpha \Rightarrow (\gamma \Rightarrow \delta)\big)$$

M. p. liefert

$$\Sigma \vdash \alpha \Rightarrow (\gamma \Rightarrow \delta) \qquad (1)$$

(A4) $\quad \big(\varphi \Rightarrow (\sigma \Rightarrow \tau)\big) \Rightarrow \big((\varphi \Rightarrow \sigma) \Rightarrow (\varphi \Rightarrow \tau)\big)$

Wähle $\varphi \coloneqq \alpha, \sigma \coloneqq \gamma, \tau \coloneqq \delta$:

$$\big(\alpha \Rightarrow (\gamma \Rightarrow \delta)\big) \Rightarrow \big((\alpha \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \delta)\big)$$

M. .p. liefert mit Hilfe von (1):

$$\Sigma \vdash (\alpha \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \delta) \qquad (2)$$

Analog kann man zeigen:

$$\Sigma \vdash (\alpha \Rightarrow \delta) \Rightarrow (\alpha \Rightarrow \gamma) \qquad (3)$$

Folglich ((2), (3))

$$\alpha \Rightarrow \gamma \approx \alpha \Rightarrow \delta \qquad (4)$$

(A3) $\quad (\varphi \Rightarrow \sigma) \Rightarrow \big((\sigma \Rightarrow \tau) \Rightarrow (\varphi \Rightarrow \tau)\big)$

Wähle $\varphi \coloneqq \beta, \sigma \coloneqq \alpha, \tau = \delta$

$$(\beta \Rightarrow \alpha) \Rightarrow \big((\alpha = \delta) \Rightarrow (\beta \Rightarrow \delta)\big)$$

M. p. liefert:

$$(\alpha \Rightarrow \delta \Rightarrow (\beta \Rightarrow \delta) \qquad (5)$$

Analog erhält man

$$\Sigma \vdash (\beta \Rightarrow \delta) \Rightarrow (\alpha \Rightarrow \delta) \qquad (6)$$

Also:

$$\alpha \Rightarrow \delta \approx \beta \Rightarrow \delta \qquad (7)$$

Folglich (wegen Transitivität von $\approx$ und (4), (7))

$$\alpha \Rightarrow \gamma \approx \beta \Rightarrow \delta,$$

d.h. $\approx$ ist mit $\Rightarrow$ verträglich.

Zwecks Nachweis der Verträglichkeit von $\approx_\Sigma$ mit $\wedge$ und $\vee$ betrachten wir die folgende Relation $\leq_\Sigma$, von der wir anschließend zeigen, dass sie eine reflexive Halbordnung auf $F_{/\approx_\Sigma}$ (Menge aller Äquivalenzklassen von $\approx_\Sigma$) ist.

[XXX: Bild]

Def.:

$[\alpha]_{\approx_\Sigma} \leq_\Sigma [\beta]_{\approx_\Sigma}$ genau dann, wenn $\Sigma \vdash \alpha \Rightarrow \beta$

Wegen

$$\text{(A1)} \qquad \varphi \Rightarrow \varphi$$

ist $\leq_\Sigma$ reflexiv.

Wegen

$$\text{(A3)} \qquad (\alpha \Rightarrow \beta) \Rightarrow \big((\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma)\big)$$

ist $\leq_\Sigma$ transitiv.

Die Antisymmetrie folgt aus der Def. von $\approx_\Sigma$:

Sei $[\alpha]_{\approx_\Sigma} \leq [\beta]_{\approx_\Sigma}$, d. h. $\Sigma \vdash \alpha \Rightarrow \beta$

Angenommen, $\Sigma \vdash \beta \Rightarrow \alpha$

Dann $\alpha \approx_\Sigma \beta$

Also $[\alpha]_{\approx_\Sigma} = [\beta]_{\approx_\Sigma}$, d. h. $\leq_\Sigma$ ist reflexive Halbordnung.

