Permutationsgruppen

Jesko Hüttenhain

Winter 2013

Sei N eine endliche Menge. Dann bezeichnen wir mit

$$\mathfrak{S}_N := \{\sigma : N \to N \mid \sigma \text{ bijektiv}\}$$

die **symmetrische Gruppe** auf N. Für $n \in \mathbb{N}$ sei $[n] := \{1, \ldots, n\}$. Wir schreiben auch $\mathfrak{S}_n := \mathfrak{S}_{[n]}$.

1 Zykelzerlegung und Signum

Definition 1. Sei N eine endliche Menge und $A = \{a_0, \ldots, a_{k-1}\} \subseteq N$, wobei $2 \leq k \leq n$ und die a_i paarweise verschieden seien. Wir bezeichnen mit

$$\sigma = (a_0\, a_1\, \cdots\, a_{k-1}) \tag{†}$$

das Element von $\mathfrak{S}_N$, welches definiert ist durch

$$\sigma(x) = \begin{cases} x & ; \quad x \notin A \\ a_{i+1} & ; \quad x = a_i \text{ mit } i + 1 < k \\ a_0 & ; \quad x = a_{k-1}. \end{cases}$$

Wir nennen σ dann einen **Zykel der Länge** k oder auch kurz k**-Zykel**. Die Zykel $(x\, y)$ heißen **Transpositionen**. Sie vertauschen lediglich die Elemente x und y. Wir definieren außerdem $(\,)$ als die Identitätsabbildung mit leerem Träger.

Wir nennen allgemein $A := \{x \in N \mid \sigma(x) \neq x\}$ den **Träger** einer (beliebigen) Permutation $\sigma \in \mathfrak{S}_N$ und $N^\sigma := \{x \in N \mid \sigma(x) = x\}$ die Menge der **Fixpunkte** von σ. ●

Lemma 2. Sei N eine endliche Menge. Wenn $\sigma, \pi \in \mathfrak{S}_N$ disjunkte Träger haben, so gilt $\sigma \circ \pi = \pi \circ \sigma$.

Beweis. Sei $A \subseteq N$ der Träger von σ und $B \subseteq N$ der Träger von π. Sei $x \in N$. Wenn x weder in A noch in B ist, so ist

$$\pi(\sigma(x)) = \pi(x) = x = \sigma(x) = \pi(\sigma(x)).$$

Wenn $x \in A$ mit $y = \sigma(x) \in A$, so sind $x, y \notin B$ und daher $\pi(x) = x$ und $\pi(y) = y$. Es folgt

$$\pi(\sigma(x)) = \pi(y) = y = \sigma(x) = \sigma(\pi(x)).$$

Ein äquivalentes Argument zeigt $\pi(\sigma(x)) = \sigma(\pi(x))$ für den Fall $x \in B$, somit gilt dies also für jedes $x \in N$. Damit ist $\pi \circ \sigma = \sigma \circ \pi$. ∎

Satz 3 (Zykelzerlegung). Sei N eine endliche Menge und $\sigma \in \mathfrak{S}_N$. Dann gibt es eine eindeutige Partition $N = N^\sigma \mathbin{\dot\cup} A_1 \mathbin{\dot\cup} \cdots \mathbin{\dot\cup} A_r$ und Zykel σ_i mit Träger A_i, so dass $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$. Wir nennen dies die **Zykelzerlegung** von σ.

Beweis. Wir dürfen für den Beweis davon ausgehen, dass $N^\sigma = \emptyset$: Die Menge N^σ ist immer eindeutig durch σ bestimmt.

Wir beweisen die Aussage per Induktion nach $n := |N|$. Im Fall $n = 1$ ist die Aussage trivial, da $\mathfrak{S}_N$ in diesem Fall nur aus dem leeren Zykel besteht. Sei also $|N| > 1$. Wähle $x \in N$ und setze $x_i := \sigma^i(x)$ für $i \in \mathbb{N}$, wobei also $x_0 = x$, dann $x_1 = \sigma(x)$ und weiter $x_{i+1} = \sigma(x_i)$. Da N eine endliche Menge ist, gibt es $j, k \in \mathbb{N}$ mit $x_j = x_{j+k}$. Wir fixieren ein j und wählen k minimal mit dieser Eigenschaft. Wir setzen dann $a_i := x_{i+j}$, somit ist $\sigma(a_i) = a_{i+1}$ für alle $i \in \mathbb{N}$ und es gilt $\sigma(a_k) = a_0$.

