

- **Transformationen**

Ist  $A$  eine Menge, so ist die Menge

$$\mathcal{T}(A) = \{f : A \rightarrow A\}$$

bezüglich der Komposition (Hintereinanderausführung)  $\circ$  als Operation und der identischen Abbildung  $id$  als neutralem Element ein Monoid  $(\mathcal{T}(A); \circ, id)$ .

Beachte:  $\circ$  ist nicht kommutativ!

Es wird vereinbart, dass

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

gilt, d.h. die Hintereinanderausführung wird von rechts nach links gelesen.

Für die iterierte Hintereinanderausführung derselben Transformation wird geschrieben

$$f^{(n)} = \underbrace{f \circ f \circ \dots \circ f}_{n \text{ Faktoren}}, \text{ also } f^{(i+j)} = f^{(i)} \circ f^{(j)}.$$

Notation: sind  $a, b$  ganze Zahlen, so ist  $[a, b] = \{a, a+1, a+2, \dots, b\}$  für  $a \leq b$  das Intervall der ganzen Zahlen zwischen  $a$  und  $b$  (einschliesslich). Für  $a > b$  ist dies die leere Menge.

Ist  $A$  eine total geordnete, endliche Menge, etwa  $A = [1, 2] = \{1, 2, \dots, n\}$ , so kann ein  $f \in \mathcal{T}(A)$  in Listenform dargestellt werden:

$$f \leftrightarrow [f(1), f(2), \dots, f(n)].$$

Offensichtlich ist in diesem endlichen Fall mit  $\#A = n$  für die Mächtigkeit

$$\#\mathcal{T}(A) = n^n.$$

- **Bäume**

$A$  sei eine endliche Menge. Eine Transformation  $f \in \mathcal{T}(A)$  ist *baumartig*, kurz: ein *Baum*, wenn es ein  $m \in \mathbb{N}$  gibt, für das  $f^{(m)}$  eine konstante Abbildung ist, d.h. es gibt ein  $r \in A$  mit  $f^{(m)}(a) = r$  für alle  $a \in A$ . Das Element  $r$  heisst dann *Wurzel* (root) des Baumes  $f$ .

Die Anzahl der Bäume auf einer  $n$ -elementigen Menge ist  $n^{n-1}$ .

Hinweis: nach dieser Terminologie sind Bäume *gerichtete* Graphen (Kanten zur wurzel hin gerichtet). Betrachtet man (wie in der Graphentheorie üblich), Bäume als zusammenhängende und kreisfreie ungerichtete Graphen und zeichnet keinen Knoten als Wurzel aus, so gibt es auf einer  $n$ -Menge genau  $n^{n-2}$  Bäume dieser Art (Formel von CAYLEY).

• **Permutationen**

Die Menge

$$\mathcal{S}(A) = \{f \in \mathcal{T}(A); f \text{ bijektiv}\}$$

der *Permutationen* von  $A$  ist bezüglich  $\circ$  und  $id$  sogar eine Gruppe, die *symmetrische Gruppe* von  $A$ . Im endlichen Fall,  $\#A = n$ , gilt bekanntlich

$$\#\mathcal{S}(A) = n!$$

und die Elemente  $s \in \mathcal{S}(A)$  können in wie oben Listenform geschrieben werden

$$s \leftrightarrow [s(1), s(2), \dots, s(n)],$$

wobei die  $s(i)$  paarweise verschieden sind.

• **Zyklische Permutationen**

Spezielle Permutationen sind die *Zyklen* oder *zyklischen Permutationen*:

Ist  $a_1, a_2, \dots, a_k$  mit  $k \geq 2$  eine Folge von paarweise verschiedenen Elementen aus  $A$ , so ist  $c = (a_1, a_2, \dots, a_k)$  die durch

$$c : \begin{cases} a_i \mapsto a_{i+1 \bmod k} & \text{für } 1 \leq i \leq k \\ a \mapsto a & \text{falls } a \notin \{a_1, a_2, \dots, a_k\} \end{cases}$$

bestimmte Permutation von  $A$ , ein Zyklus der Länge  $k$  und mit der Trägermenge  $|c| = \{a_1, a_2, \dots, a_k\}$ .

