Musterlösung Serie 8

PERMUTATIONSGRUPPEN, SEMI-DIREKTE PRODUKTE

---

45. In dieser Aufgabe wird gezeigt, dass für alle n mit $n \geqslant 3$ und $n \neq 6$ gilt: $\mathrm{Aut}(S_n) \cong S_n$.
Im Folgenden sei n eine natürliche Zahl mit $n \geqslant 3$ und $n \neq 6$.

(a) Sei $\alpha \in \mathrm{Aut}(S_n)$.
Zeige: Für jede Transposition $(i\ j) \in S_n$ ist $\alpha(i\ j)$ eine Transposition.

Hinweis: Da $\mathrm{ord}\big(\alpha(i\ j)\big) = 2$, ist $\alpha(i\ j)$ ein Produkt von r paarweise disjunkten Transpositionen, wobei $2 \leqslant 2r \leqslant n$, und ist $(l\ k) \in S_n$ eine Transposition, so ist auch $\alpha(l\ k)$ ein Produkt von r paarweise disjunkten Transpositionen. Es genügt also $r = 1$ zu zeigen.

(b) Zeige, dass für jeden Automorphismus $\alpha \in \mathrm{Aut}(S_n)$ ein $\vartheta \in S_n$ existiert, sodass für alle $\sigma \in S_n$ gilt:

$$\alpha(\sigma) = \vartheta\sigma\vartheta^{-1}\,.$$

Hinweis: Da $S_n = \langle (1\ 2), \ldots, (1\ n) \rangle$ genügt es folgendes zu zeigen: Es existiert ein $\vartheta \in S_n$, sodass für alle Transpositionen $(1\ k) \in S_n$ gilt, $\alpha(1\ k) = (\vartheta(1)\ \vartheta(k))$.

(c) Zeige $\mathrm{Aut}(S_n) \cong S_n$.

Lösung:

(a) Die Permutation $\alpha(i\ j)$ hat Ordnung zwei, also ist sie das Produkt von r disjunkten Transpositionen. Da α ein Automorphismus ist, induziert diese Abbilung eine Bijektion

$$[(i\ j)] \cong [\alpha(i\ j)]$$

zwischen den Konjugationsklassen einer Transposition und einem Produkt von r disjunkten Transpositionen.
Die Konjugationsklassen einer Transposition enthält alle Transposition, also gilt

$$|[(i\ j)]| = \binom{n}{2} = \frac{n(n-1)}{2}.$$

Die Konjugationsklasse eines Produkts von r disjunkten Transpositionen enthält alle Produkte von r disjunkten Transpositionen, also gilt

$$|[\alpha(i\ j)]| = \frac{1}{r!}\binom{n}{2}\binom{n-2}{2} \cdot \ldots \cdot \binom{n-2(r-1)}{2}.$$

Nun besagt die obige Bijektion

$$\frac{n(n-1)}{2} = \frac{n(n-1) \cdot \ldots \cdot (n-2r+2)(n-2r+1)}{2^r r!}.$$

Für $r = 1$ stimmt diese Gleichung immer. Für $r = 2$ besagt diese Gleichung

$$4 = (n-2)(n-3).$$

und für $r = 3$

$$24 = (n-2)(n-3)(n-4)(n-5).$$

Für $n \leqslant 6$ kann man von Hand prüfen, dass diese Gleichungen nur gelten können falls $n = 6$. Für $n = 7$ ist die rechte Seite strikt grösser als die linke und ein Monozitätsargument beweist, dass keine der Gleichungen für $n \geqslant 7$ gelten kann. Für $r \geqslant 4$ erhalten wir aus $n \geqslant 2r$ die Ungleichungen

$$\begin{aligned}(n-2)(n-3)\cdot\ldots\cdot(n-2r+1) &\geqslant (2r-2)\cdot\ldots\cdot 1\\ &= (2r-2)\cdot\ldots\cdot(r+1)r!\\ &\geqslant 4^{r-2}r! = 2^{2(r-2)}r! > 2^{r-1}r!.\end{aligned}$$

Weil $n \neq 6$ folgt also $r = 1$. Dies sagt genau, dass $\alpha(i\ j)$ eine Transposition ist.

