VII: Boole'sche Algebren

Freitag, 5. Januar 2024 10:10

Eine Menge B mit den Operationen $\vee, \wedge : B \times B \to B$ und eine Abbildung $\bar{\ } : B \to B$
(schreibe $\bar{x}$ statt $\bar{\ }(x)$, sprich „x quer" oder „x-Komplement", $\vee$ „sup", $\wedge$ „inf")
heißt Boole'sche Algebra, falls gilt:

(I) $a \vee b = b \vee a \quad \forall a,b \in B$
$a \wedge b = b \wedge a \quad \forall a,b \in B$ } $\wedge, \vee$ sind kommutativ

(II) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad \forall a,b,c \in B$
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad \forall a,b,c \in B$ } $\vee, \wedge$ sind wechselseitig distributiv

(III) es existiert $\perp$ (Bottom-Element) mit $a \vee \perp = \perp \vee a = a \quad \forall a \in B$
es existiert $\top$ (Top-Element) mit $a \wedge \top = \top \wedge a = a \quad \forall a \in B$ } neutrale Elemente

(IV) $a \vee \bar{a} = \top \quad \forall a \in B$
$a \wedge \bar{a} = \perp \quad \forall a \in B$ } Inverse

$\Longrightarrow$ Assoziativität folgt aus Eigenschaften

Bsp: M - Menge, $B := \mathcal{P}(M)$, $a \vee b := a \cup b$, $a \wedge b := a \cap b$, $\bar{a} = M \setminus a$
definiert eine Boole'sche Algebra mit $\perp = \emptyset$, $\top = M$

$B = \{0,1\}^m$, Operationen $+, \cdot$, $\bar{0} = 1$, $\bar{1} := 0$

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

Setze $+, \cdot$ fort auf ganz B

$(a_1, \dots, a_m) + (b_1, \dots, b_m) = (a_1 + b_1, \dots, a_m + b_m)$

$(a_1, \dots, a_m) \cdot (b_1, \dots, b_m) = (a_1 \cdot b_1, \dots, a_m \cdot b_m)$

$\overline{(a_1, \dots, a_m)} = (\bar{a}_1, \dots, \bar{a}_m)$

B mit $+, \cdot, \bar{\ }$ ist auch eine Boole'sche Algebra mit $\perp = (0, \dots, 0)$ und $\top = (1, \dots, 1)$

(Prototypen Boole'scher Algebren)

$f = (a_0, a_1, \dots)$, $f = \sum_{k \in \mathbb{N}} a_k x^k$ in $R[[x]]$

$\operatorname{supp} f = \{k \in \mathbb{N} : a_k \neq 0\}$

Sei $R[x] = \{f \in R[[x]] : \operatorname{supp} f \text{ endlich}\}$ (Polynome)

$R[x]$ ist Unterring von $R[[x]]$, dies folgt aus dem Beweis der folgenden Gradformel

Satz (Gradformeln)

Für $f \in R[x]$, $f \neq 0$, sei $\operatorname{grad} f := \max(\operatorname{supp} f)$ der Grad von f, $f(\operatorname{grad} f)$ heißt Leitkoeffizient von f.

Für f, g aus $R[x] \setminus \{0\}$ gilt

(I) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\}$, falls $f+g \neq 0$

(II) $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$, falls $f \cdot g \neq 0$, mit „=" genau dann, wenn $f(\operatorname{grad} f) \cdot g(\operatorname{grad} g) \neq 0$

Bew:

(I) Für $k > \max\{\operatorname{grad} f, \operatorname{grad} g\}$ ist $k > \operatorname{grad} f$ und $k > \operatorname{grad} g$, also $f(k) = 0$ und $g(k) = 0$, also $(f+g)(k) = 0$
$\to \operatorname{supp}(f+g) \subseteq \{0, 1, \dots, \max\{\operatorname{grad} f, \operatorname{grad} g\}\} \to f+g \in R[x]$ und $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\}$

(II) Für $k = i+j$ und $k > \operatorname{grad} f + \operatorname{grad} g$ ist $i > \operatorname{grad} f$ oder $j > \operatorname{grad} g$, also $f(i) = 0$ oder $g(j) = 0$, also $f(i) \cdot g(j) = 0$
$\to (f \cdot g)(k) = \sum_{\substack{i,j \geq 0 \\ i+j=k}} f(i) \cdot g(j) = 0 \to \operatorname{supp}(f \cdot g) \subseteq \{0, 1, \dots, \operatorname{grad} f + \operatorname{grad} g\} \to f \cdot g \in R[x]$ und $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$

Für $k = i+j = \operatorname{grad} f + \operatorname{grad} g$ ist $(f \cdot g)(k) = \sum_{\substack{i,j \geq 0 \\ i+j=k}} \underbrace{f(i) \cdot g(j)}_{\substack{\neq 0 \text{ nur} \\ \text{für } i \leq \operatorname{grad} f \\ \text{und } j \leq \operatorname{grad} g}} = f(\operatorname{grad} f) \cdot g(\operatorname{grad} g)$. Dies zeigt (II). $\square$

Alle anderen Eigenschaften vererben sich.

