Musterlösung Serie 4

Symmetrische Gruppe

1. Konstruiere für jedes $n \geqslant 1$ einen injektiven Homomorphismus $S_n \hookrightarrow A_{n+2}$.

   Lösung: Zu jeder Permutation $\sigma \in S_n$ assoziieren wir die Permutation $i(\sigma) \in S_n$, die auf der Teilmenge $\{1, \ldots, n\}$ wie σ operiert und die Punkte $n+1$ und $n+2$ festlässt. Offensichtlich ist dies ein injektiver Homomorphismus $i\colon S_n \hookrightarrow S_{n+2}$. Sodann betrachten wir die Transposition $\tau := (n+1\ n+2) \in S_{n+2}$. Da diese die Ordnung 2 hat, haben wir einen eindeutigen Isomorphismus von der multiplikativen Gruppe $t\colon \{\pm 1\} \xrightarrow{\sim} \langle\tau\rangle$ mit $t(-1) = \tau$. Betrachte nun die Abbildung

$$\varphi\colon S_n \to S_{n+1}, \quad \sigma \mapsto i(\sigma)t(\operatorname{sgn}(\sigma)).$$

   Da i und $t \circ \operatorname{sgn}$ Homomorphismen sind und $\operatorname{Bild}(i)$ mit $\operatorname{Bild}(t)$ kommutiert, ist dies ein Homomorphismus; das heisst, für alle $\sigma, \sigma' \in S_n$ gilt

$$\begin{aligned}\varphi(\sigma\sigma') &= i(\sigma\sigma')t(\operatorname{sgn}(\sigma\sigma')) = i(\sigma)i(\sigma')t(\operatorname{sgn}(\sigma))t(\operatorname{sgn}(\sigma')) \\ &= i(\sigma)t(\operatorname{sgn}(\sigma))i(\sigma')t(\operatorname{sgn}(\sigma')) = \varphi(\sigma)\varphi(\sigma').\end{aligned}$$

   Für alle $\sigma \in S_n$ und alle $1 \leqslant a \leqslant n$ gilt nach Konstruktion $\varphi(\sigma(a)) = \sigma(a)$; somit ist φ injektiv. Nach Konstruktion gilt weiter $\operatorname{sgn}(i(\sigma)) = \operatorname{sgn}(\sigma)$ sowie $\operatorname{sgn}(t(e)) = e$ für alle $e \in \{\pm 1\}$, und daher

$$\operatorname{sgn}(\varphi(\sigma)) = \operatorname{sgn}(i(\sigma)t(\operatorname{sgn}(\sigma))) = \operatorname{sgn}(i(\sigma))\operatorname{sgn}(t(\operatorname{sgn}(\sigma))) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma) = 1.$$

   Somit ist $\operatorname{Bild}(\varphi) \subset A_{n+2}$.

2. (a) Bestimme für jedes n das Zentrum der symmetrischen Gruppe S_n.

   (b) Berechne den Zentralisator von $(2\ 3\ 4)$ in S_5.

   (c) Berechne den Zentralisator von $(1\ 2\ 3)(4\ 5\ 6)$ in S_7.

   Lösung: (a) Für $n \leqslant 2$ ist S_n abelsch, also $Z(S_n) = S_n$. Sei nun $n \geqslant 3$ und $\sigma \neq \mathrm{id}$ ein nicht-triviales Element von S_n. Dann gibt es ein i mit $\sigma(i) \neq i$ und ein $k \notin \{i, \sigma(i)\}$. Für die Transposition $\tau := (\sigma(i)\ k)$ gilt dann

$$(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i) \neq k = \tau(\sigma(i)) = (\tau\sigma)(i),$$

   und daher $\sigma\tau \neq \tau\sigma$. Somit ist $\sigma \notin Z(S_n)$, und es folgt $Z(S_n) = \{\mathrm{id}\}$.