Zeigen nun die Verträglichkeit von $\approx_\Sigma$ mit $\wedge$ und $\vee$:

$$\text{(A5)} \qquad \alpha \Rightarrow (\alpha \vee \beta), \qquad \beta \Rightarrow (\alpha \vee \beta)$$

Liefert

$$[\alpha] \leq [\alpha \vee \beta], \qquad [\beta] \leq [\alpha \vee \beta]$$

(Hier und weiter unten benutzen wir die Kurzschreibweise $[\dots] \coloneqq [\dots]_{\approx_\Sigma}$ sowie $\leq \coloneqq \leq_\Sigma$)

Angenommen, es existiert ein γ mit $[\alpha] \leq [\gamma]$ (d. h. $\Sigma \vdash \alpha \Rightarrow \gamma$) und $[\beta] \leq [\gamma]$ (d. h. $\Sigma \vdash \beta \Rightarrow \gamma$).

Wegen

$$\text{(A6)} \qquad (\alpha \Rightarrow \gamma) \Rightarrow ((\beta \Rightarrow \gamma) \Rightarrow \big((\alpha \vee \beta_{\Rightarrow \gamma})\big)$$

und M. p. folgt hieraus

$$[\alpha \vee \beta] \leq [\gamma]$$

womit

$$\sup([\alpha], [\beta]) \eqqcolon \{\alpha] \vee [\beta] = [\alpha \vee \beta]$$

Analog folgt aus (A7) und (A8):

$$\inf([\alpha], [\beta]) \eqqcolon [\alpha] \wedge [\beta] = [\alpha \wedge \beta]$$

Also ist $\approx_\Sigma$ mit $\wedge$ und $\vee$ verträglich.

■

Aus dem oben Gezeigten folgt

3. Behauptung:

$(F_{/\approx_\Sigma}; \leq_\Sigma)$ ist Verband.

■

4. Behauptung:

$(F_{/\approx_\Sigma}; \leq_\Sigma)$ ist distributiver Verband.

Beweis:

Die Behauptung folgt aus

$$\begin{array}{rl} \text{(A9)} & \big((\alpha \wedge \beta) \vee \gamma\big) \Rightarrow \big((\alpha \vee \gamma) \wedge (\beta \vee \gamma)\big) \\ & (\alpha \vee \gamma) \wedge (\beta \vee \gamma) \Rightarrow \big((\alpha \wedge \beta) \vee \gamma\big) \\ \text{(A10)} & \big((\alpha \vee \beta) \wedge \gamma\big) \Rightarrow \big((\alpha \wedge \gamma) \vee (\beta \wedge \gamma)\big) \\ & \big((\alpha \wedge \gamma) \vee (\beta \wedge \gamma)\big) \Rightarrow \big((\alpha \vee \beta) \wedge \gamma\big) \end{array}$$

■

5. Behauptung:

$\big(F_{/\approx_\Sigma}; \vee, \wedge, \neg, [\overbrace{\alpha \wedge \bar{\alpha}}^{\alpha \wedge (\neg \alpha)}]_{\approx_\Sigma}, \{\alpha | \Sigma \vdash \alpha\}\big)$ ist Boolesche Algebra

Beweis:

Bereits gezeigt: $\big(F_{/\approx_\Sigma}; \wedge, \vee\big)$ ist distributiver Verband.

Noch zu zeigen:

$[\alpha \wedge \bar{\alpha}]_{\approx_\Sigma}$ ist kleinstes Element („0“)

$\{\alpha | \Sigma \vdash \alpha\}$ ist größtes Element („1“)

dieses Verbandes und es gilt:

$$\begin{array}{llll} (B_2) & x \wedge „0“ = „0“, & x \vee „1“ = „1“ \\ (B_3) & x \wedge \bar{x} = „0“, & x \vee \bar{x} = „1“ \end{array}$$

Wegen

$$\text{(A12)} \qquad (\alpha \wedge \neg \alpha) \Rightarrow \beta$$

Ist $[\alpha \wedge \bar{\alpha}]_{\approx_\Sigma}$ kleinstes Element.

