Algebra für Informationssystemtechniker

Prof. Dr. Ulrike Baumann

Fachrichtung Mathematik

Institut für Algebra

www.math.tu-dresden.de/∼baumann

Ulrike.Baumann@tu-dresden.de

07.05.2018

10. Vorlesung

- Permutationsgruppen
- Zyklenschreibweise für Permutationen
- Darstellung von Permutationen als Produkt von Transpositionen
- Signum (Vorzeichen) von Permutationen
- Beispiel aus der Codierungstheorie

Permutationsgruppen

- Eine bijektive Abbildung einer Menge $X \neq \emptyset$ auf sich heißt **Permutation** auf X.
  Das Produkt (die Hintereinanderausführung) $\circ$ von Permutationen α, β auf einer Menge X ist wie folgt definiert:

  $$\forall x \in X : \ (\alpha \circ \beta)(x) := \alpha(\beta(x))$$

  ($\alpha \circ \beta$ wird gelesen: α nach β)

- Mit S_X wird die Menge aller Permutationen auf X bezeichnet.
  Für $|X| = n$ ist $S_n := S_X$.

- $(S_n, \circ)$ ist eine Gruppe.

- Die Gruppe $(S_n, \circ)$ (kurz: S_n) wird **symmetrische Gruppe vom Grad n** genannt.

- Die Untergruppen der symmetrischen Gruppe S_n heißen **Permutationsgruppen**.

Zyklenschreibweise für Permutationen

- Jede Permutation auf einer endlichen Menge lässt sich als Produkt disjunkter Zyklen schreiben:
- $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 7 & 3 & 5 & 6 & 1 & 9 & 8 \end{pmatrix} \in S_9$

  Zyklenschreibweise:

  $\alpha = (12437)(5)(6)(89)$ bzw.
  $\alpha = (12437)(89) = (89)(12437) \in S_9$.
  $\beta = (123)(45)(6789) \in S_9$

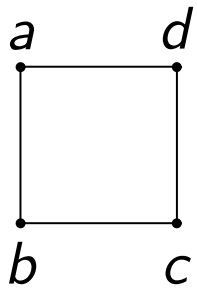
- Die Berechnung des Produktes ist auch in Zyklenschreibweise möglich:

  $\alpha \circ \beta = (14532796)$ $\qquad$ $\beta \circ \alpha = (13867254)$

- Im Falle disjunkter Zyklen ist die Reihenfolge der Hintereinanderausführung vertauschbar, z.B.:

  $(12437)(89) = (12437) \circ (89) = (89) \circ (12437) = (89)(12437)$

Symmetrieabbildungen des Quadrats



- Das Quadrat hat 8 Symmetrieabbildungen (Drehungen und Spiegelungen):

$$\begin{aligned} \mathrm{id} \qquad & \sigma := (a\,d)(b\,c) \\ \delta := (a\,b\,c\,d) \qquad & \delta \circ \sigma = (b\,d) \\ \delta^2 = (a\,c)(b\,d) \qquad & \delta^2 \circ \sigma = (a\,b)(c\,d) \\ \delta^3 = (a\,d\,c\,b) \qquad & \delta^3 \circ \sigma = (a\,c) \end{aligned}$$

- Die Symmetriegruppe des Quadrats ist eine Permutationsgruppe der Ordnung 8 (Diedergruppe D_4).

