

WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

11-07-2004

Satz

Sei $b \in \mathbb{N}_0$ und $p \in \mathbb{N}$ eine Primzahl. Dann gilt:

$$b^p \equiv b \pmod{p}, \text{ (falls } b \neq 0 : b^{p-1} \equiv 1 \pmod{p})$$

(gemeint ist: die Gleichung $b^p = b$ gilt modulo p)

Beweis.

$$\mathbb{Z}_p^* = \{n \in \{1, \dots, p-1\}; \text{ggT}(n, p) = 1\}$$

1. Fall: $b = 0$: $0^p = 0 \pmod p$
2. Fall: $1 \leq b < p$: Betrachte $S_b = \langle \{b^0, b^1, \dots, b^{\text{ord}(b)-1}\}, \cdot \rangle$.
 S_b ist Untergruppe von \mathbb{Z}_p^* .
 Lagrange: $(\text{ord}(b) =) |S_b| \mid |\mathbb{Z}_p^*| (= p-1)$

$$\Rightarrow (\exists q \in \mathbb{N}) [q \cdot \text{ord}(b)] = p-1$$

Da $b^{\text{ord}(b)} = 1$ (Einselement) ist, gilt:

$$b^p = b^{p-1} \cdot b = b^{q \cdot \text{ord}(b)} \cdot b = 1^q \cdot b = b \pmod p$$

3. Fall: $b \geq p$: Dann gilt:

$$(\exists q, r \in \mathbb{N}_0, 0 \leq r < p) [b = q \cdot p + r].$$

Damit:

$$b^p = (q \cdot p + r)^p \stackrel{(*)}{=} r^p \pmod p \stackrel{(**)}{=} r \pmod p = b \pmod p$$

(*) Binomialentwicklung, die ersten p Summanden fallen weg (jeweils $= 0 \pmod p$); (**) Fall 1 bzw. 2

Beweis.

$$\mathbb{Z}_p^* = \{n \in \{1, \dots, p-1\}; \text{ggT}(n, p) = 1\}$$

1. Fall: $b = 0$: $0^p = 0 \bmod p$
2. Fall: $1 \leq b < p$: Betrachte $S_b = \langle \{b^0, b^1, \dots, b^{\text{ord}(b)-1}\}, \cdot \rangle$.
 S_b ist Untergruppe von \mathbb{Z}_p^* .
 Lagrange: $(\text{ord}(b) =) |S_b| \mid |\mathbb{Z}_p^*| (= p-1)$

$$\Rightarrow (\exists q \in \mathbb{N}) [q \cdot \text{ord}(b)] = p-1$$

Da $b^{\text{ord}(b)} = 1$ (Einselement) ist, gilt:

$$b^p = b^{p-1} \cdot b = b^{q \cdot \text{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$

3. Fall: $b \geq p$: Dann gilt:

$$(\exists q, r \in \mathbb{N}_0, 0 \leq r < p) [b = q \cdot p + r].$$

Damit:

$$b^p = (q \cdot p + r)^p \stackrel{(*)}{=} r^p \bmod p \stackrel{(**)}{=} r \bmod p = b \bmod p$$

(*) Binomialentwicklung, die ersten p Summanden fallen weg (jeweils $= 0 \bmod p$); (**) Fall 1 bzw. 2

Beweis.

$$\mathbb{Z}_p^* = \{n \in \{1, \dots, p-1\}; \text{ggT}(n, p) = 1\}$$

1. Fall: $b = 0$: $0^p = 0 \bmod p$
2. Fall: $1 \leq b < p$: Betrachte $S_b = \langle \{b^0, b^1, \dots, b^{\text{ord}(b)-1}\}, \cdot \rangle$.
 S_b ist Untergruppe von \mathbb{Z}_p^* .
 Lagrange: $(\text{ord}(b) = |S_b| \mid |\mathbb{Z}_p^*| (= p-1))$

$$\Rightarrow (\exists q \in \mathbb{N}) [q \cdot \text{ord}(b)] = p - 1$$

Da $b^{\text{ord}(b)} = 1$ (Einselement) ist, gilt:

$$b^p = b^{p-1} \cdot b = b^{q \cdot \text{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$

3. Fall: $b \geq p$: Dann gilt:

$$(\exists q, r \in \mathbb{N}_0, 0 \leq r < p) [b = q \cdot p + r].$$

Damit:

$$b^p = (q \cdot p + r)^p \stackrel{(*)}{=} r^p \bmod p \stackrel{(**)}{=} r \bmod p = b \bmod p$$

(*) Binomialentwicklung, die ersten p Summanden fallen weg (jeweils $= 0 \bmod p$); (**) Fall 1 bzw. 2

Die umgekehrte Richtung

Satz

Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

$$b^{n-1} \equiv 1 \pmod{n} \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \implies n \text{ ist prim.}$$

Beweis.