Offensichtlich definiert die Folge  $a_2, a_3, \dots, a_k, a_1$  die gleiche zyklische Permutation wie die Folge  $a_1, a_2, \dots, a_k$ . Oft ist es zweckmässig, unter den  $k$  verschiedenen Folgen, die eine zyklische Permutation der Länge  $k$  definieren, diejenige als Repräsentanten auszuwählen, für die  $a_1$  maximal ist (bezüglich einer totalen Ordnung auf  $A$ ), d.h.

$$a_1 = \max_{1 \leq i \leq k} a_i = \max |c|.$$

Einige Bemerkungen:

- Auf einer  $k$ -elementigen Trägermenge gibt es genau  $(k - 1)!$  verschiedene zyklische Permutationen.
- Sind  $c_1, c_2$  zyklische Permutationen mit disjunktem Träger, d.h.  $|c_1| \cap |c_2| = \emptyset$ , so kommutieren sie als Permutationen:

$$c_1 \circ c_2 = c_2 \circ c_1.$$

- Ist  $c = (a_1, a_2, \dots, a_k)$  ein Zyklus der Länge  $k$ , so ist der  $k$ -Zyklus

$$c^{-1} = (a_k, a_{k-1}, \dots, a_1)$$

die dazu inverse Permutation.

- Ist  $m \in \mathbb{N}$  und  $d = \text{ggT}(m, k)$ , so ist  $c^{(m)}$  das Produkt von  $d$  disjunkten Zyklen der Länge  $k/d$ : (Indices immer modulo  $k$  genommen)

$$c^{(m)} = (a_1, a_{1+m}, a_{1+2m}, \dots)(a_2, a_{2+m}, a_{2+2m}, \dots) \cdots (a_d, a_{d+m}, a_{d+2m}, \dots)$$

Insbesondere gilt  $c^{(m)} = id \Leftrightarrow k \mid m$ .

### • Darstellungen von Permutationen als Produkte

**Satz:** Jede Permutation  $s \in \mathcal{S}(A)$  lässt sich als Produkt von disjunkten Zyklen schreiben, d.h.

$$s = c_1 \circ c_2 \circ \cdots \circ c_r, \text{ mit } |c_i| \cap |c_j| = \emptyset \ (i \neq j)$$

und zwar eindeutig, wenn man  $\max |c_1| < \max |c_2| < \dots < \max |c_r|$  fordert.

Das Inverse von  $s = c_1 \circ c_2 \circ \cdots \circ c_r$  ist natürlich

$$s^{-1} = (c_1 \circ c_2 \circ \cdots \circ c_r)^{-1} = c_r^{-1} \circ c_{r-1}^{-1} \circ \cdots \circ c_1^{-1} = c_1^{-1} \circ c_2^{-1} \circ \cdots \circ c_r^{-1}$$

(Kommutierende Faktoren wegen Disjunktheit!)

Ein Zyklus  $c = (a, b)$  der Länge 2 wird auch als *Transposition* bezeichnet.

Jeder Zyklus  $c = (a_1, a_2, \dots, a_k)$  der Länge  $k$  lässt sich als Produkt von  $k - 1$  (aber nicht weniger!) Transpositionen (dann natürlich nicht disjunkten!) schreiben, z.B.:

$$(a_1, a_2, \dots, a_k) = (a_1, a_k) \circ (a_1, a_{k-1}) \circ \cdots \circ (a_1, a_3) \circ (a_1, a_2)$$

(Dies ist nur eine von vielen Möglichkeiten). Daher gilt:

**Satz:** Jede Permutation lässt sich als Produkt von Transpositionen schreiben:

$$s = t_1 \circ t_2 \circ \cdots \circ t_p.$$

(Dafür gibt es viele verschiedene Möglichkeiten). Die (exakte !) *minimale* Anzahl der Faktoren ist dabei  $n - \text{cyc}(s)$ , wobei  $\text{cyc}(s)$  die Anzahl der Zyklen von  $s$  (inklusive der Fixpunkte als Zyklen der Länge 1) ist.

Ist  $A = [1, n] = \{1, 2, \dots, n\}$ , so bezeichnet man die speziellen Transpositionen  $\tau_j = (j, j + 1)$  als *Transpositionen benachbarter Elemente*. Jede Transposition  $t = (j, k)$  mit  $j < k$  lässt sich als Produkt von  $\tau_i$ 's schreiben:

$$(j, k) = \tau_j \circ \tau_{j+1} \circ \cdots \circ \tau_{k-2} \circ \tau_{k-1} \circ \tau_{k-2} \circ \cdots \circ \tau_{j+1} \circ \tau_j.$$

Für die  $\tau_j$  untereinander gelten folgende Beziehungen, die sog. COXETER-Relationen