Wir behaupten, dass es keine Indizes $0 \leq i < j < k$ mit $a_i = a_j$ gibt. Andernfalls wäre $a_{k-(j-i)} = \sigma^{k-j}(a_i) = \sigma^{k-j}(a_j) = a_k = a_0$, doch die strikte Ungleichung $k - (j - i) < k$ widerspricht der Minimalität von k. Da σ keine Fixpunkte hat, ist $k \geq 2$. Damit haben wir gezeigt, dass $A := \{a_0, \ldots, a_{k-1}\}$ eine Menge von $k \geq 2$ paarweise verschiedenen Elementen ist, welche von σ zyklisch abgebildet werden. Insbesondere gilt $\sigma(A) = A$. Sei nun $M := N \setminus A$, dann ist auch $\sigma(M) = M$, da σ bijektiv ist. Die Permutation $\pi := \sigma|_M$ ist eine bijektive Abbildung der kleineren Menge M. Mit $\sigma_1 := (a_0 \cdots a_{k-1})$ gilt nun $\sigma = \sigma_1 \circ \pi = \pi \circ \sigma$, letzteres gemäß Lemma 2. Nach Induktionsvoraussetzung lässt sich $\pi \in \mathfrak{S}_M$ eindeutig in Zykel zerlegen, damit ist die Existenz der Zerlegung bewiesen. Die Zerlegung ist außerdem eindeutig, weil die Zykelzerlegung von $\pi = \sigma|_M$ und die Zykelzerlegung von $\sigma_1 = \sigma|_A$ eindeutig sind. ■

Korollar 4. Die Gruppe $\mathfrak{S}_n$ wird erzeugt von
(1) den Transpositionen.
(2) den Transpositionen $(x \mapsto x+1)$.
Solche Transpositionen nennen wir auch **Nachbarschaftsvertauschungen**.

Beweis. Man kann leicht überprüfen, dass

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

Also folgt 1 aus Satz 3. Es genügt für 2, eine Transposition $(x\,y)$ als Verkettung von Nachbarschaftsvertauschungen zu schreiben. Wir nehmen ohne Einschränkung an, dass $x < y$. Wir führen Induktion nach $y - x$. Für $y - x = 1$ sind wir fertig, sei also $z := y - 1 > x$. Dann ist

$$(z\,y) \circ (x\,z) \circ (z\,y) = (x\,y),$$

und wir können nach Induktionsvoraussetzung $(x\,z)$ als Verkettung von Nachbarschaftsvertauschungen schreiben. Damit sind wir fertig. ■

Definition 5. Wenn $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ die Zykelzerlegung von $\sigma \in \mathfrak{S}_n$ ist und σ_i die Länge μ_i hat, so setzen wir $(-1)^\sigma := (-1)^{\mu_1 - 1} \cdots (-1)^{\mu_r - 1}$. Wir nennen dies das **Signum** von σ. ●

Definition 6. Sei N eine endliche Menge. Wir bezeichnen mit

$$\binom{N}{k} := \{K \subseteq N \mid k = |K|\}$$

die Menge aller k-elementigen Teilmengen von N. Die Notation stammt daher, dass für $n = |N|$ die Formel $\left|\binom{N}{k}\right| = \binom{n}{k}$ gilt.

Sei nun $\sigma \in \mathfrak{S}_n$. Für $\{i, j\} \in \binom{[n]}{2}$ ist der Ausdruck

$$\frac{\sigma(i) - \sigma(j)}{i - j} = \frac{\sigma(j) - \sigma(i)}{j - i}$$

unabhängig von der Ordnung der Elemente i und j, daher können wir

$$\operatorname{sgn}(\sigma) := \prod_{\substack{\{i,j\}\subseteq[n]\\ i\neq j}} \frac{\sigma(i)-\sigma(j)}{i-j}$$

definieren. Anhand der Definition ist zunächst lediglich $\operatorname{sgn}(\sigma) \in \mathbb{Q}$, wir werden jedoch später sehen, dass $\operatorname{sgn}(\sigma) \in \{\pm 1\}$. Wir nennen $\{i,j\} \in \binom{[n]}{2}$ einen **Fehlstand** von $\sigma \in \mathfrak{S}_n$, wenn $\frac{\sigma(i)-\sigma(j)}{i-j} < 0$ gilt. Damit wissen wir bereits, dass das Vorzeichen von $\operatorname{sgn}(\sigma)$ genau dann negativ ist, wenn es eine ungerade Anzahl Fehlstände gibt. ●

Lemma 7. Für $\sigma, \pi \in \mathfrak{S}_n$ gilt $\operatorname{sgn}(\sigma \circ \pi) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\pi)$.