   (b) Eine Permutation $\sigma \in S_5$ liegt genau dann im Zentralisator von $(2\ 3\ 4)$, wenn

$$(2\ 3\ 4) = \sigma(2\ 3\ 4)\sigma^{-1} = (\sigma(2)\ \sigma(3)\ \sigma(4))$$

ist. Allgemein gilt nun für Dreizykel

$$(a\ b\ c) = (d\ e\ f) \;\Leftrightarrow\; (d, e, f) \in \{(a, b, c),\ (b, c, a),\ (c, a, b)\}. \tag{1}$$

Somit muss σ die Teilmenge $\{2, 3, 4\}$ in sich abbilden, und für die Einschränkung von σ auf $\{2, 3, 4\}$ gibt es nur die drei Möglichkeiten id, $(2\ 3\ 4)$, $(2\ 4\ 3)$. Ausserdem muss auch das Komplement $\{1, 5\}$ auf sich abgebildet werden, und für die Einschränkung von σ auf $\{1, 5\}$ gibt es nur die Möglichkeiten id, $(1\ 5)$. Insgesamt besteht der Zentralisator von $(2\ 3\ 4)$ also aus den 6 Permutationen

$$\mathrm{id},\ (2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 5),\ (1\ 5)(2\ 3\ 4),\ (1\ 5)(2\ 4\ 3).$$

(c) Eine Permutation $\sigma \in S_7$ liegt genau dann im Zentralisator von $(1\ 2\ 3)(4\ 5\ 6)$, wenn

$$(1\ 2\ 3)(4\ 5\ 6) = \sigma(1\ 2\ 3)(4\ 5\ 6)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3))(\sigma(4)\ \sigma(5)\ \sigma(6))$$

ist. Diese Gleichheit gilt in den beiden Fällen

$$\begin{aligned}
&(1\ 2\ 3) = (\sigma(1)\ \sigma(2)\ \sigma(3)) \quad \text{und} \quad (4\ 5\ 6) = (\sigma(4)\ \sigma(5)\ \sigma(6)), \quad \text{bzw.} \\
&(1\ 2\ 3) = (\sigma(4)\ \sigma(5)\ \sigma(6)) \quad \text{und} \quad (4\ 5\ 6) = (\sigma(1)\ \sigma(2)\ \sigma(3)).
\end{aligned}$$

Nach der obigen Gleichung (1) gibt es in jedem dieser Fälle genau $3 \cdot 3 = 9$ Möglichkeiten für die Einschränkung $\sigma|\{1, 2, 3, 4, 5, 6\}$. Dabei wird $\{1, 2, 3, 4, 5, 6\}$ bijektiv auf sich abgebildet, darum muss $\sigma(7) = 7$ sein. Somit hat der Zentralisator von $(1\ 2\ 3)(4\ 5\ 6)$ genau $2 \cdot 9 = 18$ Elemente. Im Einzelnen erhalten wir

$$\begin{aligned}
Z_{S_7}((1\ 2\ 3)(4\ 5\ 6)) \;=\; \{\, &\mathrm{id}, (4\ 5\ 6), (4\ 6\ 5), \\
&(1\ 2\ 3), (1\ 2\ 3)(4\ 5\ 6), (1\ 2\ 3)(4\ 6\ 5), \\
&(1\ 3\ 2), (1\ 3\ 2)(4\ 5\ 6), (1\ 3\ 2)(4\ 6\ 5), \\
&(1\ 4)(2\ 5)(3\ 6), (1\ 4\ 2\ 5\ 3\ 6), (1\ 4\ 3\ 6\ 2\ 5), \\
&(1\ 5\ 2\ 6\ 3\ 4), (1\ 5\ 3\ 4\ 2\ 6), (1\ 5)(2\ 6)(3\ 4), \\
&(1\ 6\ 3\ 5\ 2\ 4), (1\ 6)(2\ 4)(3\ 5), (1\ 6\ 2\ 4\ 3\ 5)\}.
\end{aligned}$$

*3. (a) Für alle n und k bestimme die durchschnittliche Anzahl von Bahnen der Länge k eines Elements von S_n, wobei jedes Element von S_n als gleich wahrscheinlich betrachtet wird. Kontrolliere, dass das Resultat kompatibel mit der Gesamtzahl n der Ziffern ist.

(b) Bestimme die durchschnittliche Anzahl der Bahnen eines Elements von S_n, und deren asymptotisches Verhalten für $n \to \infty$.

(c) Bestimme die Wahrscheinlichkeit, dass zwei zufällige Elemente von S_n miteinander kommutieren, und deren asymptotisches Verhalten für $n \to \infty$. (Für letzteres Literatursuche.)