- (1)  $\tau_j \circ \tau_j = id$  d.h.  $\tau_j^2 = id$   $1 \leq j < n$
- (2)  $\tau_j \circ \tau_k = \tau_k \circ \tau_j$  d.h.  $(\tau_j \circ \tau_k)^2 = id$   $|j - k| \geq 2$
- (3)  $\tau_j \circ \tau_{j+1} \circ \tau_j = \tau_{j+1} \circ \tau_j \circ \tau_{j+1}$  d.h.  $(\tau_j \circ \tau_{j+1})^3 = id$   $1 \leq j < n$

**Satz:** Jede Permutation  $s \in \mathcal{S}_n = \mathcal{S}([1, n])$  lässt sich als Produkt von Transpositionen benachbarter Elemente schreiben:  $s = \tau_{i_1} \circ \tau_{i_2} \circ \dots \circ \tau_{i_k}$ .

Die (exakte!) minimale Anzahl der Faktoren ist dabei gleich der Anzahl  $\text{inv}(s)$  der Inversionen von  $s$  (siehe weiter unten).

Zwei Produkte  $\tau_{i_1} \circ \tau_{i_2} \circ \dots \circ \tau_{i_k}$  und  $\tau_{j_1} \circ \tau_{j_2} \circ \dots \circ \tau_{j_\ell}$  stellen genau dann die gleiche Permutation dar, wenn sie sich durch Anwendung der Regeln (1),(2),(3) ineinander überführen lassen.

### • Gerade und ungerade Permutationen

**Satz:** Folgende Eigenschaften sind für eine Permutation  $s \in \mathcal{S}(A)$  äquivalent:

1. Bei der Darstellung  $s = c_1 \circ c_2 \circ \dots \circ c_r$  als Produkt elementfremder Zyklen ist die Anzahl der Faktoren mit gerader Länge *gerade*.
2. Jede Darstellung von  $s$  als Produkt von Transpositionen  $s = t_1 \circ t_2 \circ \dots \circ t_p$  hat eine *gerade* Anzahl  $p$  von Faktoren.

Permutationen mit den beschriebenen Eigenschaften nennt man *gerade Permutationen*, die anderen *ungerade Permutationen*. Für die Bedeutung dieser Unterscheidung sei an die Definition der Determinanten für Matrizen erinnert!

- Das Produkt  $s_1 \circ s_2$  zweier Permutationen ist genau dann eine gerade Permutation, wenn beide Faktoren gerade oder beide Faktoren ungerade sind.
- Das Inverse eine geraden Permutation ist ebenfalls eine gerade Permutation.
- Es gibt auf einer Menge  $A$  mit  $\#A = n > 1$  genauso viele gerade wie ungerade Permutationen, nämlich  $n!/2$ .
- Die geraden Permutation einer Menge bilden für sich eine Gruppe, genannt *alternierende Gruppe*.

### • Inversionen

Ist  $\ell = (\ell_1, \ell_2, \dots, \ell_n)$  eine Liste von natürlichen Zahlen (oder von Elementen irgendeiner totalgeordneten Menge), so heisst jedes Indexpaar  $(j, k)$  mit  $1 \leq j < k \leq n$  eine *Inversion* von  $\ell$ , falls  $\ell_j > \ell_k$ .

Inversionen spielen eine wichtige Rolle beim Studium von Sortieralgorithmen!

- Die Anzahl der Inversionen  $\text{inv}(s)$  einer Permutation  $s \in \mathcal{S}(A)$  in Listendarstellung ist die minimale Anzahl von Faktoren, die man zur Darstellung von  $s$  als Produkt von Transpositionen benötigt.
- Eine Permutation ist genau dann gerade, wenn die Anzahl der Inversionen in ihrer Listendarstellung gerade ist.

Ist  $\ell = (\ell_1, \ell_2, \dots, \ell_n)$  eine Liste von natürlichen Zahlen, so bezeichnet

$$\text{ivector}(\ell) = (i_1, i_2, \dots, i_n), \quad \text{wobei } i_k = \#\{1 \leq j < k; \ell_j > \ell_k\}$$

den *Inversionsvektor* von  $\ell$ . Offenbar gilt  $0 \leq i_k < k$ , d.h.  $i_k \in [0, k-1]$  ( $1 \leq k \leq n$ ).

**Satz:** Permutationen sind durch ihre Inversionsvektoren eindeutig bestimmt. Die Abbildung

$$\text{ivec} : \mathcal{S}(A) \rightarrow [0, 0] \times [0, 1] \times [0, 2] \times \cdots \times [0, n - 1] : s \mapsto \text{ivec}(s)$$

ist eine Bijektion.

### Beispiele

In allen Beispielen ist  $A = [1, 6]$ .