(durch Widerspruch)

Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \stackrel{\text{n.V.}}{\equiv} 0 \pmod{n},$$

also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n.$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Die umgekehrte Richtung

Satz

Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

$$b^{n-1} \equiv 1 \pmod{n} \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \implies n \text{ ist prim.}$$

Beweis.

(durch Widerspruch)

Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \stackrel{\text{n.V.}}{\equiv} 0 \pmod{n},$$

also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n.$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Die umgekehrte Richtung

Satz

Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

$$b^{n-1} \equiv 1 \pmod{n} \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \implies n \text{ ist prim.}$$

Beweis.

(durch Widerspruch)

Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \stackrel{\text{n.V.}}{\equiv} 0 \pmod{n},$$

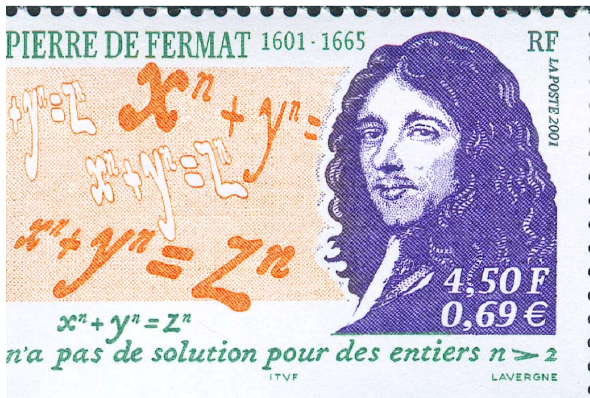
also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n.$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Pierre de Fermat (1601–1665)





Definition

Sei $n \in \mathbb{N}$, $n > 1$. Dann bezeichnet

$$\varphi(n) := |\mathbb{Z}_n^*|$$

die Anzahl der zu n teilerfremden Reste.

Satz

Sei $n \in \mathbb{N}$, $n > 1$. Dann gilt in der Gruppe $\langle \mathbb{Z}_n^*, \times_n, 1 \rangle$:

$$b^{\varphi(n)} = 1 \text{ f\u00fcr alle } b \in \mathbb{Z}_n^* .$$

Beweis.

Folgt sofort aus dem Satz von Lagrange! □

Definition

Sei $n \in \mathbb{N}$, $n > 1$. Dann bezeichnet

$$\varphi(n) := |\mathbb{Z}_n^*|$$

die Anzahl der zu n teilerfremden Reste.

Satz

Sei $n \in \mathbb{N}$, $n > 1$. Dann gilt in der Gruppe $\langle \mathbb{Z}_n^*, \times_n, 1 \rangle$:

$$b^{\varphi(n)} = 1 \text{ f\u00fcr alle } b \in \mathbb{Z}_n^* .$$

Beweis.

Folgt sofort aus dem Satz von Lagrange! □

Definition

Sei $n \in \mathbb{N}$, $n > 1$. Dann bezeichnet

$$\varphi(n) := |\mathbb{Z}_n^*|$$

die Anzahl der zu n teilerfremden Reste.

Satz

Sei $n \in \mathbb{N}$, $n > 1$. Dann gilt in der Gruppe $\langle \mathbb{Z}_n^*, \times_n, 1 \rangle$:

$$b^{\varphi(n)} = 1 \text{ f\u00fcr alle } b \in \mathbb{Z}_n^* .$$

Beweis.

Folgt sofort aus dem Satz von Lagrange! □

Leonhard Euler (1707–1783)



Leonhard Euler (1707–1783)



2.5.6 Zyklische Gruppen

Definition

Eine Gruppe $G = \langle S, \circ, 1 \rangle$ heißt **zyklisch**, wenn es ein $b \in G$ gibt, so dass

$$G = S_b$$

wobei $S_b = \langle \{b^i \mid i \in \mathbb{Z}\}, \circ, 1 \rangle$.

Satz

17 Sei G eine zyklische Gruppe. Falls G unendlich ist, ist G zu $\langle \mathbb{Z}, +, 0 \rangle$ isomorph; falls G endlich ist, dann ist G isomorph zu $\langle \mathbb{Z}_m, +_m, 0 \rangle$ für ein $m \in \mathbb{N}$.