Wegen

$$\text{(A2)} \qquad \alpha \Rightarrow (\beta \Rightarrow \alpha)$$

gilt für alle $\beta \in F$ und alle $\alpha \in F$ mit $\Sigma \vdash \alpha$

$$\Sigma \vdash \beta \Rightarrow \alpha$$

d. h.

$$[\beta]_{\approx_\Sigma} \leq [\alpha]_{\approx_\Sigma}$$

Also ist $\{\alpha | \Sigma \vdash \alpha\}$ die „1“ von $F_{/\approx_\Sigma}$.

(B_2) ist klar, da oben gezeigt wurde, dass $1 = \inf, v = \sup$ und „0“ (bzw. „1“) kleinstes (bzw. größtes Element) sind.

(B_3) erhält man aus

$$\text{(A13)} \qquad \beta \Rightarrow (\alpha \vee \neg \alpha)$$

wie folgt:

$$[\alpha] \wedge [\beta] = [\alpha \wedge (\neg \alpha)] \equiv „0“$$
$$[\alpha] \vee [\{\neg \alpha)] = [\alpha \vee (\neg \alpha)] \equiv „1“$$

(wegen $[\beta] \leq [\alpha \vee \neg \alpha]$

■

[XXX: fehlt was]

6. Behauptung:

[XXX: fehlt was]

(a) Es existiert eine homomorphe [XXX: gnah]

(b) Es existiert eine Belegung (Bewertung) u von F mit $u(\varphi) = 0$ und $u(\alpha) = 1$ für alle $\alpha \in \Sigma$.

Beweis:

(a) Die Abbildung

$$f: F \to F_{/\approx_\Sigma}, \qquad \alpha \mapsto [\alpha]_{\approx_\Sigma}$$

ist nach Behauptung 2 eine homomorphe Abbildung.
Eine homomorphe Abbildung

$$g: F_{/\approx_\Sigma} \to \{0, 1\}$$

mit $g([\varphi]) = 0$ *und* $g(„1“) = 1$.
[XXX: fehlt was]

(b) Da für alle Belegungen (Bewertungen)

$$u: F \to \{0, 1\}$$

die Gleichung

$$u(\alpha \Rightarrow \beta) = u(\bar{\alpha} \vee \beta)$$

gilt, folgt (b) aus (a).

■

Nach all diesen Vorbereitungen lässt sich

$$\operatorname{cons} \Sigma = \operatorname{Cons} \Sigma$$

wie folgt beweisen: Angenommen, $\operatorname{cons} \Sigma \underset{\neq}{\subset} \operatorname{Cons} \Sigma$.
Dann existiert $\varphi \in \operatorname{Cons} \Sigma \setminus \operatorname{cons} \Sigma$, d. h. $\Sigma \vDash \varphi$ und $\Sigma \nvdash \varphi$, d. h. $\varphi \notin „1“$. Wegen der 6. Behauptung (6) existiert folglich eine Belegung u von F mit $u(\varphi) = 0$ und $u(\alpha) = 1$ für alle $\alpha \in \Sigma$, was wegen [XXX: juhu]

Def.:

Σ heißt *erfüllbar*, genau dann, wenn $\exists$ Belegung $u\colon F \to \{0,1\}$ [XXX: toll]

Beispiel:

$$\Sigma = \{\underbrace{\big(A \lor (B \land C)\big)}_{\alpha}, \underbrace{(B \Rightarrow \bar{C})}_{\beta}\}$$

[XXX: Tabelle]

Def.:

$\Sigma \subseteq F$
Σ heißt *widerspruchsvoll*, genau dann, wenn Σ *nicht* erfüllbar.

Als nächstes suchen wir äquivalente Bedingungen zu *„Σ ist erfüllbar"*.

Def.:

$\Sigma \subseteq F$
Σ heißt *konsistent*, genau dann, wenn $\forall \alpha \in F\colon \Sigma \nvdash (\alpha \land \neg\alpha)$.