Beweis. Wir berechnen

$$\begin{aligned}
\operatorname{sgn}(\sigma\circ\pi) &= \prod_{\substack{\{i,j\}\subseteq[n]\\ i\neq j}} \frac{\sigma(\pi(i))-\sigma(\pi(j))}{i-j} \\
&= \prod_{\substack{\{i,j\}\subseteq[n]\\ i\neq j}} \frac{\sigma(\pi(i))-\sigma(\pi(j))}{\pi(i)-\pi(j)} \cdot \frac{\pi(i)-\pi(j)}{i-j} \\
&= \prod_{\substack{\{i,j\}\subseteq[n]\\ i\neq j}} \frac{\sigma(\pi(i))-\sigma(\pi(j))}{\pi(i)-\pi(j)} \cdot \operatorname{sgn}(\pi) \\
&= \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\pi).
\end{aligned}$$

Die letzte Gleichheit folgt, da $\{i,j\} \mapsto \{\pi(i),\pi(j)\}$ eine Bijektion auf den zweielementigen Teilmengen $\binom{[n]}{2} \to \binom{[n]}{2}$ definiert. ■

Lemma 8. Für einen k-Zykel $\sigma = (a_1 \cdots a_k) \in \mathfrak{S}_n$ gilt $\operatorname{sgn}(\sigma) = (-1)^{k-1}$.

Beweis. Wegen ($\star$) und Lemma 7 genügt es, für eine beliebige Transposition $\tau = (x\,y)$ zu zeigen, dass $\operatorname{sgn}(\tau) = -1$. Sei $M := [n] \setminus \{x,y\}$. Dann ist

$$\begin{aligned}
\operatorname{sgn}(\tau) &= \frac{y-x}{x-y} \cdot \prod_{i\in M} \frac{\tau(i)-\tau(x)}{i-x} \cdot \frac{\tau(i)-\tau(y)}{i-y} \cdot \prod_{\{i,j\}\in\binom{M}{2}} \frac{\tau(i)-\tau(j)}{i-j} \\
&= \frac{y-x}{x-y} \cdot \prod_{i\in M} \frac{i-y}{i-x} \cdot \frac{i-x}{i-y} \cdot \prod_{\{i,j\}\in\binom{M}{2}} \frac{i-j}{i-j} = \frac{y-x}{x-y} = -1.
\end{aligned}$$

■

Theorem 9. Für $\sigma \in \mathfrak{S}_n$ ist $\operatorname{sgn}(\sigma) = (-1)^\sigma$. Die Abbildung

$$\begin{aligned} \operatorname{sgn}_n \colon \mathfrak{S}_n &\longrightarrow \{\pm 1\} \\ \sigma &\longmapsto (-1)^\sigma \end{aligned}$$

ist ein Gruppenhomomorphismus.

Beweis. Wegen Satz 3 und Lemma 8 ist $\operatorname{sgn}(\sigma) = (-1)^\sigma$. Daraus folgt, dass $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ für alle $\sigma \in \mathfrak{S}_n$ und Lemma 7 besagt, dass sgn ein Gruppenhomomorphismus ist. ■

Korollar 10. Sei $\sigma \in \mathfrak{S}_n$ und $k \in \mathbb{N}$ die Anzahl der Fehlstände von σ. Dann ist $\operatorname{sgn}(\sigma) = (-1)^k$. ■

Definition 11. Sei N eine endliche Menge. Wir definieren $\operatorname{sgn}_N \colon \mathfrak{S}_N \to \{\pm 1\}$ durch $\operatorname{sgn}_N(\sigma) := (-1)^\sigma$. Diese Abbildung ist gemäß Theorem 9 ein Gruppenhomomorphismus. ●