2.5.6 Zyklische Gruppen

Definition

Eine Gruppe $G = \langle S, \circ, 1 \rangle$ heißt **zyklisch**, wenn es ein $b \in G$ gibt, so dass

$$G = S_b$$

wobei $S_b = \langle \{b^i \mid i \in \mathbb{Z}\}, \circ, 1 \rangle$.

Satz

17 Sei G eine zyklische Gruppe. Falls G unendlich ist, ist G zu $\langle \mathbb{Z}, +, 0 \rangle$ isomorph; falls G endlich ist, dann ist G isomorph zu $\langle \mathbb{Z}_m, +_m, 0 \rangle$ für ein $m \in \mathbb{N}$.

Beweis:

1. Fall: Sei G unendlich. Wir wissen: $G = \{b^i \mid i \in \mathbb{Z}\}$ für ein geeignetes $b \in G$, nach Voraussetzung. Betrachte die Abbildung

$$h : \mathbb{Z} \ni i \mapsto b^i \in G$$

Behauptung: h ist bijektiv.

Nach Voraussetzung ist h surjektiv.

Die Injektivität beweisen wir mittels Widerspruch. Annahme:

$$(\exists i, j, i \neq j)[b^i = b^j]$$

Daraus folgt:

$$b^{i-j} = 1$$

Daher ist G endlich, es gilt nämlich:

$$G \subseteq \{b^k; 0 \leq k < |i - j|\}$$

Dies ist ein Widerspruch zur Annahme, G sei unendlich!

2. Fall: G endlich:

Wiederum ist die Abbildung h nach Voraussetzung surjektiv.

Nach dem Schubfachprinzip

$$(\exists i, j, i \neq j)[b^i = b^j] .$$

Nach der Kürzungsregel können wir $j = 0$ wählen. Falls $i > 0$ und i minimal gewählt wird, folgt sofort

$$G \text{ isomorph } \langle \mathbb{Z}_i, +_i, 0 \rangle .$$

q. e. d.

2. Fall: G endlich:

Wiederum ist die Abbildung h nach Voraussetzung surjektiv.

Nach dem Schubfachprinzip

$$(\exists i, j, i \neq j)[b^i = b^j] .$$

Nach der Kürzungsregel können wir $j = 0$ wählen. Falls $i > 0$ und i minimal gewählt wird, folgt sofort

$$G \text{ isomorph } \langle \mathbb{Z}_i, +_i, 0 \rangle .$$

q. e. d.

Satz

18 Jede Untergruppe einer zyklischen Gruppe ist wieder zyklisch.

Beweis.

Sei G zyklisch, $H \subseteq G$ Untergruppe von G .

1. Fall: $|G| = \infty$, also $G \cong \langle \mathbb{Z}, +, 0 \rangle$ (\cong isomorph).

Sei H' die durch den Isomorphismus gegebene Untergruppe von $\langle \mathbb{Z}, +, 0 \rangle$, die H entspricht.

Zu zeigen ist: H' ist zyklisch.

Sei $i := \min \{ k \in H'; k > 0 \}$.

Die Behauptung ist:

$$H = S_i.$$

Es gilt sicher:

$$S_i \subseteq H'.$$

Falls ein $k \in H' \setminus S_i$ existiert, folgt $k \bmod i \in H'$. Dies stellt einen Widerspruch zur Wahl von i dar. Also ist $H' = S_i$, damit ist gezeigt, dass H zyklisch ist.

2. Fall: $|G| < \infty$: Der Beweis läuft analog.



Beweis.

Sei G zyklisch, $H \subseteq G$ Untergruppe von G .

1. Fall: $|G| = \infty$, also $G \cong \langle \mathbb{Z}, +, 0 \rangle$ (\cong isomorph).

Sei H' die durch den Isomorphismus gegebene Untergruppe von $\langle \mathbb{Z}, +, 0 \rangle$, die H entspricht.

Zu zeigen ist: H' ist zyklisch.

Sei $i := \min \{ k \in H'; k > 0 \}$.

Die Behauptung ist:

$$H = S_i.$$

Es gilt sicher:

$$S_i \subseteq H'.$$

Falls ein $k \in H' \setminus S_i$ existiert, folgt $k \bmod i \in H'$. Dies stellt einen Widerspruch zur Wahl von i dar. Also ist $H' = S_i$, damit ist gezeigt, dass H zyklisch ist.