Symmetriegruppe des Quadrats

$\circ$	id	δ	δ^2	δ^3	σ	$\delta \circ \sigma$	$\delta^2 \circ \sigma$	$\delta^3 \circ \sigma$
id	id	δ	δ^2	δ^3	σ	$\delta \circ \sigma$	$\delta^2 \circ \sigma$	$\delta^3 \circ \sigma$
δ	δ	δ^2	δ^3	id	$\delta \circ \sigma$	$\delta^2 \circ \sigma$	$\delta^3 \circ \sigma$	σ
δ^2	δ^2	δ^3	id	δ	$\delta^2 \circ \sigma$	$\delta^3 \circ \sigma$	σ	$\delta \circ \sigma$
δ^3	δ^3	id	δ	δ^2	$\delta^3 \circ \sigma$	σ	$\delta \circ \sigma$	$\delta^2 \circ \sigma$
σ	σ	$\delta^3 \circ \sigma$	$\delta^2 \circ \sigma$	$\delta \circ \sigma$	id	δ^3	δ^2	δ
$\delta \circ \sigma$	$\delta \circ \sigma$	σ	$\delta^3 \circ \sigma$	$\delta^2 \circ \sigma$	δ	id	δ^3	δ^2
$\delta^2 \circ \sigma$	$\delta^2 \circ \sigma$	$\delta \circ \sigma$	σ	$\delta^3 \circ \sigma$	δ^2	δ	id	δ^3
$\delta^3 \circ \sigma$	$\delta^3 \circ \sigma$	$\delta^2 \circ \sigma$	$\delta \circ \sigma$	σ	δ^3	δ^2	δ	id

Transpositionen

- **Transpositionen** sind Zyklen der Länge $\ell = 2$.
- Jeder Zyklus lässt sich als Produkt von Transpositionen schreiben. Für Zyklen der Länge $\ell \geq 3$ gilt:

$$(i_1\ i_2\ i_3\ \ldots\ i_{\ell-1}\ i_\ell) = (i_1\ i_\ell) \circ (i_1\ i_{\ell-1}) \circ \cdots \circ (i_1\ i_3) \circ (i_1\ i_2)$$

- Jede Permutation einer endlichen Menge kann als Produkt von Transpositionen dargestellt werden.
- Gibt es für eine Permutation α eine Darstellung als Produkt von k_1 Transpositionen und eine Darstellung als Produkt von k_2 Transpositionen, dann gilt:

$$k_1 \pmod 2 \ = \ k_2 \pmod 2$$

Signum von Permutationen

- Jeder Permutation $\alpha \in S_n$ kann man eine Zahl $\text{sgn}(\alpha) \in \{-1, 1\}$ zuordnen, das **Signum** (oder Vorzeichen) von α, so dass gilt:
  - $\text{sgn}(\tau) = -1$ für jede Transposition τ.
  - $\text{sgn}(\alpha \circ \beta) = sgn(\alpha) \cdot sgn(\beta)$ für alle $\alpha, \beta \in S_n$
- Eine Permutation heißt **ungerade**, falls ihr Signum -1 ist, andernfalls **gerade**.
- Ist $\alpha = (i_1 i_2 \dots i_\ell)$ die Zyklendarstellung der Permutation α, dann gilt $\text{sgn}(\alpha) = (-1)^{\ell-1}$.
- Eine Permutation ist genau dann gerade, wenn in ihrer Zyklendarstellung die Anzahl der Zyklen gerader Länge gerade ist.

Erzeugen der symmetrischen Gruppe S_n

- Die Transpositionen aus S_n erzeugen die Gruppe S_n.
- Die Transpositionen $(1\,2),\ (1\,3)\ \ldots, (1\,n)$ erzeugen die Gruppe S_n.
- Die Transpositionen $(1\,2),\ (2\,3)\ \ldots, (n-1\,n)$ erzeugen die Gruppe S_n.
- Die Transposition $(1\,2)$ und der Zyklus $(1\,2\,\ldots\,n)$ erzeugen die Gruppe S_n.
- Die geraden Permutationen bilden eine Unterguppe A_n der symmetrischen Gruppe S_n.

  A_n wird alternierende Gruppe vom Grad n genannt.

  Es gilt $|A_n| = \frac{1}{2} \cdot n!$

  Für $n \geq 3$ wird A_n von Zyklen der Läge 3 erzeugt.

Codierungsverfahren mit der Diedergruppe D_5

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

$\boxed{a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11}}$ mit $a_i \in \{0, 1, \ldots, 9\}$

Prüfgleichung: $T(a_1) * T^2(a_2) * \cdots * T^{10}(a_{10}) * a_{11} = 0$ mit

$$T = (0\,1\,5\,8\,9\,4\,2\,7)(8\,9)$$

$*$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0