Definition 12. Wir definieren die **alternierende Gruppe**

$$\mathfrak{A}_N := \ker(\operatorname{sgn}_N) = \{\sigma \in \mathfrak{S}_N \mid (-1)^\sigma = 1\}\,.$$

Wir nennen Permutationen σ **gerade**, wenn $(-1)^\sigma = 1$ und **ungerade**, falls $(-1)^\sigma = -1$. Die alternierende Gruppe besteht also aus den geraden Permutationen. Da die Identität gerade ist, bilden die ungeraden Permutationen keine Untergruppe. ●

2 Konjugationswirkung

Wir interessieren uns nun für die Kojugationsklassen der Gruppe $\mathfrak{S}_N$. Dazu lassen wir $\mathfrak{S}_N$ auf sich selbst durch Konjugation wirken, wir betrachten also die Abbildung

$$\begin{aligned} \alpha : \mathfrak{S}_N \times \mathfrak{S}_N &\longrightarrow \mathfrak{S}_N \\ (\pi, \sigma) &\longmapsto \pi\sigma\pi^{-1} \end{aligned}$$

und fragen uns nach den Bahnen dieser Abbildung. Das Studium einzelner Zykel hilft uns auch in diesem Fall:

Satz 13. Sei $\sigma = (a_1 \cdots a_k)$ ein k-Zykel und $\pi \in \mathfrak{S}_N$ eine Permutation. Sei $b_i = \pi(a_i)$. Dann ist $\pi\sigma\pi^{-1} = (b_1 \cdots b_k)$ ebenfalls ein k-Zykel.

Beweis. Es ist sicherlich $(\pi\sigma\pi^{-1})(b_i) = (\pi\sigma)(a_i) = \pi(a_{i+1}) = b_{i+1}$. Sei $A = \{a_1, \ldots, a_k\}$ der Träger von σ. Wenn dann $b \in N \setminus \pi(A)$, so ist auch $a := \pi^{-1}(b) \in N \setminus A$. Also ist $(\pi\sigma\pi^{-1})(b) = (\pi\sigma)(a) = \pi(a) = b$. ■

Definition 14. Sei $\sigma \in \mathfrak{S}_N$ und $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ die Zykelzerlegung von σ. Sei σ_i ein Zykel der Länge μ_i. Wir ordnen die μ_i derart, dass $\mu_1 \geq \cdots \geq \mu_r$ gilt. Dann ist $\mu = (\mu_1, \ldots, \mu_r)$ der **Zykeltyp** von σ. ●

Theorem 15. Die Bahnen unter der Konjugationswirkung von $\mathfrak{S}_N$ auf sich selbst bestehen aus Permutationen mit gleichem Zykeltyp.

Beweis. Seien $\varrho, \sigma \in \mathfrak{S}_N$ Permutationen mit Zykelzerlegungen $\varrho = \varrho_1 \circ \ldots \circ \varrho_r$ und $\sigma = \sigma_1 \circ \ldots \circ \sigma_s$. Wir sortieren die Zykel dabei jeweils absteigend nach Länge. Sei jeweils A_i der Träger von σ_i und B_j der Träger von ϱ_j.

Wenn $\pi \in \mathfrak{S}_N$ eine Permutation mit $\pi\sigma\pi^{-1} = \varrho$ ist, so ist

$$\begin{aligned}
\varrho_1 \circ \ldots \circ \varrho_r &= \pi \circ \sigma \circ \pi^{-1} \\
&= \pi \circ \sigma_1 \circ \ldots \circ \sigma_s \circ \pi^{-1} \\
&= \pi \circ \sigma_1 \circ (\pi^{-1} \circ \pi) \circ \sigma_2 \circ (\pi \circ \pi^{-1}) \circ \ldots \circ (\pi \circ \pi^{-1}) \circ \sigma_s \circ \pi^{-1} \\
&= (\pi\sigma_1\pi^{-1}) \circ \ldots \circ (\pi\sigma_s\pi^{-1}).
\end{aligned}$$

Nach Satz 13 ist beides eine Zykelzerlegung von ϱ: Da die Träger der σ_i disjunkt sind, sind gemäß Satz 13 auch die Träger ihrer Konjugierten disjunkt. Da die Zykelzerlegung eindeutig ist, gilt ohne Einschränkung $r = s$ und $\varrho_i = \pi\sigma_i\pi^{-1}$. Erneut nach Satz 13 haben ϱ_i und σ_i die gleiche Länge für alle $1 \leq i \leq r$, also haben ϱ und σ gleichen Zykeltyp.

