

Wiederholung

• $R = \mathbb{Z}$, oder $R = K[X]$, $0 \neq m \in R$, $m \in \mathbb{N}$ falls $R = \mathbb{Z}$

- $a, b \in R$: $a \equiv_m b \Leftrightarrow m \mid a - b$

- \equiv_m ist ÄR auf R , \bar{a} ÄK von $a \in R$

$$R / \equiv_m =: R / (m), \quad \mathbb{Z}_m := \mathbb{Z} / (m)$$

- $a \in R$

$a \bmod m := r$, falls ~~a~~ $a = qm + r$ und

$$\begin{cases} 0 \leq r < m, & \text{falls } R = \mathbb{Z}, \\ \deg r < \deg m, & \text{falls } R = K[X] \end{cases}$$

- $a, b \in R$:

$$a \equiv_m b \Leftrightarrow a \bmod m = b \bmod m$$

$$\bar{a} = a + Rm := \{a + xm \mid x \in R\} \text{ Restklasse}$$

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

$\bar{0}$: Menge der geraden Zahlen
 $\bar{1}$: " " ungerade "

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

$$\mathbb{Z}_1 = \{\bar{0}\}$$

Repräsentantensystem für \mathbb{Z}_m : $\{0, 1, \dots, m-1\}$

" " $K[X]/(m)$: $K[X]_{< \deg m}$

$R/(m)$ kommutativer Ring mit

$$\bar{a} + \bar{b} := \overline{a+b}, \quad \bar{a} \cdot \bar{b} := \overline{a \cdot b}, \quad 1 = \bar{1}, \quad 0 = \bar{0}$$

$$-\bar{a} = \overline{-a}$$

$$\cdot (\mathbb{R}/(m))^{\times} = \{ \bar{a} \mid \text{ggT}(a, m) = 1 \}$$

Sei $a \in \mathbb{R}$ mit $\text{ggT}(a, m) = 1$

Bestimme $x, y \in \mathbb{R}$ mit $xa + ym = 1$

$$\Rightarrow \bar{x} = \bar{a}^{-1}$$

$$[ym = xa - 1 \Rightarrow m \mid xa - 1 \Rightarrow xa \equiv_m 1$$

$$\Rightarrow \overline{xa} = \bar{1} \Rightarrow \bar{x} \cdot \bar{a} = \bar{1} = 1]$$

$\cdot p \in \mathbb{N}$ Primzahl, falls $p > 1$ und 1, p die einzigen Teiler von p in \mathbb{N} .

$g \in K[X]$ irreduzibel, falls $g \neq c$, $\deg g > 1$ ~~und~~ und es gilt:

Ist $g = f \cdot h$, $f, h \in K[X] \Rightarrow f \in K^{\times}$ oder $h \in K^{\times}$.

$\cdot \mathbb{R}/(m)$ ist Körper $(\Rightarrow) \begin{cases} m \text{ Primzahl} & (\mathbb{R} = \mathbb{Z}) \\ m \text{ irreduzibel} & (\mathbb{R} = K[X]) \end{cases}$

Beweis: " \Rightarrow " m nicht Primzahl / irreduzibel

$$\Rightarrow m = a \cdot b \text{ mit } a, b \notin \mathbb{R}^\times$$

$$\Rightarrow \bar{a} \neq 0, \bar{b} \neq 0 \text{ in } \mathbb{R}/(m) \text{ und } \bar{a} \cdot \bar{b} = \bar{0} = 0$$

$$\Rightarrow \mathbb{R}/(m) \text{ ist kein Körper.}$$

" \Leftarrow " Sei $a \in \mathbb{R}$ mit $\bar{a} \neq \bar{0} \Rightarrow m \nmid a$

$$\Rightarrow \text{ggT}(a, m) = 1$$

$$[m = \text{ggT}(a, m) \cdot q, m \text{ irreduzibel} \Rightarrow \text{ggT}(a, m) = 1 \text{ oder } q \in \mathbb{R}^\times]$$

$$\Rightarrow \text{ggT}(a, m) = 1 \text{ oder } m \mid \text{ggT}(a, m)$$

$$\Rightarrow \text{ggT}(a, m) = 1 \text{ oder } m \mid a \text{ da } \text{ggT}(a, m) \mid a]$$

$$\text{Damit } \bar{a} \in (\mathbb{R}/(m))^\times. \quad \text{ZZZ}$$

Endliche Primkörper

Definition

$$p \in \mathbb{P}$$

Primkörper zu p : $\mathbb{F}_p := \mathbb{Z}/(p) \cong \mathbb{Z}_p$

Beispiel

$$\blacktriangleright \mathbb{F}_2 = \mathbb{Z}/(2) = \{\bar{0}, \bar{1}\}$$

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

\cdot	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Endliche Primkörper (Forts.)