(b) Das Produkt von zwei Tranpsitionen

$$(a\ b)(c\ d)$$

hat Ordnung drei dann und nur dann, falls $|\{a, b\} \cap \{c, d\}| = 1$. Wir betrachten zwei verschiedene Zahlen $1 < i, j \leqslant n$ Aus Aufgabe (a) wissen wir, dass $1 \leqslant a, b, c, d \leqslant n$ existieren, so dass

$$\alpha(1\ i) = (a\ b),\ \alpha(1\ j) = (c\ d)$$

gilt. Die Permutation $(1\ i)(1\ j)$ hat Ordnung 3 also hat $\alpha((1\ i)(1\ j)) = (a\ b)(c\ d)$ Ordnung 3. O.B.d.A. folgt nun $a = c$.

Also existiert $1 \leqslant a \leqslant n$, so dass für alle $1 \leqslant i \leqslant n$ ein eindeutiges $1 \leqslant \vartheta(i) \leqslant n$ mit

$$\alpha(1\ i) = (a\ \vartheta(i))$$

existiert. Diese Abildung definiert eine Permutation $\vartheta \in S_n$. Nun besagt die Defition von ϑ

$$\alpha(1\ i) = \vartheta(1\ i)\vartheta^{-1}$$

für alle $1 \leqslant i \leqslant n$. Da diese Transpositionen die Gruppe S_n erzeugen, erhalten wir

$$\alpha(\sigma) = \vartheta\sigma\vartheta^{-1}$$

für alle $\sigma \in S_n$.

(c) Betrachte die Abbildung

$$S_n \to \mathrm{Aut}(S_n),\ \vartheta \mapsto (\sigma \mapsto \vartheta\sigma\vartheta^{-1}).$$

Diese Abbildung ist ein Gruppenhomomorphismus mit Kern $Z(S_n)$. Sei $\vartheta \in Z(S_n)$. Die Konjugation wird durch die Gleichung

$$\vartheta(i\ j)\vartheta^{-1} = (\vartheta(i)\ \vartheta(j))$$

beschrieben. Sei $3 \leqslant i \leqslant n$, dann haben wir die Gleichungen $(\vartheta(1)\ \vartheta(2)) = (1\ 2)$ und $(\vartheta(1)\ \vartheta(i)) = (1\ i)$. Diese können nur gelten falls $\vartheta(1) = 1$, also folgt auch $\vartheta(2) = 2$ und $\vartheta(i) = i$. Somit folgt $\vartheta = e$. Also ist der Kern trivial und somit ist der Gruppenhomomorphismus injektiv. Nach Aufgabe (b) ist dieser Gruppenhomomorphismus surjektiv. Also ist er ein Isomorphismus und wir können

$$\mathrm{Aut}(S_n) \cong S_n$$

schreiben.

46. Sei $p > 2$ eine Primzahl und sei G eine Gruppe der Ordnung $|G| = 2p$.

Zeige, dass G entweder zyklisch oder isomorph zur Diedergruppe D_p ist.

Lösung: Mit dem ersten Sylowsatz oder Cauchy's Theorem folgt, dass die Gruppe G Elemente x und y mit $\mathrm{ord}(x) = 2$ und $\mathrm{ord}(y) = p$ enthält. Die Untergruppe $N = \langle y \rangle$ erzeugt durch y ist eine Sylow p-Untergruppe von G. Mit dem zweiten Sylow Satz folgt, dass die Anzahl der Sylow p-Untergruppen $2p$ teilt und kongruent 1 modulo p ist. Es kann also nur eine solche Sylow p-Untergruppe geben, da $2, p$ und $2p$ nicht kongruent 1 modulo p sind. Sei nun g ein beliebiges Element von G, dann ist gNg^{-1} eine Sylow p-Untergruppe von G und es folgt $gNg^{-1} = N$. Somit ist N ein Normalteiler von G mit Ordnung p.