Wir zeigen nun die andere Richtung: Wenn ϱ und σ den gleichen Zykeltyp haben, so is $r = s$ und $|N^\sigma| = |N^\varrho|$. Fixiere einen Index $1 \leq i \leq r$. Wenn $A_i = \{a_1, \ldots, a_k\}$ und $B_i = \{b_1, \ldots, b_k\}$ so nummeriert sind, dass $\sigma_i = (a_1 \ldots a_k)$ und $\varrho_i = (b_1 \ldots b_k)$, so definieren wir die Bijektion $p_i \colon A_i \to B_i$ durch $p_i(a_j) = b_j$.

Es gibt außerdem auch eine Bijektion $p_0\colon N^\sigma \to N^\varrho$, insgesamt ergeben diese Abbildungen eine Bijektion $\pi \in \mathfrak{S}_N$, mittels $\pi|_{A_i} = p_i$ und $\pi|_{N^\sigma} = p_0$, also

$$\begin{array}{ccccccccccc} N^\sigma & \dot\cup & A_1 & \dot\cup & A_2 & \dot\cup & \cdots & \dot\cup & A_r & = & N \\ \downarrow{\scriptstyle p_0} & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle p_2} & & \cdots & & \downarrow{\scriptstyle p_r} & & \downarrow{\scriptstyle \pi} \\ N^\varrho & \dot\cup & B_1 & \dot\cup & B_2 & \dot\cup & \cdots & \dot\cup & B_r & = & N \end{array}$$

Nach Satz 13 ist nun $\pi\sigma\pi^{-1} = \varrho$. ■

Definition 16. Sei G eine Gruppe, im Folgenden meistens eine Untergruppe der $\mathfrak{S}_N$. Wir bezeichnen mit

$$Z_G(\sigma) := \left\{\pi \in G \,\middle|\, \pi\sigma\pi^{-1} = \sigma\right\}$$

den Zentralisator von σ in G, also den Stabilisator von σ unter der Konjugationswirkung. Wir schreiben $C_G(\sigma) := \{\pi\sigma\pi^{-1} \mid \pi \in G\}$ für die Konjugationsklasse, also die Bahn von σ unter der Konjugationswirkung. ●

Lemma 17. Sei $\sigma \in \mathfrak{S}_n$ vom Zykeltyp $\mu = (\mu_1, \dots, \mu_r)$. Bezeichne die Anzahl der k-Zykel, die im Zykeltyp von σ vorkommen, mit $c_k := |\{i \in [r] \mid \mu_i = k\}|$. Dann gilt

$$|Z_{\mathfrak{S}_n}(\sigma)| = \prod_{k=1}^{n} c_k! \cdot k^{c_k}.$$

Beweis. Sei $\pi \in \mathfrak{S}_n$ mit $\pi\sigma\pi^{-1} = \sigma$. Nach Satz 13 muss dann π die Elemente jedes k-Zykels von σ bis auf Indexverschiebung in gleicher Reihenfolge auf die Elemente eines anderen k-Zykels in σ abbilden. Bis auf Permutation der k-Zykel untereinander gibt es dafür gerade k Möglichkeiten pro k-Zykel. ■

Bemerkung 18. Mit Lemma 17 kann man auch die Größe der Konjugationsklasse $C_{\mathfrak{S}_n}(\sigma)$ von σ ausrechnen. Nach der Bahnformel gilt

$$|C_{\mathfrak{S}_n}(\sigma)| \cdot |Z_{\mathfrak{S}_n}(\sigma)| = |\mathfrak{S}_n| = n!.$$ ●

Satz 19. Sei τ eine Transposition in $\mathfrak{S}_n$. Für jede Permutation $\sigma \in \mathfrak{A}_n$ gilt:
(1) Wenn $Z_{\mathfrak{S}_n}(\sigma) \subseteq \mathfrak{A}_n$, dann gilt
$Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$ und $C_{\mathfrak{S}_n}(\sigma) = C_{\mathfrak{A}_n}(\sigma) \,\dot\cup\, C_{\mathfrak{A}_n}(\tau\sigma\tau^{-1})$.

