**Satz.** (Existenz und Eindeutigkeit der Zykelzerlegung)
Jede Permutation $\pi \in S_n$ kann als Produkt von Zykeln $\tau_i$ der Länge $\geq 2$ mit paarweise disjunkten Trägern geschrieben werden,

$$\pi = \tau_1 \cdots \tau_m \ .$$

Die Zykel $\tau_i$ sind bis auf Reihenfolge eindeutig.

*Beweis. Existenz:* Schreibe $M = \{1, 2, \dots, n\}$ und betrachte die zyklische Gruppe $\langle \pi \rangle \leq S_n$. Wir definieren eine Äquivalenzrelation auf $M$ wie folgt: für $m, m' \in M$ gelte $m \sim m'$ genau dann, wenn es ein $\sigma \in \langle \pi \rangle$ gibt mit $\sigma(m) = m'$ (d.h. $m' = \pi^k(m)$ für ein geeignetes $k \in \mathbb{Z}$ – später in der Vorlesung werden wir das eine Bahn der $\langle \pi \rangle$-Wirkung auf $M$ nennen).

Sei $\Lambda := M/\sim$ die Menge der Äquivalenzklassen in $M$. Dann $\bigcup_{A \in \Lambda} = M$, und für $A, B \in \Lambda$ mit $A \neq B$ gilt $A \cap B = \emptyset$ (wobei $A, B$ die Äquivalenzklassen bezeichnen, also insbesondere selber Teilmengen von $M$ sind). Per Konstruktion gilt für jedes $A \in \Lambda$ und eine beliebige Wahl von $m \in A$:

$$A = \{m, \pi(m), \pi^2(m), \dots, \pi^{N-1}(m)\} \ ,$$

wobei $N = |A|$ (Warum?). Setze $m_1 := m$, $m_2 := \pi(m)$, $\dots$, $m_N := \pi^{N-1}(m)$ und definiere den Zykel

$$\tau_A = (m_1 \cdots m_N) \ .$$

Hier benutzen wir unsere Konvention, dass im Fall $N = 1$ die Schreibweise $\tau_A = (m)$ bedeutet, dass $\tau_A$ die Identitätsabbildung ist. Per Konstruktion gilt:

$$\tau_A\big|_B = \begin{cases} \pi_B & ; A = B \\ id_B & ; A \neq B \end{cases}$$

(Warum?). Falls $|A| > 1$ gilt weiterhin, dass $\mathrm{supp}(\tau_A) = A$ (für $|A| = 1$ ist $\tau_A = id$ und der Träger ist die leere Menge). Da insbesondere für $A \neq B$ die Zykel $\tau_A$ und $\tau_B$ disjunkte Träger haben, gilt $\tau_A \tau_B = \tau_B \tau_A$. Schreibe

$$\sigma := \prod_{A \in \Lambda} \tau_A \ ,$$

wobei die Reihenfolge der Komposition der $\tau_A$ wegen der gerade festgestellten Kommutativität irrelevant ist. Für alle $B \in \Lambda$ gilt

$$\sigma\big|_B = \tau_B \big| B = \pi\big|_B \ .$$

(Warum gilt hier die erste Gleichheit?) Definiere $\Lambda' \subset \Lambda$ als die Teilmenge der Äquivalenzklassen mit $|A| \geq 2$. Da $\tau_A = id$, falls $|A| = 1$, gilt insgesamt

$$\pi = \sigma = \prod_{A \in \Lambda'} \tau_A \ .$$

*Eindeutigkeit:* Sei $\pi = \nu_1 \cdots \nu_k$ eine andere Zerlegung wie im Satz. Auf $X := \operatorname{supp}(\nu_i)$ gilt $\pi|_X = \nu_i|_X$, und somit muss $X$ eine Äquivalenzklasse in $\Lambda'$ sein (Warum?). Dies definiert eine injektive Abbildung $\{1, \ldots, k\} \to \Lambda'$. Andererseits gilt

$$\bigcup_{i=1}^{k} \operatorname{supp}(\nu_i) = \operatorname{supp}(\pi) = \bigcup_{A \in \Lambda'} A \ ,$$

so dass diese Abbildung auch surjektiv ist. $\square$