Lösung: (a) Für $k > n$ ist die gesuchte Zahl gleich 0. Für $1 \leqslant k \leqslant n$ ist sie $\frac{1}{n!}$ mal die Anzahl der Paare (σ, I) bestehend aus einer Permutation $\sigma \in S_n$ und einer Bahn $I \subset \{1, \ldots, n\}$ der Länge k von σ. Die Anzahl der Möglichkeiten für I ist $\binom{n}{k}$. Für gegebenes I besteht σ aus einem k-Zykel auf I und einer beliebigen Permutation von $\{1, \ldots, n\} \smallsetminus I$. Für letztere gibt es genau $(n-k)!$ Möglichkeiten. Die k-Zykel auf I entsprechen den Auflistungen der Elemente von I bis auf zyklische Vertauschung, deren Anzahl ist daher $\frac{k!}{k}$. Wegen $|S_n| = n!$ ist die gesuchte Zahl für $1 \leqslant k \leqslant n$ also

$$\frac{1}{n!} \cdot \binom{n}{k} \cdot \frac{k!}{k} \cdot (n-k)! \;=\; \frac{1}{k}.$$

(b) Nach (a) ist die gesuchte Zahl gleich

$$\sum_{k=1}^{n} \frac{1}{k} \;\approx\; \log n + \gamma$$

für die Euler-Mascheroni-Konstante γ.

(c) Die gesuchte Zahl ist $\frac{1}{(n!)^2}$ mal die Anzahl der Paare (σ, τ) bestehend aus Permutationen $\sigma, \tau \in S_n$ mit $\sigma\tau = \tau\sigma$. Für jedes $\sigma \in S_n$ ist die Menge der $\tau \in S_n$ mit $\sigma\tau = \tau\sigma$ genau der Zentralisator von σ. Wegen $\mathrm{Cent}_{S_n}({}^\rho\sigma) = {}^\rho\,\mathrm{Cent}_{S_n}(\sigma)$ für alle $\rho \in S_n$ hängt dessen Kardinalität nur von der Konjugationsklasse $O_{S_n}(\sigma)$ ab. Ist $\mathcal{R}_n$ ein Repräsentantensystem der Konjugationsklassen von S_n, so ist die gesuchte Zahl also

$$\begin{aligned}
\tfrac{1}{(n!)^2} \cdot \textstyle\sum_{\sigma \in S_n} |\,\mathrm{Cent}_{S_n}(\sigma)| \;&=\; \tfrac{1}{(n!)^2} \cdot \textstyle\sum_{\sigma \in \mathcal{R}_n} |O_{S_n}(\sigma)| \cdot |\,\mathrm{Cent}_{S_n}(\sigma)| \\
&=\; \tfrac{1}{(n!)^2} \cdot \textstyle\sum_{\sigma \in \mathcal{R}_n} [S_n : \mathrm{Cent}_{S_n}(\sigma)] \cdot |\,\mathrm{Cent}_{S_n}(\sigma)| \\
&=\; \tfrac{1}{(n!)^2} \cdot \textstyle\sum_{\sigma \in \mathcal{R}_n} |S_n| \\
&=\; \tfrac{|\mathcal{R}_n|}{n!} \;=\; \tfrac{p(n)}{n!}.
\end{aligned}$$

Die Asymptotik der Partitionsfunktion $p(n)$ für $n \to \infty$ ist gegeben durch

$$p(n) \;\sim\; \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right);$$

(siehe `https://en.wikipedia.org/wiki/Partition_(number_theory)#Partition_function`). Mit der Stirlingschen Formel folgt

$$\frac{p(n)}{n!} \;\sim\; \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right) \cdot \frac{e^n}{n^n\sqrt{2\pi n}}.$$

4. Sei K ein endlicher Körper der Ordnung q. Betrachte die Operation von $\mathrm{PGL}_2(K)$ auf $\mathbb{P}^1(K)$ wie in Aufgabe 7 der Serie 3. Durch Nummerieren der Elemente von

$\mathbb{P}^1(K)$ entspricht diese einem Homomorphismus $\mathrm{PGL}_2(K) \to S_{q+1}$. Bestimme dessen Bild für alle $q \leqslant 4$.

Lösung: Nach Aufgabe 7 der Serie 3 operiert $\mathrm{PGL}_2(K)$ scharf dreifach transitiv auf $\mathbb{P}^1(K)$. Insbesondere ist die Operation treu, also der Homomorphismus injektiv. Sein Bild ist somit eine Untergruppe von S_{q+1} der Ordnung

$$|\,\mathrm{PGL}_2(K)| \;=\; |\,\mathrm{GL}_2(K)|/|K^\times| \;=\; (q^2-1)(q^2-q)/(q-1) \;=\; q^3-q.$$

In den einzelnen Fällen erhalten wir

q	$\lvert\,\mathrm{PGL}_2(K)\rvert$	$\lvert S_{q+1}\rvert$
2	6	6
3	24	24
4	60	120

Für $q = 2$ und $q = 3$ ist das Bild also gleich S_{q+1}. Für $q = 4$ ist es eine Untergruppe vom Index 2 von S_5. Es genügt also zu zeigen:

Behauptung: Die einzige Untergruppe vom Index 2 von S_n ist die A_n.

