Script generated by TTT

Title: Mayr: 2012 ds (20.11.2012)

Date: Tue Nov 20 13:44:00 CET 2012

Duration: 93:06 min

Pages: 42

WS 2012/13

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2012WS/ds/

Wintersemester 2012

Inhaltsverzeichnis

5.8 Transformationsgruppen

Definition 101

Eine Transformationsgruppe ist eine Gruppe von bijektiven Abbildungen einer Menge U auf sich selbst mit der Komposition $\circ$ als binärem Operator:

$$g \circ f : U \ni x \mapsto g(f(x)) \in U$$

Satz 102 (Darstellungssatz für Gruppen)

Jede Gruppe ist isomorph zu einer Transformationsgruppe.

Beweis:

Sei $G = (S, \circ, 1)$, $g \in G$. Betrachte die Abbildung

$$\tilde{g} : S \ni a \mapsto g \circ a \in S$$

Aus der Kürzungsregel und der Existenz eines Inversen folgt, dass $\tilde{g}$ eine bijektive Abbildung ist.

Wir betrachten nun $\tilde{G} := (\tilde{S}, \circ, \tilde{1})$ mit $\tilde{S} = \{\tilde{g};\ g \in G\}$. Die Abbildung

$$\tilde{\ } :\ S \ni g \mapsto \tilde{g} \in \tilde{S}$$

ist ein Gruppenisomorphismus. Für $h, g \in G$ gilt:

$$(\widetilde{h \circ g})(a) = (h \circ g) \circ a = h \circ (g \circ a) = h \circ \tilde{g}(a) = \tilde{h}(\tilde{g}(a)) = (\tilde{h} \circ \tilde{g})(a)$$

□

Beweis:

Sei $G = (S, \circ, 1)$, $g \in G$. Betrachte die Abbildung

$$\tilde{g} : S \ni a \mapsto g \circ a \in S$$

Aus der Kürzungsregel und der Existenz eines Inversen folgt, dass $\tilde{g}$ eine bijektive Abbildung ist.

Wir betrachten nun $\tilde{G} := (\tilde{S}, \circ, \tilde{1})$ mit $\tilde{S} = \{\tilde{g};\ g \in G\}$. Die Abbildung

$$\tilde{\ } :\ S \ni g \mapsto \tilde{g} \in \tilde{S}$$

ist ein Gruppenisomorphismus. Für $h, g \in G$ gilt:

$$(\widetilde{h \circ g})(a) = (h \circ g) \circ a = h \circ (g \circ a) = h \circ \tilde{g}(a) = \tilde{h}(\tilde{g}(a)) = (\tilde{h} \circ \tilde{g})(a)$$

□

Beweis:

Sei $G = (S, \circ, 1)$, $g \in G$. Betrachte die Abbildung

$$\tilde{g} : S \ni a \mapsto g \circ a \in S$$

Aus der Kürzungsregel und der Existenz eines Inversen folgt, dass $\tilde{g}$ eine bijektive Abbildung ist.

Wir betrachten nun $\tilde{G} := (\tilde{S}, \circ, \tilde{1})$ mit $\tilde{S} = \{\tilde{g};\ g \in G\}$. Die Abbildung

$$\tilde{\ } :\ S \ni g \mapsto \tilde{g} \in \tilde{S}$$

ist ein Gruppenisomorphismus. Für $h, g \in G$ gilt:

$$(\widetilde{h \circ g})(a) = (h \circ g) \circ a = h \circ (g \circ a) = h \circ \tilde{g}(a) = \tilde{h}(\tilde{g}(a)) = (\tilde{h} \circ \tilde{g})(a)$$

□

5.9 Permutationsgruppen

Definition 103

Eine Permutation ist eine bijektive Abbildung einer endlichen Menge auf sich selbst; o. B. d. A. sei dies die Menge $U := \{1, 2, \ldots, n\}$.

S_n (Symmetrische Gruppe für n Elemente) bezeichnet die Menge aller Permutationen auf $\{1, 2, \ldots, n\}$.

