Musterlösung 11

Symmetrische Gruppe, Einfache Gruppen

1. Eine Gruppe heisst *metabelsch*, wenn es eine normale Untergruppe N gibt, derart dass N und G/N abelsch sind. Zeige, dass jede Untergruppe einer metabelschen Gruppe auch metabelsch ist.

   Lösung: Let G be a metabelian group with $N \triangleleft G$ as in the statement of the exercise. Let H be any subgroup of G. Then $H \cap N$ is normal in H and, being a subgroup of the abelian group N, itself abelian. By the first isomorphism theorem $H/H \cap N \cong HN/N < G/N$. Since G/N is assumed to be abelian, it follows that $H/H \cap N$ is as well. Thus H is metabelian.

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

   (b) Berechnen Sie den Zentralisator von (234) in S_5.

   (c) Berechnen Sie den Zentralisator von $(123)(456)$ in S_7.

   Lösung: (a) Für $n = 1$ und $n = 2$ ist S_n abelsch, es gilt also $Z(S_1) = S_1$ und $Z(S_2) = S_2$.

   Sei nun $n \geqslant 3$ und $\sigma \neq \mathrm{id}$ ein nicht-triviales Element von S_n. Dafür gibt es ein i mit $\sigma(i) \neq i$ und ein $k \notin \{i, \sigma(i)\}$. Für $\tau := (\sigma(i)\ k)$ ist dann

$$\begin{aligned}(\sigma\tau)(i) &= \sigma(i)\\ (\tau\sigma)(i) &= k,\end{aligned}$$

   insbesondere $\sigma\tau \neq \tau\sigma$, also ist $\sigma \notin Z(S_n)$. Da σ ein beliebiges nicht-triviales Element von S_n war, folgt $Z(S_n) = \{\mathrm{id}\}$.

   (b) Ein Element $\sigma \in S_5$ liegt genau dann im Zentralisator von (234), wenn

$$(234) = \sigma(234)\sigma^{-1} = (\sigma(2)\ \sigma(3)\ \sigma(4))$$

   ist. Allgemein gilt für Dreizykel

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

   deshalb gibt es für die Einschränkung von σ auf $\{2, 3, 4\}$ die drei Möglichkeiten $\mathrm{id}, (234), (243)$. Da dabei $\{2, 3, 4\}$ auf sich abgebildet wird, muss auch $\{1, 5\}$ auf sich abgebildet werden. Somit ist die Einschränkung von σ auf $\{1, 5\}$ entweder die Identität oder die Transposition (15). Insgesamt gibt es daher 6 Elemente im Zentralisator von (234):

$$Z_{S_5}((234)) = \{\mathrm{id},\ (234),\ (243),\ (15),\ (15)(234),\ (15)(243)\}$$

(c) Ein Element $\sigma \in S_7$ liegt ganau dann im Zentralisator von (123)(456), wenn

$$(123)(456) = \sigma(123)(456)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3))(\sigma(4)\ \sigma(5)\ \sigma(6))$$

ist. Diese Gleichheit gilt in den beiden Fällen

$$\begin{array}{ll} \text{(i)} & (123) = (\sigma(1)\ \sigma(2)\ \sigma(3)),\quad (456) = (\sigma(4)\ \sigma(5)\ \sigma(6)) \\ \text{(ii)} & (123) = (\sigma(4)\ \sigma(5)\ \sigma(6)),\quad (456) = (\sigma(1)\ \sigma(2)\ \sigma(3)). \end{array}$$

Wegen (**??**) gibt es je solchen Fall $3 \cdot 3 = 9$ Möglichkeiten für die Einschränkung von σ auf $\{1,2,3,4,5,6\}$. Dabei wird $\{1,2,3,4,5,6\}$ auf sich abgebildet, darum muss $\sigma(7) = 7$ in beiden Fällen gelten. Somit hat der Zentralisator von (123)(456) genau $2 \cdot 9 = 18$ Elemente (je Zeile alle Elemente mit einer festen Einschränkung von σ auf $\{1,2,3\}$ aufgelistet):

$$\begin{aligned} Z_{S_7}((123)(456)) \; = \{ & \mathrm{id}, (456), (465), \\ & (123), (123)(456), (123)(465), \\ & (132), (132)(456), (132)(465), \\ & (14)(25)(36), (142536), (143625), \\ & (152634), (153426), (15)(26)(34), \\ & (163524), (16)(24)(35), (162435)\}. \end{aligned}$$