Unterdrücke den Querstrich in der Notation

► $\mathbb{F}_3 = \mathbb{Z}/(3) = \{0, 1, 2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

► $\mathbb{F}_5 = \mathbb{Z}/(5) = \{0, 1, 2, 3, 4\}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Restklassenkörper von Polynomringen

Beispiel

$\mathbb{R}[X]/(X^2 + 1)$ ist Körper

Definition

Körper der komplexen Zahlen: $\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$

Terminologien und Notationen:

- ▶ *komplexe Zahl:* Element von \mathbb{C}
- ▶ *imaginäre Einheit:* $i := \bar{X} \in \mathbb{C}$

$$i^2 = \bar{X}^2 = \overline{X^2 + 1} - \bar{1} = -1.$$

Restklassenkörper von Polynomringen (Forts.)

Bemerkung

► $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$

► $a, b, a', b' \in \mathbb{R}$

$$a + bi = a' + b'i \Leftrightarrow a = a' \text{ und } b = b'$$

► $a, b, c, d \in \mathbb{R}$

Ersetze $a := \bar{a}$ für $\mathbb{R}[X]_{<1}$.

Ersetze jedes ~~Polynom~~ Restklassen durch ihren Repräsentanten in $\mathbb{R}[X]_{<2} =$

~~$\mathbb{R}[X]$~~ $\{a + bX \mid a, b \in \mathbb{R}\}$

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

Restklassenkörper von Polynomringen (Forts.)

Definition

$z \in \mathbb{C}$, $a, b \in \mathbb{R}$ mit $z = a + bi$

- ▶ *Realteil* von z : $\operatorname{Re} z := a$
- ▶ *Imaginärteil* von z : $\operatorname{Im} z := b$

Beispiel

- ▶ $\operatorname{Re}(2 - i) = 2$
- ▶ $\operatorname{Im}(2 - i) = -1$

Restklassenkörper von Polynomringen (Forts.)

Definition

$$z \in \mathbb{C}$$

zu z konjugierte komplexe Zahl: $\bar{z} := \operatorname{Re} z - (\operatorname{Im} z)i$

Beispiel

$$\overline{3 - 2i} = 3 + 2i$$

Restklassenkörper von Polynomringen (Forts.)

Beispiel

- ▶ $\mathbb{F}_2[X]/(X^2 + X + 1)$ ist Körper
- ▶ $\mathbb{F}_2[X]/(X^3 + X + 1)$ ist Körper
- ▶ $\mathbb{F}_3[X]/(X^2 + 1)$ ist Körper

Notation

- ▶ $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2 + X + 1); \quad \alpha := \overline{X} \text{ in } \mathbb{F}_4$
- ▶ $\mathbb{F}_8 := \mathbb{F}_2[X]/(X^3 + X + 1); \quad \beta := \overline{X} \text{ in } \mathbb{F}_8$
- ▶ $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2 + 1); \quad \iota := \overline{X} \text{ in } \mathbb{F}_9$

Restklassenkörper von Polynomringen (Forts.)

Bemerkung

► $\mathbb{F}_4 = \{a + b\alpha \mid a, b \in \mathbb{F}_2\}$

► $a, b, a', b' \in \mathbb{F}_2$

$$a + b\alpha = a' + b'\alpha \Leftrightarrow a = a' \text{ und } b = b'$$

► $a, b, c, d \in \mathbb{F}_2$

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$$

$$(a + b\alpha) \cdot (c + d\alpha) = (ac + bd) + (ad + bc + bd)\alpha$$

$$\alpha^2 = -1 - \alpha = 1 + \alpha \quad \left[\text{Weil } \bar{X}^2 + \bar{X} + \bar{1} = \bar{0} \right]$$

Restklassenkörper von Polynomringen (Forts.)