Sei nun $\pi \in S_n$. Es existiert folgende naive Darstellung:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n-1) & \pi(n) \end{pmatrix}$$

Kürzer schreibt man auch

$$\pi = \begin{pmatrix} \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n-1) & \pi(n) \end{pmatrix}$$

Sei $a \in \{1,2,3,\ldots,n\}$. Betrachte die Folge

$$a = \pi^0(a),\ \pi^1(a),\ \pi^2(a),\ \pi^3(a),\ \ldots$$

Aus dem Schubfachprinzip und der Kürzungsregel folgt, dass es ein minimales $r = r(a)$ mit $r \le n$ gibt, so dass $\pi^r(a) = a$. Damit bildet

$$\left(a = \pi^0(a)\ \ \pi^1(a)\ \ \pi^2(a)\ \ \pi^3(a)\ \ \ldots\ \ \pi^{r-1}(a)\right)$$

einen Zyklus der Permutation $\pi \in S_n$.
Umgekehrt liefert

$$(a\ \ \pi^1(a)\ \ \pi^2(a)\ \ \pi^3(a)\ \ \ldots\ \ \pi^{r-1}(a))$$

eine zyklische Permutation der Zahlen

$$\{a,\ \pi^1(a),\ \pi^2(a),\ \pi^3(a),\ \ldots,\ \pi^{r-1}(a)\} \subseteq \{1,2,\ldots,n\}\,.$$

Satz 104

Sei $\pi = (a_0\ \ a_1\ \ a_2\ \ \ldots\ \ a_{n-1})$ *eine zyklische Permutation von* $\{1,2,\ldots,n\}$*, also*

$$\pi\colon\ a_i \mapsto a_{(i+1) \bmod n}$$

Dann gilt:

1. $\pi^k(a_i) = a_{(i+k) \bmod n}$
2. π *hat die Ordnung* n.

Beweis:

Satz 104

Sei $\pi = (a_0\ \ a_1\ \ a_2\ \ \ldots\ \ a_{n-1})$ *eine zyklische Permutation von* $\{1,2,\ldots,n\}$*, also*

$$\pi\colon\ a_i \mapsto a_{(i+1) \bmod n}$$

Dann gilt:

1. $\pi^k(a_i) = a_{(i+k) \bmod n}$
2. π *hat die Ordnung* n.

Beweis:

1. Leicht durch Induktion zu zeigen.
2. Aus 1. folgt: $\pi^n = \pi^0 = id$. Wäre $\operatorname{ord}\pi = m < n$, dann hätte der Zyklus die Form $(a_0\ \ a_1\ \ a_2\ \ \ldots\ \ a_{m-1})$ und a_m wäre gleich a_0, was einen Widerspruch zur Voraussetzung darstellt.

$\square$

Sei $a \in \{1,2,3,\ldots,n\}$. Betrachte die Folge

$$a = \pi^0(a),\ \pi^1(a),\ \pi^2(a),\ \pi^3(a),\ \ldots$$

Aus dem Schubfachprinzip und der Kürzungsregel folgt, dass es ein minimales $r = r(a)$ mit $r \le n$ gibt, so dass $\pi^r(a) = a$. Damit bildet

$$\left(a = \pi^0(a)\ \ \pi^1(a)\ \ \pi^2(a)\ \ \pi^3(a)\ \ \ldots\ \ \pi^{r-1}(a)\right)$$

einen Zyklus der Permutation $\pi \in S_n$.
Umgekehrt liefert

$$(a\ \ \pi^1(a)\ \ \pi^2(a)\ \ \pi^3(a)\ \ \ldots\ \ \pi^{r-1}(a))$$

eine zyklische Permutation der Zahlen

$$\{a,\ \pi^1(a),\ \pi^2(a),\ \pi^3(a),\ \ldots,\ \pi^{r-1}(a)\} \subseteq \{1,2,\ldots,n\}\,.$$

Satz 105

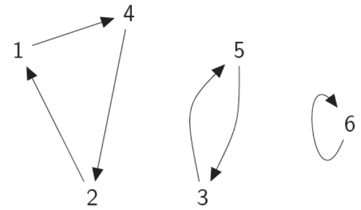
Jede Permutation aus S_n kann als Komposition (von endlich vielen) disjunkten Zyklen dargestellt werden.