Beweis: Jede Untergruppe $H < S_n$ vom Index 2 ist ein Normalteiler. Betrachte einen beliebigen 3-Zykel $\sigma \in S_n$ und bezeichne mit $\bar\sigma$ sein Bild in der Faktorgruppe S_n/H. Aus $\sigma^3 = 1$ folgt dann $\bar\sigma^3 = 1$, und aus $|S_n/H| = 2$ folgt $\bar\sigma^2 = 1$. Zusammen impliziert dies $\bar\sigma = 1$ und folglich $\sigma \in H$. Somit enthält H alle 3-Zykel in S_n. Da diese aber die Untergruppe A_n erzeugen, folgt daraus $A_n < H$. Mit

$$2 \;=\; [S_n : A_n] \;=\; [S_n : H]\cdot[H : A_n] \;=\; 2\cdot[H : A_n]$$

erhalten wir $[H : A_n] = 1$ und damit $H = A_n$. $\square$

5. Sei p eine Primzahl und sei $H < S_p$ eine Untergruppe, die einen p-Zykel und eine Transposition enthält. Zeige, dass $H = S_p$ gilt.

Lösung: Sei $H = \langle\sigma, \tau\rangle$ für einen p-Zykel σ und eine Transposition τ. Für jedes $\alpha \in S_n$ gilt dann ${}^\alpha H = \langle{}^\alpha\sigma, {}^\alpha\tau\rangle$; daher dürfen wir das Paar (σ, τ) durch das Paar $({}^\alpha\sigma, {}^\alpha\tau)$ ersetzen. Da je zwei Transpositionen in S_n konjugiert sind, dürfen wir deshalb insbesondere $\tau = (1\ 2)$ annehmen.

Weiter operiert σ als p-Zykel transitiv auf $\{1, \ldots, p\}$, daher gibt es eine ganze Zahl $1 \leqslant i \leqslant p-1$ mit $\sigma^i(1) = 2$. Da p eine Primzahl ist, erzeugen σ und σ^i dieselbe Untergruppe von S_p. Darum gilt auch $\langle\sigma, \tau\rangle = \langle\sigma^i, \tau\rangle$, und nach Ersetzen von σ durch σ^i dürfen wir auch $\sigma(1) = 2$ annehmen.

Dann ist also $\sigma = (i_1\ i_2\ \ldots\ i_p)$ mit $i_1 = 1$ und $i_2 = 2$. Betrachte nun die Permutation $\alpha \in S_n$ mit $\alpha j = i_j$ für alle $1 \leqslant j \leqslant p$. Dann ist $\sigma = {}^\alpha(1\ 2\ \ldots\ p)$ und $\tau = (i_1\ i_2) = {}^\alpha(1\ 2) = {}^\alpha\tau$. Nach Ersetzen von (σ, τ) durch $({}^{\alpha^{-1}}\sigma, {}^{\alpha^{-1}}\tau)$ haben wir uns damit auf den einzigen Fall $\sigma = (1\ 2\ \ldots\ p)$ und $\tau = (1\ 2)$ reduziert.

Für jede Transposition $(a\ b) \in S_n$ mit $a, b < p$ gilt nun aber ${}^{\sigma}(a\ b) = (\sigma a\ \sigma b) = (a+1\ b+1)$. Durch Induktion über i erhalten wir daraus

$$(i\ i+1) \;=\; {}^{\sigma^{i-1}}\tau \;\in\; \langle \sigma, \tau \rangle \;=\; H.$$

für alle $1 \leqslant i \leqslant p-1$. Somit enthält H alle Nachbartranspositionen in S_n. Da diese die ganze S_n erzeugen, folgt daraus $H = S_n$, wie zu zeigen war.

6. Beim *Schiebespiel* oder *15-Puzzle* sind in der Anfangsposition 15 nummerierte Steine in aufsteigender Reihenfolge in einem 4×4-Rahmen angeordnet, und das Feld unten rechts ist frei:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Ein Zug besteht darin, einen horizontal oder vertikal angrenzenden Stein auf das leere Feld zu schieben. Wir nennen eine Position *zulässig*, wenn sie mit einer endlichen Folge von Zügen aus der Anfangsposition erreicht werden kann und das Feld unten rechts leer ist.