3. Finde für alle $n \geqslant 1$ einen injektiven Homomorphismus $S_n \hookrightarrow A_{n+2}$.

Lösung: Zu jedem $\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix} \in S_n$ definieren wir

$$S_{n+2} \ni i(\sigma) := \begin{pmatrix} 1 & \dots & n & n+1 & n+2 \\ \sigma(1) & \dots & \sigma(n) & n+1 & n+2 \end{pmatrix}$$

und

$$S_{n+2} \ni t(\sigma) := \begin{cases} \begin{pmatrix} 1 & \dots & n & n+1 & n+2 \\ 1 & \dots & n & n+1 & n+2 \end{pmatrix}, & \operatorname{sign}\sigma = 1 \\ \begin{pmatrix} 1 & \dots & n & n+1 & n+2 \\ 1 & \dots & n & n+2 & n+1 \end{pmatrix}, & \operatorname{sign}\sigma = -1, \end{cases}$$

sowie $\varphi(\sigma) := i(\sigma)t(\sigma)$. Die Abbildungen $i, t\colon S_n \to S_{n+2}$ sind Homomorphismen, und ihre Bilder kommutieren elementweise. Also gilt für alle $\sigma, \sigma' \in S_n$

$$\varphi(\sigma\sigma') = i(\sigma\sigma')t(\sigma\sigma') = i(\sigma)i(\sigma')t(\sigma)t(\sigma') = i(\sigma)t(\sigma)i(\sigma')t(\sigma') = \varphi(\sigma)\varphi(\sigma'),$$

das heisst, $\varphi\colon S_n \to S_{n+2}$ ist ein Homomorphismus. Dieser ist injektiv, da $\varphi(\sigma)|_{\{1,\dots,n\}} = \sigma$ für alle $\sigma \in S_n$, und ausserdem gilt $\mathrm{sign}_{S_n}\sigma = \mathrm{sign}_{S_{n+2}} i(\sigma) = \mathrm{sign}_{S_{n+2}} t(\sigma)$ für alle $\sigma \in S_n$, also

$$\mathrm{sign}_{S_{n+2}}\varphi(\sigma) = \mathrm{sign}_{S_{n+2}} i(\sigma) \mathrm{sign}_{S_{n+2}} t(\sigma) = (\mathrm{sign}_{S_n}\sigma)^2 = 1.$$

Somit ist $\mathrm{Im}\varphi \subset A_{n+2}$.

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

   Lösung: Die zu beweisende Aussage ist invariant unter Konjugation von σ und τ, d.h. für alle $\alpha \in S_p$ erzeugen zwei Permutationen $\sigma, \tau \in S_p$ genau dann S_p, wenn $\alpha\sigma\alpha^{-1}, \alpha\tau\alpha^{-1}$ ganz S_p erzeugen. Da je zwei Transpositionen konjugiert sind, können wir o.B.d.A. $\tau = (12)$ annehmen. Weiter operiert σ als p-Zykel transitiv auf $\{1, \dots, p\}$, es gibt daher ein i mit $1 \leqslant i \leqslant p - 1$ und $\sigma^i(1) = 2$. Da p eine Primzahl ist, erzeugen σ und σ^i dieselbe Untergruppe von S_p, insbesondere ist darum $\langle\sigma, \tau\rangle = \langle\sigma^i, \tau\rangle$. Wir können deshalb o.B.d.A. $\sigma(1) = 2$ annehmen. Nach Konjugation mit einer geeigneten Permutation der Elemente $\{3, \dots, p\}$ (diese lässt $\tau = (12)$ invariant) können wir schliesslich sogar $\sigma = (12 \dots p)$ annehmen.

   Da sämtliche Transpositionen ganz S_p erzeugen, genügt es zu zeigen, dass jede Transposition von $\sigma = (12 \dots p)$ und $\tau = (12)$ erzeugt wird. In der Tat werden Transpositionen $(i\ i+1)$ benachbarter Elemente wegen

   $$(i\ i+1) = \sigma^{i-1}\tau\sigma^{-(i-1)}$$

   von σ und τ erzeugt. Eine beliebige Transposition (kl) mit $1 \leqslant k < l \leqslant p$ kann via

   $$(kl) = (k\ k+1) \cdots (l-2\ l-1)(l-1\ l)(l-2\ l-1) \cdots (k\ k+1)$$

   als Produkt von Transpositionen benachbarter Elemente geschrieben werden und wird darum auch von σ und τ erzeugt.

5. Sei K ein endlicher Körper der Ordnung q. Betrachte die Operation von $\mathrm{PGL}_2(K)$ auf $\mathbb{P}^1(K)$ wie in Serie 10 Aufgabe 7. Durch Numerieren 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 Serie 10 Aufgabe 7 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. Da jede Untergruppe vom Index 2 ein Normalteiler ist, und A_5 der einzige nichttriviale echte Normalteiler von S_5 ist, ist das Bild in diesem Fall gleich A_5.

6. (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 $\frac{k!}{k}$. Insgesamt 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

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

(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 $\operatorname{Cent}_{S_n}({}^\rho\sigma) = {}^\rho \operatorname{Cent}_{S_n}(\sigma)$ 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

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

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

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

7. Beim *Schiebespiel* oder *15-Puzzle* sind in der Anfangsposition 15 nummerierte Steine in aufsteigender Reihenfolge in einem 4×4-Rahmen angeordnet; 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 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 leere Feld das Feld unten rechts ist.

Zeige, dass A_{15} die Gruppe der möglichen Permutationen der zulässigen Positionen ist. (In anderen Worten: Die Gruppe A_{15} operiert frei und transitiv auf der Menge der zulässigen Positionen.)