#### 1. Transformationen in Listendarstellung

$$\begin{aligned} f & : [4, 6, 1, 3, 4, 6] \\ g & : [2, 3, 3, 1, 2, 3] \\ f \circ g & : [6, 1, 1, 4, 6, 1] \\ g \circ f & : [1, 3, 2, 3, 1, 3] \\ f^{(2)} & : [3, 6, 4, 1, 3, 6] \\ f^{(3)} & : [1, 6, 3, 4, 1, 6] \\ f^{(4)} & : [4, 6, 1, 3, 4, 6] \\ f^{(5)} & : [3, 6, 4, 1, 3, 6] = f^{(2)} \\ g^{(2)} & : [3, 3, 3, 2, 3, 3] \\ g^{(3)} & : [3, 3, 3, 3, 3, 3] \end{aligned}$$

$f$  ist kein Baum,  $g$  ist ein Baum.

#### 2. Permutationen in Listen- und Zyklendarstellung

$$\begin{aligned} s & : [4, 6, 1, 3, 5, 2] : (4, 3, 1)(5)(6, 2) : \text{cyc}(s) = 3 \\ s' & : [6, 4, 3, 2, 5, 1] : (3)(4, 2)(5)(6, 1) : \text{cyc}(s') = 4 \\ s \circ s' & : [2, 3, 1, 6, 5, 4] : (3, 1, 2)(5)(6, 4) : \text{cyc}(s \circ s') = 3 \\ s' \circ s & : [2, 1, 6, 3, 5, 4] : (2, 1)(5)(6, 4, 3) : \text{cyc}(s' \circ s) = 3 \end{aligned}$$

#### 3. Potenzen eines Zyklus

$$\begin{aligned} c & = (6, 5, 3, 4, 1, 2) \\ c^{(2)} & = (6, 3, 1)(5, 4, 2) \\ c^{(3)} & = (6, 4)(5, 1)(3, 2) \\ c^{(4)} & = (6, 1, 3)(5, 2, 4) \\ c^{(5)} & = (6, 2, 1, 4, 3, 5) = c^{(-1)} \\ c^{(6)} & = (6)(5)(4)(3)(2)(1) = c^{(0)} \end{aligned}$$

#### 4. Permutationen als Produkte von Transpositionen

$$\begin{aligned} s & : [4, 6, 1, 3, 5, 2] : (4, 1)(4, 3)(6, 2) \\ s' & : [6, 4, 3, 2, 5, 1] : (4, 2)(6, 1) \\ u = s \circ s' & : [2, 3, 1, 6, 5, 4] : (3, 2)(3, 1)(6, 4) \\ v = s' \circ s & : [2, 1, 6, 3, 5, 4] : (2, 1)(6, 3)(6, 4) \end{aligned}$$

5. Permutationen als Produkte von Transpositionen benachbarter Elemente

$$\begin{aligned} u &= (32)(31)(64) = \underline{(23)(12)(23)}(12)(45)(56)(45) \\ &= (12)(23)\underline{(12)(12)}(45)(56)(45) = (12)(23)(45)(56)(45) \end{aligned}$$

$$\begin{aligned} v &= (21)(63)(64) = (12)(34)\underline{(45)(56)(45)}(34)\underline{(45)(56)(45)} \\ &= (12)(34)(56)(45)(56)\underline{(34)(56)(45)(56)} = \underline{(12)(34)(56)(45)(56)(56)}(34)(45)(56) \\ &= (12)\underline{(34)(56)(45)}(34)\underline{(45)(56)} = (12)(56)(34)(45)\underline{(34)(45)(56)} \\ &= (12)\underline{(56)(45)}(34)\underline{(45)(45)}(56) = (12)(56)(45)\underline{(34)(56)} \end{aligned}$$

6. Inversionsvektoren und Anzahl der Inversionen

$$\begin{aligned} s &: [4, 6, 1, 3, 5, 2] : \text{iv}ec(s) = [0, 0, 2, 2, 1, 4] : \text{inv}(s) = 9 \\ s' &: [6, 4, 3, 2, 5, 1] : \text{iv}ec(s') = [0, 1, 2, 3, 1, 5] : \text{inv}(s') = 12 \\ u = s \circ s' &: [2, 3, 1, 6, 5, 4] : \text{iv}ec(u) = [0, 0, 2, 0, 1, 2] : \text{inv}(u) = 5 \\ v = s' \circ s &: [2, 1, 6, 3, 5, 4] : \text{iv}ec(v) = [0, 1, 0, 1, 1, 2] : \text{inv}(v) = 5 \end{aligned}$$