Beispiel:

$$\Sigma = \{A, \underbrace{(\alpha \lor \neg\alpha) \Rightarrow \big(\alpha \land (\neg\alpha)\big)}_{=:\,\gamma}\}$$

$$\frac{\dfrac{(\text{A13}),\quad \beta}{\alpha \lor \neg\alpha}\ \text{M. p.} \qquad \begin{matrix}(\text{A13})\\ \beta \Rightarrow (\alpha \lor \neg\alpha)\end{matrix}}{}$$

$$\frac{(\alpha \lor \neg\alpha),\quad \gamma}{\alpha \land (\neg\alpha)}\ \text{M. p.}$$

Also: Σ ist *nicht* konsistent.

Satz 18

Folgende Bedingungen sind äquivalent:
(1) Σ ist erfüllbar
(2) Σ ist konsistent, d. h. $\forall \alpha \in F\colon (\alpha \land \bar{\alpha}) \notin \operatorname{cons}\Sigma$
(3) Jede endliche Teilmenge von Σ ist konsistent
(4) $\operatorname{cons}\Sigma \neq F$

Beweis:

$(1) \Rightarrow (2)$
Sei u Belegung von F, die Σ erfüllt.
Dann: u ist Bewertung von F, die $\operatorname{cons}\Sigma$ erfüllt.
Folglich (da $u(\alpha \land \bar{\alpha}) = u(\alpha) \land \overline{u(\alpha)} = 0$):

$$\forall \alpha \in F\colon \alpha \land \bar{\alpha} \notin \operatorname{cons}\Sigma$$

$(2) \Rightarrow (3)$ und $(3) \Rightarrow (4)$ sind klar!
$(4) \Rightarrow (1)$
Sei $\operatorname{cons}\Sigma \neq F$
Dann gilt: $\left|F_{/\approx_\Sigma}\right| \geq 2$

[XXX: Bild]
Nach dem Primidealtheorem lässt sich F wie folgt zerlegen:
[XXX: Bild]
Folglich existieren homomorphe Abbildungen π und σ mit

$$\pi: F \to F_{/\approx_\Sigma}, \qquad \varphi \mapsto [\varphi]_{\approx_\Sigma}$$
$$\sigma: F_{/\approx_\Sigma} \to \{0,1\}$$

$\pi \,\square\, \sigma$ ist Bewertung [XXX: fehlt was]

Satz 19 (Endlichkeitssatz, Kompaktheitssatz)

Sei $\Sigma \subseteq F$. Dann gilt
(a) Falls $\Sigma \vDash \varphi$, so existiert eine *endliche* Teilmenge $\Sigma' \subseteq \Sigma$ mit $\Sigma' \vDash \varphi$.
(b) Σ ist erfüllbar, genau dann, wenn: *jede endliche* Teilmenge von Σ ist erfüllbar
(c) Σ ist widerspruchsvoll, genau dann, wenn: *es existiert eine endliche* Teilmenge von Σ, die widerspruchsvoll ist.

Beweis:

(a) $\varphi \in \operatorname{Cons}\Sigma$
Dann folgt aus Satz 17: $\varphi \in \operatorname{cons}\Sigma$
Folglich: φ in endlich vielen Schritten mit Hilfe von (A1)–(A13), M. p. und gewissen Formeln aus Σ (und damit auch Σ') herleitbar.
[XXX: fehlt was]
(b) Hinrichtung:
Sei Σ erfüllbar
Dann (wegen Satz 18) [XXX: ergänzen]

2.5 Anwendungen des Kompaktheitssatzes

Z. B. bei Beweisen:

Satz 20

Auf *jeder* Menge M ist eine irreflexive, totale Ordnung

$$< := \{(a,b), \dots\} \subseteq M \times M$$

($a < b$ genau dann, wenn $(a,b) \in <$)
definierbar, d. h. $<$ erfüllt folgende drei Bedingungen:
(1) Für alle $x \in M$ gilt $(x,x) \notin <$.
(2) Für alle $x \neq y$ aus M gilt entweder $(x,y) \in <$ oder $(y,x) \in <$.
(3) $<$ ist transitiv.