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: Wir machen zunächst folgende Beobachtungen: Ein Zug entspricht einer Permutation einer 16-elementigen Menge (den 15 nummerierten und dem freien Feld), also einem Element von S_{16}. Eine zulässige Permutation (also 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}.

Wir zeigen, dass die Gruppe G der zulässigen Permutationen 3-fach transitiv auf $\{1,\ldots,15\}$ operiert und einen 3-Zykel enthält; daraus folgt dann $A_{15} < G$. Anschliessend zeigen wir, dass jedes Element aus G gerade Signatur hat, und somit folgt $G < A_{15}$, also $G = A_{15}$.

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

Beweis: Man überzeugt sich leicht, dass es zu beliebigen paarweise verschiedenen Elementen $x, y, z \in \{1,\ldots,15\}$ eine Zugfolge gibt, die das leere Feld auf sich selbst, x auf 1, y auf 2 und z auf 3 abbildet.

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

Zu gegebenen Elementen x, y, z wählen wir eine solche Zugfolge, und nennen die zugehörige zulässige Permutation $\sigma_{x,y,z}$. Zu beliebigen paarweise verschiedenen $x, y, z \in \{1,\ldots,15\}$ und beliebigen paarweise verschiedenen $x', y', z' \in \{1,\ldots,15\}$ ist nun $\sigma := \sigma^{-1}_{x',y',z'} \circ \sigma_{x,y,z} \in G$ eine zulässige Permutation mit $(\sigma(x), \sigma(y), \sigma(z)) = (x', y', z')$. $\square$

Lemma: Die Gruppe G enthält einen 3-Zykel.

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

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

Beweis: Betrachte einen 3-Zykel $(x\ y\ z) \in G$ und einen beliebigen 3-Zykel $(x'\ y'\ z') \in A_{15}$. Wegen der dreifachen Transitivität existiert ein $\sigma \in G$ mit $(\sigma x, \sigma y, \sigma z) = (x', y', z')$. Daraus folgt aber $(x', y', z') = {}^{\sigma}(x\ y\ z) \in G$. Also enthält G alle 3-Zykel aus A_{15}. Da diese die Gruppe A_{15} erzeugen, folgt $A_{15} \subset G$. $\square$

Lemma: Jedes Element aus 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. $\square$

Also gilt $G < A_{16} \cap S_{15} = A_{15}$, woraus wie erwünscht $G = A_{15}$ folgt.

Die in der Aufgabe gegebene Position schliesslich entspricht einer Permutation in $S_{15} \setminus A_{15}$, also einer unzulässigen Position, und kann somit nicht durch eine endliche Folge von Zügen erreicht werden.

*8. Sei G eine endliche Gruppe und H eine Untergruppe, so dass der Index $p := [G : H]$ gleich dem kleinsten Primteiler der Ordnung von G ist. Zeige, dass H ein Normalteiler ist.

Hinweis: Untersuche Kern und Bild des Homomorphismus $G \to S_p$, welcher der Operation von G auf der Menge der Linksnebenklassen G/H entspricht.

Lösung: Die Gruppe G operiert auf der Menge der Linksnebenklassen G/H vermöge

$$g(xH) := (gx)H.$$

Diese Operation induziert einen Homomorphimus $\varphi : G \to S_p$. Sei $K := \ker \varphi$.

Der Stabilisator der Nebenklasse H bezüglich dieser Operation von G auf G/H ist gleich H, denn es gilt $gH = H \Leftrightarrow g \in H$. Daher ist K in H enthalten und es gilt

$$[G : K] = [G : H] \cdot [H : K] \geqslant p. \tag{2}$$

Nach dem Homomorphiesatz ist K ein Normalteiler von G und φ induziert einen injektiven Homomorphimus $G/K \hookrightarrow S_p$. Darum kann G/K mit einer Untergruppe von S_p identifiziert werden und nach dem Satz von Lagrange ist $[G : K] = |G/K|$ ein Teiler von $p! = |S_p|$. Da $p! = p \cdot (p-1)!$ gilt, wobei $(p-1)!$ nur Primfaktoren $< p$ hat, kann darum p höchstens mit Exponent 1 in der Primfaktorzerlegung von $[G : K]$ auftreten und Primfaktoren $> p$ können darin gar nicht vorkommen. Der Index $[G : K]$ ist aber auch ein Teiler von $|G|$ und hat daher nur Primteiler $\geqslant p$. Deshalb gibt es für $[G : K]$ nur die Möglichkeiten p und 1. Letztere ist aber wegen (**??**) ausgeschlossen. Es ist also $[G : K] = p = [G : H]$ und $H = K$ ist normal.

*9. (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 $A_5 \triangleleft S_5$ induziert Konjugation mit jedem $\sigma \in S_5$ einen Automorphismus von A_5. Insgesamt liefert dies einen natürlichen Homomorphismus $S_5 \to \mathrm{Aut}(A_5)$, $\sigma \mapsto \mathrm{int}_\sigma |_{A_5}$. Wie in Aufgabe 2 (a) zeigt man, 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 $A_5 \triangleleft S_5$ 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.