Wir betrachten nun das Element $xyx^{-1} \in G$. Es muss im Normalteiler $N = \langle y \rangle$ liegen und somit gibt es ein $k \in N$ mit $xyx^{-1} = y^k$. Weiter ist k nicht durch p teilbar, da xyx^{-1} nicht das neutrale Element ist. Dann gilt

$$y^{k^2} = (y^k)^k = (xyx^{-1})^k = xy^kx^{-1} = x(xyx^{-1})x^{-1} = x^2yx^{-2}.$$

Aber es ist $x^2 = x^{-2} = e$, da x Ordnung 2 hat. Es folgt $y^{k^2} = y$ und somit ist $y^{k^2-1} = e$. Also muss p die Zahl $k^2 - 1$ teilen, da y ein Element mit Ordnung p ist. Weiter ist $k^2 - 1 = (k-1)(k+1)$. Daher teilt p entweder $k-1$, dann ist $xyx^{-1} = y$, oder p teilt $k+1$, dann ist $xyx^{-1} = y^{-1}$.

Ist $xyx^{-1} = y$ erhalten wir $xy = yx$ und wir sehen sofort, dass G erzeugt von xy zyklisch ist der Ordnung $2p$. Ist jedoch $xyx^{-1} = y^{-1}$, dann ist G isomorph zur Diedergruppe D_{2p} der Ordnung $2p$. In diesem Fall erzeugen x und y die Gruppe G (da x und y eine Untergruppe von G erzeugen deren Ordnung $2p$ teilt, aber grösser als p ist und somit $2p$ sein muss). Mit diesem Isomorphismus entspricht x der Spiegelung an einer Symmetrieachse des regelmässigen p-Ecks und y der Rotation um das Zentrum um $\frac{2\pi}{p}$.

47.

48. Seien zwei Gruppen N, H und zwei Homomorphismen $\varphi, \varphi' \colon H \to \mathrm{Aut}(N)$ gegeben. Es seien $N \rtimes_\varphi H$ und $N \rtimes_{\varphi'} H$ die semidirekten Produkte.

Zeige, dass diese beiden Gruppen in den folgenden Situationen isomorph sind:

(a) Sei $\alpha \in \mathrm{Aut}(N)$ ein Automorphismus so, dass $\varphi' = \alpha \circ \varphi \circ \alpha^{-1}$. Dann gilt

$$N \rtimes_\varphi H \cong N \rtimes_{\varphi'} H.$$

(b) Sei $\beta \in \mathrm{Aut}(H)$ ein Automorphismus so, dass $\varphi = \varphi' \circ \beta$. Dann gilt

$$N \rtimes_{\varphi} H \cong N \rtimes_{\varphi'} H.$$

Lösung: (a) Wir betrachten die folgende Abbildung

$$\begin{aligned} \gamma\colon N \rtimes_{\varphi} H &\to N \rtimes_{\varphi'} H \\ (n, h) &\mapsto (\alpha(n), h). \end{aligned}$$

Dann folgt für $(n_1, h_1), (n_2, h_2) \in N \rtimes_{\varphi} H$, da α ein Automorphismus ist,

$$\begin{aligned} \gamma(n_1, h_1) \circ_{\varphi'} \gamma(n_2, h_2) &= (\alpha(n_1), h_1) \circ_{\varphi'} (\alpha(n_2), h_2) = (\alpha(n_1) \cdot \varphi'_{h_1}(\alpha(n_2)), h_1 h_2) \\ &= (\alpha(n_1) \cdot (\alpha \circ \varphi_{h_1} \circ \alpha^{-1})(\alpha(n_2)), h_1 h_2) \\ &= (\alpha(n_1) \cdot \alpha(\varphi_{h_1}(n_2)), h_1 h_2) = (\alpha(n_1 \cdot \varphi_{h_1}(n_2)), h_1 h_2) \\ &= \gamma(n_1 \cdot \varphi_{h_1}(n_2), h_1 h_2) = \gamma((n_1, h_1) \circ_{\varphi} (n_2, h_2)) \end{aligned}$$

und somit, dass γ ein Homomorphismus ist. Analog zeigt man, dass

$$\begin{aligned} \gamma'\colon N \rtimes_{\varphi'} H &\to N \rtimes_{\varphi} H \\ (n, h) &\mapsto (\alpha^{-1}(n), h) \end{aligned}$$

ebenfalls ein Homomorphismus ist und da α ein Automorphismus ist, ist dieser invers zu γ. Somit folgt, dass γ ein Isomorphismus ist und es gilt $N \rtimes_{\varphi} H \cong N \rtimes_{\varphi'} H$.