(a) Zeige, dass die Gruppe A_{15} frei und transitiv auf der Menge der zulässigen Positionen operiert.

(b) Folgere daraus, dass es keine Folge von Zügen gibt, welche die Position

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

in die Anfangsposition überführt.

Lösung: (a) Wir machen zunächst die folgenden Beobachtungen:

- Ein Zug entspricht einer Permutation einer 16-elementigen Menge (den 15 nummerierten Feldern und dem freien Feld), also einem Element von S_{16}.
- Eine zulässige Permutation, das heisst, eine Folge von Zügen, die eine zulässige Position in eine zulässige Position überführt, bildet das freie Feld auf sich selbst ab, entspricht also einem Element von S_{15}.
- Das Produkt zweier beliebiger zulässiger Permutationen ist wieder zulässig, nämlich indem man alle Teilzüge der beiden Permutationen hintereinander ausführt. Ebenso ist das Inverse einer zulässigen Permutation wieder zulässig, nämlich indem man die Teilzüge in umgekehrter Reihenfolge ausführt. Ausserdem ist die triviale Permutation zulässig. Daher ist die Menge aller zulässigen Permutationen eine Untergruppe von S_{15}. Nennen wir sie G.

Lemma 1: Die Gruppe G operiert 3-fach transitiv auf der Menge $X := \{1, \ldots, 15\}$.

Beweis: Man weiss aus Kindertagen und kann auch relativ leicht formal zeigen, dass es für beliebige paarweise verschiedene Elemente $x, y, z \in X$ eine Zugfolge gibt, die das leere Feld auf sich selbst und das Tupel (x, y, z) auf $(1, 2, 3)$ abbildet:

$$\begin{array}{|c|c|c|c|}\hline \cdots & \cdots & y & \cdots \\ \hline z & \cdots & \cdots & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ \hline \cdots & x & \cdots & \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{array}{|c|c|c|c|}\hline x & y & z & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ \hline \cdots & \cdots & \cdots & \\ \hline \end{array}$$

Die Bahn von $(1, 2, 3)$ unter G füllt daher die gesamte Menge $\{(x, y, z) \in X^3 \mid x \neq y \neq z \neq x\}$ aus. Somit ist die Operation von G auf dieser Menge transitiv. $\square$

Lemma 2: Die Gruppe G enthält einen 3-Zykel.

Beweis: Schiebt man aus der Anfangsposition nacheinander die Steine 12, 11, 15 und wieder 12 auf das jeweils leere Feld, so erhält man den 3-Zykel $(11\,15\,12)$. $\square$

Lemma 3: Es gilt $A_{15} < G$.

Beweis: Nach Lemma 2 enthält G einen 3-Zykel $(x\ y\ z)$. Nach Lemma 1 existiert für jeden 3-Zykel $(x'\ y'\ z') \in A_{15}$ ein Element $\sigma \in G$ mit $(\sigma x, \sigma y, \sigma z) = (x', y', z')$. Daraus folgt aber $(x'y'z') = {}^{\sigma}(x\ y\ z) \in G$; somit enthält G alle 3-Zykel aus A_{15}. Da diese die Gruppe A_{15} erzeugen, folgt $A_{15} \subset G$. $\square$

Lemma 4: Jede Permutation in G ist gerade.

Beweis: Ein Zug vertauscht jeweils das leere Feld mit einem benachbarten Feld, entspricht also einer Transposition in S_{16}. Denken wir uns die 16 Felder in einem Schachbrett-Muster; das Feld unten rechts sei weiss. Das leere Feld wechselt bei jedem Zug die Farbe, das heisst, nach einer geraden Anzahl Züge ist das leere Feld weiss, nach einer ungeraden Anzahl Züge schwarz. In einer zulässigen Position ist das leere Feld weiss, also können zulässige Positionen nur durch eine gerade Anzahl Züge erreicht werden. Somit ist jede zulässige Permutation das Produkt einer geraden Anzahl von Transpositionen und hat deshalb Signatur 1. $\square$

Aus Lemmas 3 und 4 folgt nun $A_{15} < G < A_{15}$ und somit $G = A_{15}$.

(b) Die in der Aufgabe angegebene Position entspricht einer ungeraden Permutation, also einer unzulässigen Position, und kann somit nicht durch eine Folge von Zügen erreicht werden.

*7. (a) Zeige, dass jede Untergruppe vom Index 5 von A_5 zu A_4 konjugiert ist.