Beweis:

Übung! □

Beispiel 106

$\pi = (1\ 4\ 2)(3\ 5)(6)$



In diesem Beispiel ist (6) ein Fixpunkt und $(3\ 5)$ eine Transposition (eine Permutation, die nur 2 Elemente vertauscht und alle anderen auf sich selbst abbildet).

Bemerkung:

Disjunkte Zyklen können vertauscht werden.

Korollar 107

Die Ordnung einer Permutation π ist das kgV der Längen ihrer Zyklen.

6. Boolesche Algebren

6.1 Definitionen

Eine Boolesche Algebra ist eine Algebra

$$(S, \oplus, \otimes, \sim, 0, 1),$$

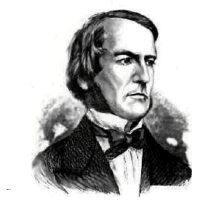
$\oplus, \otimes$ sind binäre, $\sim$ ist ein unärer Operator, 0 und 1 sind Konstanten. Es gilt:

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

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

Satz 109 (Forts.)

5. *eindeutiges Komplement:*
$$(\forall b, c \in S)\Big[b \oplus c = 1 \ \wedge \ b \otimes c = 0 \iff c = \sim b\Big]$$
6. *Involution:*
$$(\forall b \in S)\Big[\sim(\sim b) = b\Big]$$
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. □

6. Boolesche Algebren

6.1 Definitionen

Eine Boolesche Algebra ist eine Algebra

$$(S, \oplus, \otimes, \sim, 0, 1),$$

$\oplus, \otimes$ 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:
$$\begin{aligned} b \otimes (c \oplus d) = (b \otimes c) \oplus (b \otimes d) \\ b \oplus (c \otimes d) = (b \oplus c) \otimes (b \oplus d) \end{aligned}$$

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.]

□

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

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

$$\begin{aligned} a \leq b &\iff a \otimes b = a \\ a < b &\iff a \leq b \ \wedge \ a \neq b \end{aligned}$$

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

$$\begin{aligned} a \leq b &\iff a \otimes b = a \\ a < b &\iff a \leq b \ \wedge \ a \neq b \end{aligned}$$

Satz 111

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

Beweis:

$\square$

Satz 111

Durch $\le$ 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 $a \le a$, d. h. $a \otimes a = a$ (Idempotenzgesetz bzgl. $\otimes$)

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

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

$\square$

6.2 Atome

Definition 112

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

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

Satz 113

Es gilt:

6.2 Atome

Definition 112

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

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

Satz 113

Es gilt:

1. $\mathrm{atom}(a) \ \Rightarrow \ (\forall b \in S) \quad [a \otimes b = a \ \vee \ a \otimes b = 0]$
2. $\mathrm{atom}(a) \wedge \mathrm{atom}(b) \wedge a \ne b \ \Rightarrow \ a \otimes b = 0$
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):

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

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 $(S, \oplus, \otimes, \sim, 0, 1)$ 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:

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

Setze

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

Beweis:

Es gilt:

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

Setze

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

Beweis (Forts.):

Wir haben gezeigt:

$$x \otimes y = y$$

Ebenso gilt:

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

Zusammen:

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

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.):

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:

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

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 $A = (S, \oplus, \otimes, \sim, 0, 1)$ mit n Atomen ist isomorph zur Potenzmengenalgebra

$$\mathcal{P}_n := (2^{\{1,\ldots,n\}}, \cup, \cap, \bar{}, \emptyset, \{1,\ldots,n\})$$

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). □

Korollar 115

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

Korollar 116

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

$$\mathcal{P}_n := (2^{\{1,\ldots,n\}}, \cup, \cap, \bar{}, \emptyset, \{1,\ldots,n\})$$

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). □

Diskrete Strukturen
©Ernst W. Mayr
187/187

Korollar 115

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

Korollar 116

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

$$\mathcal{P}_n := (2^{\{1,\ldots,n\}}, \cup, \cap, \bar{}, \emptyset, \{1,\ldots,n\})$$

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). □