(2) Wenn $Z_{\mathfrak{S}_n}(\sigma) \not\subset \mathfrak{A}_n$, dann gilt
$(Z_{\mathfrak{S}_n}(\sigma) : Z_{\mathfrak{A}_n}(\sigma)) = 2$ und $C_{\mathfrak{S}_n}(\sigma) = C_{\mathfrak{A}_n}(\sigma)$.

Beweis. Sei $s := \operatorname{sgn}|_{Z_{\mathfrak{S}_n}(\sigma)}$, dann ist $Z_{\mathfrak{A}_n}(\sigma) = Z_{\mathfrak{S}_n}(\sigma) \cap \mathfrak{A}_n = \ker(s)$ und die universelle Eigenschaft liefert einen Gruppenhomomorphismus ϕ, wobei

$$\begin{tikzcd} Z_{\mathfrak{S}_n(\sigma)} \arrow[d, two heads] \arrow[dr, "s"] \arrow[dr, phantom, "\circlearrowleft", shift right=3ex] & \\ Z_{\mathfrak{S}_n(\sigma)}/Z_{\mathfrak{A}_n(\sigma)} \arrow[r, dotted, "\phi"] & \{\pm 1\} \end{tikzcd}$$

Es ist ϕ ein Isomorphismus von $Z_{\mathfrak{S}_n(\sigma)}/Z_{\mathfrak{A}_n(\sigma)}$ auf $\operatorname{im}(s)$. Daraus folgt

$$I := (Z_{\mathfrak{S}_n(\sigma)} : Z_{\mathfrak{A}_n(\sigma)}) = |\operatorname{im}(s)| \in \{1, 2\}\,,$$

i.e. $Z_{\mathfrak{A}_n(\sigma)}$ ist vom Index 1 oder 2 in $Z_{\mathfrak{S}_n}(\sigma)$ – je nachdem, ob $Z_{\mathfrak{S}_n}(\sigma)$ nur gerade Permutationen enthält oder nicht. Im Falle $I = 1$ folgt aus

$$2 \cdot |C_{\mathfrak{A}_n}(\sigma)| \cdot |Z_{\mathfrak{A}_n}(\sigma)| = 2 \cdot |\mathfrak{A}_n| = |\mathfrak{S}_n| = |C_{\mathfrak{S}_n}(\sigma)| \cdot |Z_{\mathfrak{S}_n}(\sigma)|\,,$$

dass $2 \cdot |C_{\mathfrak{A}_n}(\sigma)| = |C_{\mathfrak{S}_n}(\sigma)|$. Sei dann $\pi \in C_{\mathfrak{S}_n}(\sigma) \setminus C_{\mathfrak{A}_n}(\sigma)$. Dann ist $\pi = \varrho\sigma\varrho^{-1}$. Es ist $\varrho\tau^{-1} \in \mathfrak{A}_n$ und wir erhalten

$$(\varrho\tau^{-1})(\tau\sigma\tau^{-1})(\varrho\tau^{-1})^{-1} = \varrho(\tau\tau^{-1})\sigma(\tau\tau^{-1})\varrho^{-1} = \varrho\sigma\varrho^{-1} = \pi,$$

also $\pi \in C_{\mathfrak{A}_n}(\tau\sigma\tau^{-1})$. Im Fall $I = 2$ ist $|C_{\mathfrak{A}_n}(\sigma)| = |C_{\mathfrak{S}_n}(\sigma)|$. ∎

Beispiel 20. Wir erhalten Tabelle 1 mittels Lemma 17 und Bemerkung 18.

Zykel von σ	$\lvert Z_{\mathfrak{S}_5}(\sigma)\rvert$	$\lvert C_{\mathfrak{S}_5}(\sigma)\rvert$	$\operatorname{ord}(\sigma)$	$\operatorname{sgn}(\sigma)$
$(1)(2)(3)(4)(5)$	$5! = 120$	1	1	$+1$
$(1\,2)(3)(4)(5)$	$3! \cdot 2 = 12$	10	2	-1
$(1\,2\,3)(4)(5)$	$2! \cdot 3 = 6$	20	3	$+1$
$(1\,2\,3\,4)(5)$	$1! \cdot 4 = 4$	30	4	-1
$(1\,2\,3\,4\,5)$	$0! \cdot 5 = 5$	24	5	$+1$
$(1\,2)(3\,4)(5)$	$2! \cdot 2^2 = 8$	15	2	$+1$
$(1\,2\,3)(4\,5)$	$3 \cdot 2 = 6$	20	3	-1