\mathbb{F}_4

+	0	1	α	$1 + \alpha$
0	0	1	α	$1 + \alpha$
1	1	0	$1 + \alpha$	α
α	α	$1 + \alpha$	0	1
$1 + \alpha$	$1 + \alpha$	α	1	0

.	0	1	α	$1 + \alpha$
0	0	0	0	0
1	0	1	α	$1 + \alpha$
α	0	α	$1 + \alpha$	1
$1 + \alpha$	0	$1 + \alpha$	1	α

Euler-Funktion

Definition

Euler-Funktion:

$$\varphi: \mathbb{N} \rightarrow \mathbb{N}, n \mapsto |(\mathbb{Z}_n)^\times|$$

Beispiel

$$\varphi(8) = 4, \text{ da } (\mathbb{Z}_8)^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}.$$

Euler-Funktion (Forts.)

Bemerkung

$$\varphi(n) = |\{x \in \{0, 1, \dots, n-1\} \mid \text{ggT}(n, x) = 1\}|.$$

Proposition

- ▶ $p, q \in \mathbb{P}$ mit $p \neq q$

$$\varphi(pq) = (p-1)(q-1)$$

- ▶ $p \in \mathbb{P}$

$$\varphi(p) = p-1 \quad \checkmark$$

▮ Allgemein gilt: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, falls $\text{ggT}(m, n) = 1$.
(Ohne Beweis.)

Beweis: Vielfache von p in $0, 1, \dots, pq-1$:

Anzahl:

$0, p, 2p, \dots, (q-1)p$

q

Vielfache von q in $0, 1, \dots, pq-1$:

$0, q, 2q, \dots, (p-1)q$

p

$$\Rightarrow \varphi(pq) = pq - p - q + 1 = (p-1)(q-1). \quad \square$$

Euler-Funktion (Forts.)

Lemma

G endliche abelsche Gruppe, $x \in G$

$$x^{|G|} = 1$$

Beweis: $G = \{g_1, \dots, g_m\} \Rightarrow G = \{xg_1, \dots, xg_m\}, \quad m = |G|$

$$a := \prod_{i=1}^m g_i$$

$$\Rightarrow a = \prod_{i=1}^m g_i = \prod_{i=1}^m (xg_i) = x^{|G|} \prod_{i=1}^m g_i = x^{|G|} \cdot a \quad \checkmark$$

Euler-Funktion (Forts.)

Satz von Euler

$n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $\text{ggT}(n, a) = 1$


$$a^{\varphi(n)} \equiv_n 1$$

Folgt aus Lemma, angewandt auf $x = \bar{a} \in (\mathbb{Z}_n)^\times$. 

Kleiner Satz von Fermat

$p \in \mathbb{P}$, $a \in \mathbb{Z}$ mit $p \nmid a$:

$$a^{p-1} \equiv_p 1$$

Folgt aus Euler mit $n = p$, da $\varphi(p) = p-1$. 

6. Dezember 2018

Die symmetrische Gruppe

Symmetrische Gruppe

Erinnerung

Es sei A eine Menge.

$\text{Abb}(A, A)$ ist Monoid mit Verknüpfung

$$(g, f) \mapsto g \circ f = gf$$

(Komposition von Abbildungen).

Symmetrische Gruppe (Forts.)

Definition

- ▶ Es sei A eine Menge.
 - ▶ *Symmetrische Gruppe* auf A :

$$S_A := \text{Abb}(A, A)^\times$$

- ▶ *Permutation* von A : Element von S_A

- ▶ Es sei $n \in \mathbb{N}_0$.

$$\underline{n} = \{1, \dots, n\}$$

Symmetrische Gruppe vom Grad n : $\underline{0} = \emptyset$

$$S_n := S_{\underline{n}}$$

Symmetrische Gruppe (Forts.)

Notation

Für $\pi \in S_A$: $|A| = n < \infty$, $A = \{a_1, \dots, a_n\}$

$$\pi = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \pi(a_1) & \pi(a_2) & \dots & \pi(a_n) \end{pmatrix}.$$

Für $\pi \in S_n$:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

Meistens lassen wir das Zeichen „ \circ “ für die Verknüpfung weg.

Symmetrische Gruppe (Forts.)

Beispiele

$$\blacktriangleright S_0 = \{ \text{id}_\emptyset \}$$

$$\blacktriangleright S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$\blacktriangleright S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$\blacktriangleright S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Beispiele

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Symmetrische Gruppe (Forts.)