2. Fall: $|G| < \infty$: Der Beweis läuft analog.



2.5.7 Transformationsgruppen

Definition

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 (Darstellungssatz für Gruppen)

Jede Gruppe ist isomorph zu einer Transformationsgruppe.

Beweis. Sei $G = \langle S, \circ, 1 \rangle$, $g \in G$. 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 $\tilde{G} := \langle \tilde{S}, \circ, \tilde{1} \rangle$ mit $\tilde{S} = \{\tilde{g}; g \in G\}$. Die Abbildung

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

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

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

2.5.7 Transformationsgruppen

Definition

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 (Darstellungssatz für Gruppen)

Jede Gruppe ist isomorph zu einer Transformationsgruppe.

Beweis. Sei $G = \langle S, \circ, 1 \rangle$, $g \in G$. 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 $\tilde{G} := \langle \tilde{S}, \circ, \tilde{1} \rangle$ mit $\tilde{S} = \{\tilde{g}; g \in G\}$. Die Abbildung

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

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

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

2.5.7 Transformationsgruppen

Definition

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 (Darstellungssatz für Gruppen)

Jede Gruppe ist isomorph zu einer Transformationsgruppe.

Beweis. Sei $G = \langle S, \circ, 1 \rangle$, $g \in G$. 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 $\tilde{G} := \langle \tilde{S}, \circ, \tilde{1} \rangle$ mit $\tilde{S} = \{\tilde{g}; g \in G\}$. Die Abbildung

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

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

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

2.5.7 Transformationsgruppen

Definition

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 (Darstellungssatz für Gruppen)

Jede Gruppe ist isomorph zu einer Transformationsgruppe.

Beweis. Sei $G = \langle S, \circ, 1 \rangle$, $g \in G$. 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 $\tilde{G} := \langle \tilde{S}, \circ, \tilde{1} \rangle$ mit $\tilde{S} = \{\tilde{g}; g \in G\}$. Die Abbildung

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

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

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

2.5.8 Permutationsgruppen

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

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

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

Kürzer schreibt man auch $\pi = (\pi(1) \ \pi(2) \ \pi(3) \ \dots \ \pi(n-1) \ \pi(n))$.

Sei $a \in \{1, 2, 3, \dots, n\}$. Betrachte $a = \pi^0(a), \pi^1(a), \pi^2(a), \pi^3(a), \dots$. 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

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

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

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

eine zyklische Permutation der Zahlen

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

2.5.8 Permutationsgruppen

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

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

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

Kürzer schreibt man auch $\pi = (\pi(1) \ \pi(2) \ \pi(3) \ \dots \ \pi(n-1) \ \pi(n))$.

Sei $a \in \{1, 2, 3, \dots, n\}$. Betrachte $a = \pi^0(a), \pi^1(a), \pi^2(a), \pi^3(a), \dots$

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

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

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

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

eine zyklische Permutation der Zahlen

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

Satz

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

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

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 $\text{ord } \pi = m < n$, dann hätte der Zyklus die Form $(a_0 \ a_1 \ a_2 \ \dots \ a_{m-1})$ und a_m wäre gleich a_0 , was einen Widerspruch zur Voraussetzung darstellt.



Satz

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

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

Dann gilt:

- ❶ $\pi^k(a_i) = a_{(i+k) \bmod n}$
- ❷ π hat die Ordnung n .

Beweis.

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

□

Satz

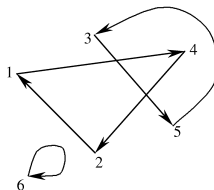
Jede Permutation aus S_n kann als Komposition (von endlich vielen) disjunkten Zyklen dargestellt werden.

Beweis.

Übung! □

Beispiel

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



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

Satz

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

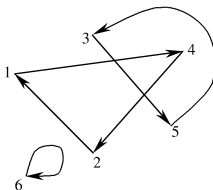
Beweis.

Übung!



Beispiel

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



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

Satz

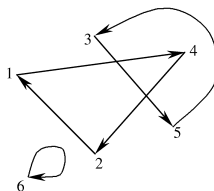
Jede Permutation aus S_n kann als Komposition (von endlich vielen) disjunkten Zyklen dargestellt werden.

Beweis.

Übung! □

Beispiel

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



In diesem Beispiel ist (6) ein **Fixpunkt**, (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: Die Ordnung einer Permutation π ist das kgV der Längen ihrer Zyklen.

Bemerkung: Disjunkte Zyklen können vertauscht werden.
Korollar: Die Ordnung einer Permutation π ist das kgV der Längen ihrer Zyklen.