Beweis:

Ist M eine endliche Menge, so gilt der Satz offensichtlich:

$$M := \{m_1, m_2, \dots, m_n\}, \qquad m_1 < m_2 < \dots < m_n$$

Für beliebige Mengen $M \neq \emptyset$ betrachten wir für jedes Paar $(a,b) \in M \times M$ die Aussagenvariable

$$p_{a,b}$$

Und für alle $a, b, c \in M$ die Aussagen

$$\bar{p}_{a,a}$$

$$(p_{a,b} \land p_{b,c}) \Rightarrow p_{a,c}$$
$$p_{a,b} \lor p_{b,a} \text{ für } a \neq b$$

Die wir zur Menge Σ zusammenfassen.
Z. B. für $M = \{\alpha, \beta, \gamma\}$:

$$\begin{aligned}\Sigma = \{&\bar{p}_{\alpha,\alpha}, \bar{p}_{\beta,\beta}, \bar{p}_{\gamma,\gamma},\\ &(p_{\alpha,\alpha} \land p_{\alpha,\alpha}) \Rightarrow p_{\alpha,\alpha},\\ &(p_{\alpha,\alpha} \land p_{\alpha,\beta}) \Rightarrow p_{\alpha,\beta},\\ &\vdots\\ &p_{\alpha,\beta} \lor p_{\beta,\alpha}, p_{\beta,\alpha} \lor p_{\alpha,\beta},\\ &p_{\alpha,\gamma}\end{aligned}$$

[XXX: ergänzen]

Damit ist gezeigt, dass R eine irreflexive, totale Ordnung ist.
Anwendung des Kompaktheitssatzes liefert Beweis des obigen Satzes.

■

[XXX: ergänzen]

Es gilt:

Vierfarbensatz:

Ein beliebiger *endlicher* planarer Graph ist 4-chromatisch.

Beweis wurde (nachdem über 100 Jahre seit Problemstellung vergangen waren und viele Mathematiker sich bemüht hatten, einen Beweis zu finden) 1976 mit Hilfe einer Computerberechnung von etwa 1200 Stunden (≈ 10 Mrd. Entscheidungen) erstmalig durch Appel und Meken geführt.

Eine Übertragung des Vierfarbensatzes auf *un*endliche Graphen ist dagegen leicht:

Sei $G = (V; E)$ planarer Graph, wobei V beliebige nichtleere Menge.
Betrachten Aussagenvariable
[XXX: ergänzen]
Falls Σ durch Bewertung u erfüllbar ist, besagt

(1) Jeder Knoten $\in V$ gehört zu einer Färbungsklasse $C_i: a \in C_i$ genau dann, wenn $u(p_{i,a}) = 1$.
(2) Die Mengen C_1, C_2, C_3, C_4 sind paarweise disjunkt.
(3) Benachbarte Knoten haben nicht die selbe Farbe

Wegen des Vierfarbensatzes ist jede *endliche* Teilmenge von Σ erfüllbar. Womit der Vierfarbensatz (laut Kompaktheitssatz) auch für unendliche Graphen gilt.

Satz 22 (Deduktionstheorem)

(D_1) $\Sigma \cup \{\psi\} \vdash \varphi$ genau dann, wenn $\Sigma \vdash (\psi \Rightarrow \varphi)$
(D_2) $\Sigma \vdash \varphi$ genau dann, wenn $\exists \psi_1, \dots, \psi_n \in \Sigma: \emptyset \vdash ((\psi_1 \land \psi_2 \land \dots \land \psi_n) \Rightarrow \varphi)$

Beweis:

(D_1)

Hinrichtung:

Sei $\Sigma \vdash (\psi \Rightarrow \varphi)$

Damit (M. p.):

$$\frac{\psi, \quad (\psi \Rightarrow \varphi)}{\varphi}$$

Also:$\Sigma \cup \{\psi\} \vdash \varphi$

Rückrichtung:

Sei $\Sigma \cup \{\psi\} \vdash \varphi$, d. h., φ ist eine Ableitung aus $\Sigma \cup \{\psi\}$.