Tabelle 1: Konjugationsklassen von $\mathfrak{S}_5$

Wie man sieht, summiert sich die Gesamtzahl der Elemente zu $120 = 5!$. Die Gruppe $\mathfrak{S}_5$ operiert durch Konjugation auf der normalen Untergruppe $\mathfrak{A}_5$. Diese zerfällt in die obigen $\mathfrak{S}_5$-Bahnen, die Signum $+1$ haben. Ihre Elementezahl summiert sich zu $60 = \frac{5!}{2}$. Wir behaupten nun, dass die Informationen in Tabelle 2 (siehe unten) korrekt sind.

Zykel von σ	$\lvert Z_{\mathfrak{A}_4}(\sigma)\rvert$	$\lvert C_{\mathfrak{A}_5}(\sigma)\rvert$	$\mathrm{ord}(\sigma)$
$(1)(2)(3)(4)(5)$	60	1	1
$(1\,2\,3)(4)(5)$	3	20	3
$(1\,2\,3\,4\,5)$	5	12	5
$(1\,2\,3\,5\,4)$	5	12	5
$(1\,2)(3\,4)(5)$	4	15	2

Tabelle 2: Konjugationsklassen von $\mathfrak{A}_5$

Zunächst ist leicht zu sehen, dass alle 3-Zykel in $\mathfrak{A}_5$ konjugiert bleiben. Wenn $\sigma \in \mathfrak{A}_5$ ein 3-Zykel ist, so gibt es ein $\pi \in \mathfrak{S}_5$ mit $\pi\sigma\pi^{-1} = (1\,2\,3)$. Dieses π muss zwei Elemente $x, y \in [n]$ fest lassen. Wenn $\pi \notin \mathfrak{A}_5$, so können wir π durch $\pi \circ (x\,y)$ ersetzen.

Die 5-Zykel liegen zwar in einer $\mathfrak{S}_5$-Konjugationsklasse, zerfallen in $\mathfrak{A}_5$ jedoch. Für den Zykel $\sigma = (1\,2\,3\,4\,5)$ gilt nämlich $Z_{\mathfrak{S}_n}(\sigma) = \langle\sigma\rangle \subseteq \mathfrak{A}_5$ und wir erhalten das Ergebnis mit Satz 19.

Schlussendlich bleiben Produkte von zwei disjunkten Transpositionen in $\mathfrak{A}_n$ konjugiert. In der Tat vertauscht bereits eine einzelne Transposition mit einer solchen Permutation und nach Satz 19 folgt die Behauptung. ●

Wir zeigen als Anwendung noch, dass die Gruppe $\mathfrak{A}_5$ keinen echten Normalteiler hat. Die Aussage gilt ebenso für alle $\mathfrak{A}_n$ mit $n \geq 5$. Dieses Resultat ist eine wichtige Zutat für den Beweis, dass man polynomielle Gleichungen vom Grad größer oder gleich 5 nicht durch „Radikale“ auflösbar ist.

Theorem 21. Die Gruppe $\mathfrak{A}_5$ hat keine nichttrivialen Normalteiler.

Beweis. Sei $K \lhd \mathfrak{A}_5$ ein Normalteiler. Nach dem Satz von Lagrange wissen wir $|K| \cdot (\mathfrak{A}_5 : K) = |\mathfrak{A}_5| = \frac{5!}{2} = \frac{120}{2} = 60$, also muss $k := |K|$ ein Teiler von $60 = 2^2 \cdot 3 \cdot 5$ sein. Außerdem ist K normal, d.h. es ist invariant unter der

Konjugationswirkung, insbesondere ist K die Vereinigung von Konjugationsklassen. Nach Tabelle 2 haben diese jedoch 1, 20, 12, 12 und 15 Elemente. Da $1 \in K$, muss k die Summe von 1 und beliebig vielen der anderen Zahlen sein. Keine solche Zahl, bis auf 1 und 60, ist ein Teiler von 60. ∎