Wichtiger Spezialfall: Ist R ein Körper, folgt aus $a \cdot b = 0$, stets $a = 0$ oder $b = 0$ (für $a, b \in R$)
Also ist für $f, g \in R[x] \setminus \{0\}$ auch $f \cdot g \neq 0$ und $\underset{\neq 0}{f(\operatorname{grad} f)} \cdot \underset{\neq 0}{g(\operatorname{grad} g)} \neq 0$
$\to$ „=" in (II)

Satz von der Division mit Rest für Polynomringe

Sei K Körper. Zu $a, b \in K[x]$ mit $b \neq 0$ existieren eindeutig bestimmte andere Polynome $q, r \in K[x]$ mit $a = q \cdot b + r$ und $r = 0$ oder $\operatorname{grad} r < \operatorname{grad} b$.

Bew.: Existenz: Für $a = 0$ oder $\operatorname{grad} a < \operatorname{grad} b$ nimm $q = 0$ und $r := a$

Für $\operatorname{grad} a \geq \operatorname{grad} b$ betrachte $p := a(\operatorname{grad} a) \cdot (b(\operatorname{grad} b))^{-1} \cdot x^{\operatorname{grad} a - \operatorname{grad} b}$

$\to \operatorname{grad}(\underbrace{a - p \cdot b}_{:= a'}) < \operatorname{grad} a$ oder $a - p \cdot b = 0$

$a = (1, 2, \dots, 3, 7, -1, \overset{\text{LK}}{17}, 0, 0, 0, \dots)$

$b = (0, 3, \dots, 4, \underset{\text{LK}}{19}, 0, 0, 0, \dots)$

$\underbrace{\qquad}_{\substack{\operatorname{grad} a - \operatorname{grad} b \\ = 2}}$

$p = \frac{17}{19} x^2 = (0, 0, \frac{17}{19}, 0, 0, 0, \dots)$

$p \cdot b = \frac{17}{19} \cdot (0, 0, 0, 3, \dots, 4, 19, 0, 0, 0, \dots)$

$= (0, 0, 0, 3 \cdot \frac{17}{19}, \dots, 4 \cdot \frac{17}{19}, 17, 0, 0, 0, \dots)$

$a - p \cdot b = (1, 2, \dots, -1 - 4 \cdot \frac{17}{19}, 0, 0, 0, \dots)$

Induktion
$\to$ es gibt $q', r' \in K[x]$ mit $a' = q' \cdot b + r'$ und $r' = 0$ oder $\operatorname{grad} r' < \operatorname{grad} b$

$\to a = a' + pb = q' \cdot b + r' + pb = (q' + p) \cdot b + r' \to q = q' + p$ und $r' = r$

Eindeutigkeit: Gelte $a = q \cdot b + r$ und $r = 0$ oder $\operatorname{grad} r < \operatorname{grad} b$
und $a = q' \cdot b + r'$ und $r' = 0$ oder $\operatorname{grad} r' < \operatorname{grad} b$

z.z.: $q = q'$ und $r = r'$

$\to 0 = (q - q') \cdot b + (r - r')$ (Subtraktion)

Wäre $r - r' \neq 0$, so auch $(q - q') \cdot b \neq 0$, also $q - q' \neq 0$

Es ist $\operatorname{grad} b > \operatorname{grad} r \underset{\text{(I) Gradformel}}{\geq} \operatorname{grad}(r - r') = \operatorname{grad}(-(r - r')) = \operatorname{grad}((q - q') \cdot b) \geq \operatorname{grad} q - q' + \operatorname{grad} b \geq \operatorname{grad} b$ ↯ (o.B.d.A. $r \neq 0$)

Also ist $r = r' \to (q - q') \cdot b = 0 \xrightarrow{b \neq 0} q - q' = 0 \to q = q'$

$\square$

Für $f \in R[x]$ und $a \in R$

Sei $\varphi_a(f) := \sum_{k \in \mathbb{N}} f(k) \cdot a^k$. Dies definiert eine Abbildung $\varphi_a : R[x] \to R$

φ_a ist ein Ringhomomorphismus, d.h. $\varphi_a(f+g) = \varphi_a(f) + \varphi_a(g)$
und $\varphi_a(f \cdot g) = \varphi_a(f) \cdot \varphi_a(g)$

Statt $\varphi_a(f)$ schreibe auch $f(a)$, in dieser Schreibweise gilt

$(f+g)(a) = f(a) + f(g)$

$(f \cdot g)(a) = f(a) \cdot f(g)$