Nach Def. können in dieser Ableitung nur endlich viele Formeln

$$\psi_1, \dots, \psi\_n \in \Sigma$$

Vorkommen.

Damit: $\{\psi_1, \dots, \psi_n, \psi\} \vdash \varphi$

Und $(\psi_1 \wedge \dots \wedge \psi_n) \Rightarrow (\psi \Rightarrow \varphi)$ ist Tautologie. Da eine Tautologie aus Σ ableitbar, folgt mittels M. p. die Behauptung:

Wegen $\psi_1, \dots, \psi\_n \in \Sigma$ und $\vdash = \vDash$ gilt

$$\Sigma \vdash \psi_1 \wedge \psi_2 \wedge \dots \wedge \psi_n$$

Damit

$$\frac{\psi_1 \wedge \psi_2 \wedge \dots \wedge \psi_n, \quad ((\psi_1 \wedge \dots \wedge \psi_n) \Rightarrow (\psi \Rightarrow \varphi)}{\psi \Rightarrow \varphi} \text{ M. p.}$$

Also: $\Sigma \vdash (\psi \Rightarrow \varphi)$

(D_2)

Hinrichtung:

Sei $\Sigma \vdash \varphi$, d. h., es existiert eine Ableitung von φ aus gewissen Formeln $\psi_1, \dots, \psi_n \in \Sigma$. Nach Definition einer abgeleiteten Formel bedeutet dies, dass

$$(\psi_1 \wedge \dots \wedge \psi_n) \Rightarrow \varphi$$

Eine Tautologie ist.

Also gilt: $\emptyset \vdash \big((\psi_1 \wedge \dots \wedge \psi_n) \Rightarrow \varphi\big)$

Rückrichtung:

Für gewissen $\psi_1, \dots, \psi_n \in \Sigma$ sei $\big((\psi_1 \wedge \dots \wedge \psi_n) \Rightarrow \varphi\big)$ eine Tautologie. Dies geht nur, wenn für jede Belegung u mit

$$u(\psi_1) = \cdots = u(\psi_n) = 1$$

Stets $u(\varphi) = 1$ gilt.

Folglich gilt für jede Belegung u' mit $u'(\psi) = 1$ für alle $\psi \in \Sigma$ auch $u'(\varphi) = 1$, d. h. $\Sigma \vDash \varphi$ bzw. $\Sigma \vdash \varphi$.

■

Für $\Sigma = \emptyset$ erhält man aus obigem Satz

(D) $\quad \psi \vdash \varphi$ genau dann, wenn $\vdash (\psi \Rightarrow \varphi)$

(D) kann man benutzen, um Tautologien ohne viel Aufwand zu gewinnen. Dazu

Beispiele:

1. $p \Rightarrow (q \Rightarrow p)$ ist Tautologie
   Wegen

$\vdash \left(p \Rightarrow (q \Rightarrow p)\right)$ genau dann, wenn $p \vdash (q \Rightarrow p)$ genau dann, wenn $\{p, q\} \vdash p$

2. $\left(\left((p \Rightarrow q) \Rightarrow r\right) \Rightarrow \left((p \Rightarrow q) \Rightarrow (p \Rightarrow r)\right)\right) =: \alpha$ ist Tautologie wegen
$\vdash \alpha$ genau dann, wenn $\left((p \Rightarrow q) \Rightarrow r\right) \vdash \left((p \Rightarrow q) \Rightarrow (q \Rightarrow r)\right)$ genau dann, wenn $\left\{\left((p \Rightarrow q) \Rightarrow r\right), (p \Rightarrow q)\right\} \vdash p \Rightarrow r$
[XXX: ergänzen]