Definition

Für $n \in \mathbb{N}_0$ ist $n! \in \mathbb{N}$, gesprochen „ n Fakultät“, definiert durch

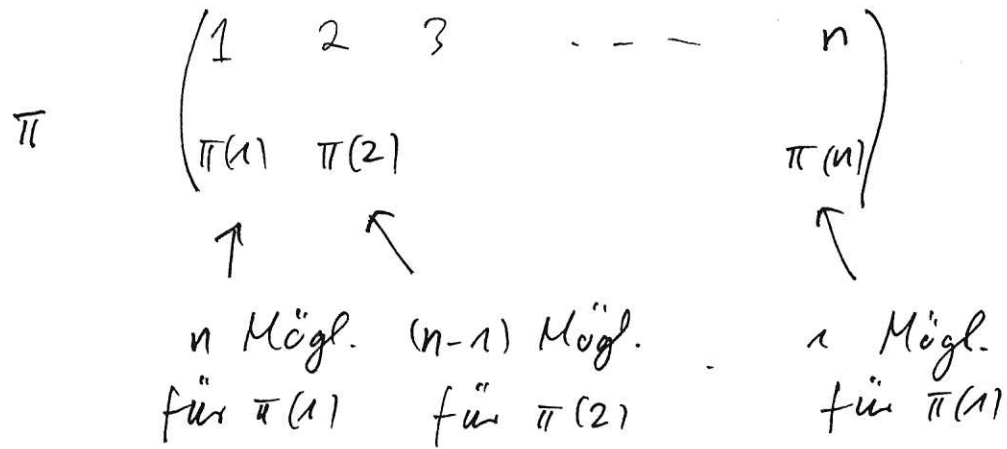
$$0! := 1, \quad \begin{array}{l} 1! = 1 \\ 2! = 2 \\ 3! = 6 \\ 4! = 24 \\ 5! = 120 \\ 6! = 720 \end{array}$$
$$n! := \prod_{i=1}^n i = 1 \cdot 2 \cdot 3 \cdots n$$

für $n > 0$.

Proposition

Für $n \in \mathbb{N}_0$ ist $|S_n| = n!$.

Beweis der Proposition



Träger einer Permutation

Definition


Für $\pi \in S_A$ heißt

$$T_\pi := \{a \in A \mid \pi(a) \neq a\} \subseteq A$$

der Träger von π .

Beispiel

$\in A \setminus T_\pi$


$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix},$$

$$T_\pi = \{1, 2, 4, 5, 6, 7, 8, 10, 11\}.$$

Träger einer Permutation (Forts.)

Bemerkung

Es seien $\pi, \psi \in S_A$. $T_\pi \subseteq A$

$$(a) \blacktriangleright \pi(T_\pi) = T_\pi. \quad \bar{\pi}(T_\pi) := \{ \pi(a) \mid a \in T_\pi \}$$

(b) \blacktriangleright Gilt $T_\pi \subseteq B$, so kann π auch als Element von S_B aufgefasst werden.

(c) \blacktriangleright Haben π und ψ disjunkte Träger, so gilt $\pi \circ \psi = \psi \circ \pi$.

Beweis der Bemerkung:

$$(a) \quad - \quad \mathcal{B} := A \setminus T_\pi, \text{ d.h. } T_\pi \cap \mathcal{B} = \emptyset$$

$$\Rightarrow \pi(\mathcal{B}) = \{\pi(b) \mid b \in \mathcal{B}\} = \mathcal{B}$$

$$- \quad \pi \text{ injektiv} \Rightarrow \pi(T_\pi) \cap \pi(\mathcal{B}) = \emptyset$$

$$\Rightarrow \pi(T_\pi) \cap \mathcal{B} = \emptyset$$

$$\Rightarrow \pi(T_\pi) \subseteq A \setminus \mathcal{B} = T_\pi$$


$$\Rightarrow \pi(T_\pi) = T_\pi \quad \text{weil } |\pi(T_\pi)| = |T_\pi|$$

$$(b) \quad T_\pi \cap T_\psi = \emptyset \Rightarrow \pi \circ \psi = \psi \circ \pi$$

$$a \in T_\pi \Rightarrow \pi(a) \in T_\pi \quad \text{nach (a)}$$

$$\Rightarrow \psi(a) = a, \quad \psi(\pi(a)) = \pi(a) \quad \text{da } a, \pi(a) \notin T_\psi.$$

$$\Rightarrow \pi \circ \psi(a) = \pi(\psi(a)) = \pi(a) = \psi(\pi(a)) = \psi \circ \pi(a).$$

Analog für $a \in T_\psi$. 

Zykel

Definition

Es seien $x_1, x_2, \dots, x_k \in A$ paarweise verschieden.

