WS 2005/06

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2005WS/ds/index.html.de

22. November 2005

6.2 Atome

Definition 109

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

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

Satz 110

Es gilt:

1. $\text{atom}(a) \;\Rightarrow\; (\forall b \in S) \quad [a \otimes b = a \;\vee\; a \otimes b = 0]$
2. $\text{atom}(a) \wedge \text{atom}(b) \wedge a \neq b \;\Rightarrow\; a \otimes b = 0$
3. *Falls gilt:* $(\forall a \in S)[\text{atom}(a) \;\Rightarrow\; a \otimes b = 0]$, *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 111 (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:

$$x \otimes \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a \overset{\text{D-G.}}{=} \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} (x \otimes a) \overset{\text{Satz 110}}{=} \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a$$

Setze

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

Wir haben gezeigt:

$$x \otimes y = y$$

Ebenso gilt:

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

Zusammen:

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

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 $\left(\overline{S_1 \cap S_2}\right)$.

Dann gilt:

$$
\begin{aligned}
x &= x \otimes x = \Big(\bigoplus_{a \in S_1} a\Big) \otimes \Big(\bigoplus_{a \in S_2} a\Big) \\
&= \bigoplus_{\substack{a \in S_1 \\ a' \in S_2}} \underbrace{a \otimes a'}_{=0} \\
&\overset{\text{Satz 110 (2)}}{=} \bigoplus_{\substack{a \in S_1 \\ a' \in S_2}} 0 = 0,
\end{aligned}
$$

was ein Widerspruch zur Annahme ist. □

Korollar 112

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

Korollar 113

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 114

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 115

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 116

- 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 117

- $\mathbb{Q}$ (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 118

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 118 gilt sogar in Ringen.

Definition 119

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 120

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

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

(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 118 folgt damit:

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

□

2.1 Größter gemeinsamer Teiler (ggT)

Definition 121

- 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

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