(b) Folgere daraus, dass $\mathrm{Aut}(A_5) \cong S_5$ ist.

Lösung: (a) Sei $H < A_5$ mit $[A_5 : H] = 5$. Nach Lagrange ist dann $|H| = |A_5|/5 = 60/5 = 12$. Die Länge jeder Bahn von H auf $\{1,2,3,4,5\}$ ist also $\leqslant 5$ und ein Teiler von 12, und deshalb $\leqslant 4$.

Hat H eine Bahn der Länge 1, also einen Fixpunkt, so sei dieser nach Konjugation oBdA gleich 5. Dann ist H in der $S_4 < S_5$ enthalten, welche nur die Ziffern $1,2,3,4$ vertauscht. Wegen $S_4 \cap A_5 = A_4$ und $|H| = 12 = |A_4|$ ist dann $H = A_4$, wie gewünscht.

Andernfalls bleibt nur die Möglichkeit, dass H zwei Bahnen der Längen 2 und 3 hat. Identifiziere $S_2 \times S_3$ mit dem Stabilisator in S_5 der entsprechenden Zerlegung von $\{1,2,3,4,5\}$. Weil jede Transposition Signatur -1 hat, ist der zusammengesetzte Homomorphismus $S_2 \times S_3 \hookrightarrow S_5 \xrightarrow{\mathrm{sgn}} \{\pm 1\}$ nicht trivial. Also ist er surjektiv, und sein Kern $(S_2 \times S_3) \cap A_5$ hat Index 2. Somit ist $|(S_2 \times S_3) \cap A_5| = |S_2 \times S_3|/2 = 2 \cdot 6/2 = 6$. Nach Konstruktion ist aber $H < (S_2 \times S_3) \cap A_5$ und $|H| = 12$, was einen Widerspruch bedeutet.

(b) Wegen $A_5 \lhd S_5$ induziert Konjugation mit jedem $\sigma \in S_5$ einen Automorphismus von A_5. Insgesamt liefert dies einen natürlichen Homomorphismus $S_5 \to \mathrm{Aut}(A_5)$, $\sigma \mapsto \mathrm{int}_\sigma |_{A_5}$. Aus Aufgabe 2 (a) wissen wir, dass kein nichttriviales Element von S_5 mit allen Elementen aus A_5 kommutiert. Also ist der genannte Homomorphismus injektiv. Es bleibt zu zeigen, dass er surjektiv ist.

Sei U die Menge aller Untergruppen vom Index 5 von A_5. Die Aussage (a) bedeutet, dass die Elemente von U genau die Stabilisatoren der Ziffern $1,2,3,4,5$ sind. Also ist die Abbildung $\{1,2,3,4,5\} \to U$, $x \mapsto \mathrm{Stab}_{A_5}(x)$ surjektiv. Da jedes $\mathrm{Stab}_{A_5}(x)$ nur den einen Fixpunkt x hat, ist sie auch injektiv, und deshalb bijektiv.

Wegen $A_5 \lhd S_5$ bildet Konjugation mit S_5 jedes Element von U auf ein ebensolches ab, liefert also eine natürliche Operation von S_5 auf U. Aufgrund der soeben gezeigten Bijektivität entspricht diese Operation einem Isomorphismus $i\colon S_5 \xrightarrow{\sim} S(U)$ mit $i(\sigma)(H) = {}^\sigma H$.

Sei jetzt φ ein beliebiger Automorphismus von A_5. Dann induziert auch dieser eine bijektive Abbildung $U \to U$, $H \mapsto \varphi(H)$. Unter i entspricht diese einem Element $\sigma \in S_5$ mit der Eigenschaft $\varphi(H) = i(\sigma)(H) = {}^\sigma H$ für alle $H \in U$. Für alle $\tau \in A_5$ und $H \in U$ gilt dann

$$ {}^{\sigma\tau}H \;=\; {}^\sigma({}^\tau H) \;=\; \varphi({}^\tau H) \;\overset{!}{=}\; {}^{\varphi(\tau)}\varphi(H) \;=\; {}^{\varphi(\tau)}({}^\sigma H) \;=\; {}^{\varphi(\tau)\sigma}H. $$

Da S_5 treu auf U operiert, folgt daraus $\sigma\tau = \varphi(\tau)\sigma$ für alle $\tau \in A_5$. Dies ist aber äquivalent zu $\varphi(\tau) = \sigma\tau\sigma^{-1} = {}^\sigma\tau$. Also ist $\varphi = \mathrm{int}_\sigma |_{A_5}$, wie gewünscht.