$\sigma \in S_A$ mit

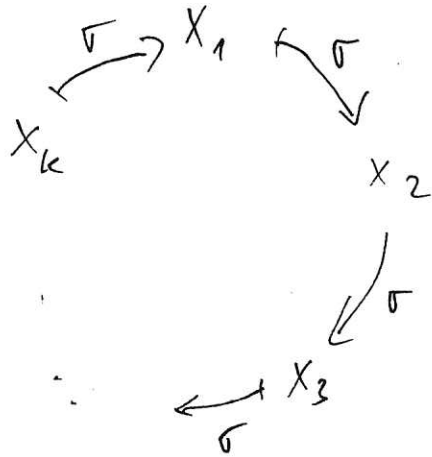
$$\sigma(x) = \begin{cases} x_{i+1} & \text{falls } x = x_i \text{ und } i < k, \\ x_1 & \text{falls } x = x_k, \\ x & \text{falls } x \neq x_1, x_2, \dots, x_k, \end{cases}$$

heißt *Zykel der Länge k* oder kurz *k-Zykel* von S_A .

Schreibweise:

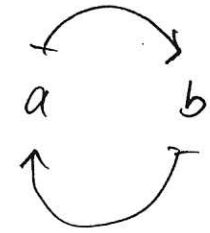
$$\sigma = (x_1, x_2, \dots, x_k).$$

Die 2-Zykel heißen auch *Transpositionen* von S_A .



k -Zykel

x



Transposition

$$\sigma_x = \text{id} \quad \forall x \in A$$

Zykel (Forts.)

Beispiele

$$= (5, 2, 4, 1)$$

- Der 4-Zykel $\sigma := (1, 5, 2, 4) \in S_5$ ist die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$$

- $(1, 2, 3, 4, 5)(2, 1)(5, 4) = (1, 3, 4)(2)(5)$

- $(1, 2)(2, 3) = (1, 2, 3)$

- $(1, 2, 3)(3, 2, 1) = (1)(2)(3) = \text{id}$

Zykel (Forts.)

$$(x_1, x_2, \dots, x_{k-1}, x_k)(x_k, x_{k-1}, \dots, x_2, x_1) = (x_1)(x_2) \cdots (x_k)$$

Bemerkung

- ▶ Es gilt stets $(x_1, x_2, \dots, x_k)^k = \text{id}$.
- ▶ Es gilt stets $(x_1, x_2, \dots, x_k)^{-1} = (x_k, x_{k-1}, \dots, x_1)$.
- ▶ Für Transpositionen τ gilt $\tau^{-1} = \tau$. $(a, b)(a, b) = \text{id}$
- ▶ Jeder 1-Zykel ist die Identität.
- ▶ Jeder k -Zykel läßt sich als Produkt von $k - 1$ Transpositionen schreiben:

$$(x_1, x_2, \dots, x_k) = (x_1, x_2)(x_2, x_3) \cdots (x_{k-1}, x_k).$$

Eine solche Zerlegung ist im Allgemeinen nicht eindeutig.

Zykel (Forts.)

Satz

Jede Permutation $\pi \in S_A$ läßt sich als Produkt von Zykeln schreiben, deren Träger paarweise disjunkt sind.

Eindeutigkeit: Bis auf Reihenfolge der Faktoren.

Sprechweise: Zerlegung von π in *paarweise disjunkte Zykeln*.

Konvention: Lasse 1-Zykel weg.

Zykel (Forts.)

Beispiel

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix} =$$

$$(1, 5, 2, 8)(4, 6, 7)(10, 11).$$

Beweis des Satzes: Induktion über $|T_\pi|$.

• $|T_\pi| = 0 \Rightarrow \pi = \text{id} \quad \checkmark$

• $T_\pi \neq \emptyset$, nehme $x_1 \in T_\pi$: Betrachte die Folge:

$$x_1, x_2 := \pi(x_1), x_3 := \pi(x_2), \dots \quad x_i := \pi^i(x_1), i \geq 1$$

$$\Rightarrow \text{es ex. } i, j, i < j \text{ mit } \pi^i(x_1) = \pi^j(x_1)$$

$$\Rightarrow x_1 = \pi^k(x_1) \text{ für } k = j - i$$

$$\Rightarrow \tau := (x_1, x_2, \dots, x_k) \text{ ist ein } k\text{-Zykel.}$$

Iteriere diesen Prozess. 