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 $r \leq n$ 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:

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.

$\square$

Satz 105

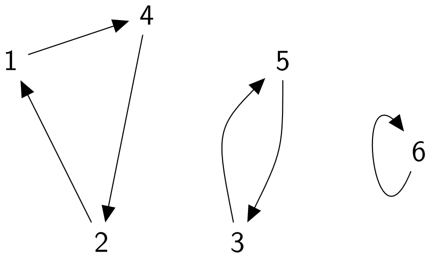
Jede Permutation aus S_n kann als Komposition (von endlich vielen) disjunkten Zyklen dargestellt werden.

Beweis:

Übung! $\square$

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

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

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

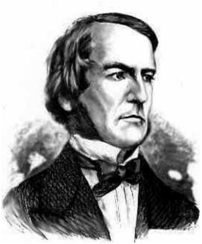
1. $\oplus$ und $\otimes$ sind assoziativ und kommutativ.
2. 0 ist Einselement für $\oplus$, 1 ist Einselement für $\otimes$.
3. für $\sim$ gilt:
$$\begin{aligned} b \oplus \sim b &= 1 \\ b \otimes \sim b &= 0 \quad \forall b \in S. \end{aligned}$$
4. Distributivgesetz:
$$\begin{aligned} b \otimes (c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

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

Beispiel 108

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

George Boole (1815–1864)



George Boole

lived from 1815 to 1864

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

Satz 109 (Eigenschaften Boolescher Algebren)

1. *Idempotenz:*
$$(\forall b \in S)\Big[b \oplus b = b \quad \wedge \quad b \otimes b = b\Big]$$
2. *Nullelement:*
$$(\forall b \in S)\Big[b \oplus 1 = 1 \quad \wedge \quad b \otimes 0 = 0\Big]$$
3. *Absorption:*
$$(\forall b, c \in S)\Big[b \oplus (b \otimes c) = b \quad \wedge \quad b \otimes (b \oplus c) = b\Big]$$
4. *Kürzungsregel:*
$$(\forall b, c, d \in S)\left[\begin{array}{l}(b \oplus c = b \oplus d) \wedge (\sim b \oplus c = \sim b \oplus d) \Leftrightarrow c = d \\ (b \otimes c = b \otimes d) \wedge (\sim b \otimes c = \sim b \otimes d) \Leftrightarrow c = d\end{array}\right]$$

Satz 109 (Forts.)

5. *eindeutiges Komplement:*

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

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. $\square$

Folgende Hilfsbehauptung ist sehr nützlich:

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

Beweis:

[Es werden nur Teile des Satzes bewiesen.]

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

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

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

$\square$

Beobachtung:

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

Da die Axiome unter Dualität abgeschlossen sind, folgt:

Das Duale eines Satzes ist wieder ein Satz.

Definition 110

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

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

Satz 111

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

Beweis:

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

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

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

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

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

$\square$