(b) Wir betrachten die folgende Abbildung

$$\begin{aligned} \delta\colon N \rtimes_{\varphi} H &\to N \rtimes_{\varphi'} H \\ (n, h) &\mapsto (n, \beta(h)) \end{aligned}$$

Da β ein Automorphismus ist, gilt $\varphi' = \varphi \circ \beta^{-1}$. Dann folgt für $(n_1, h_1), (n_2, h_2) \in N \rtimes_{\varphi} H$

$$\begin{aligned} \delta(n_1, h_1) \circ_{\varphi'} \delta(n_2, h_2) &= (n_1, \beta(h_1)) \circ_{\varphi'} (n_2, \beta(h_2)) = (n_1 \cdot \varphi'_{\beta(h_1)}(n_2), \beta(h_1) \cdot \beta(h_2)) \\ &= (n_1 \cdot (\varphi \circ \beta^{-1})(\beta(h_1))(n_2), \beta(h_1 h_2)) = (n_1 \cdot \varphi_{h_1}(n_2), \beta(h_1 h_2)) \\ &= \delta(n_1 \cdot \varphi_{h_1}(n_2), h_1 h_2) = \delta((n_1, h_1) \circ_{\varphi} (n_2, h_2)) \end{aligned}$$

und somit, dass δ ein Homomorphismus ist. Analog zeigt man, dass

$$\begin{aligned} \delta'\colon N \rtimes_{\varphi'} H &\to N \rtimes_{\varphi} H \\ (n, h) &\mapsto (n, \beta^{-1}(h)) \end{aligned}$$

ebenfalls ein Homomorphismus ist und dass dieser invers zu δ ist. Somit folgt, dass δ ein Isomorphismus ist und es gilt $N \rtimes_{\varphi} H \cong N \rtimes_{\varphi'} H$.

49. Bestimme bis auf Isomorphie alle Gruppen der Ordnung 28.

Hinweis: Zeige mit dem Sylow-Theorem, dass eine Gruppe der Ordnung 28 immer einen nicht-trivialen Normalteiler hat.

Lösung: Sei G eine Gruppe der Ordnung 28. Zuerst berechnen wir $|G| = 28 = 4 \cdot 7$. Die Anzahl aller Sylow 7-Untergruppen muss kongruent 1 modulo 7 sein und 4 teilen, ist also gleich 1. Es gibt also nur eine, sie ist normal und isomorph zu C_7. Sei $H \leqslant G$ eine Untergruppe der Ordnung 4. Da $C_7 \trianglelefteq G$ ist gilt $C_7H = HC_7$ und somit ist C_7H nach Aufgabe 16(b) eine Untergruppe von G. Wegen $C_7 \leqslant C_7H$ und $H \leqslant C_7H$, wird $|C_7H|$ nach dem Satz von Lagrange von 4 und 7 geteilt. Deshalb gilt $|C_7H| = 28$ und somit ist $C_7H = G$. Weiters muss $C_7 \cap H = \{e\}$ sein, denn die Ordnung jedes Elements im Schnitt muss die beiden teilerfremden Zahlen 4 und 7 teilen, also gleich 1 sein. Somit sind alle Eigenschaften des semidirekten Produktes erfüllt. Es gibt also ein $\varphi\colon H \to \mathrm{Aut}(C_7)$ mit $G \cong H \ltimes_\varphi C_7$. In Aufgabe 35 haben wir $\mathrm{Aut}(C_7)$ bestimmt. Es ist

$$\mathrm{Aut}(C_7) := \{\psi_k \mid 1 \leqslant k \leqslant 6\},$$

wobei ψ_k der Automorphismus ist, der $a \in C_7$ auf a^k sendet. Wir machen nun eine Fallunterscheidung, nämlich $H = C_4 = \langle g \rangle$ und $H = C_2 \times C_2 = \langle g \rangle \times \langle g \rangle$.

Sei zuerst $H = C_4$. Dann ist $\varphi\colon H \to \mathrm{Aut}(C_7) \cong C_6$ eindeutig durch das Bild eines Erzeugers von H gegeben. Wegen $\mathrm{ord}(\varphi(g)) \mid \mathrm{ord}(g)$ gibt es nur die beiden Möglichkeiten $\varphi(g) = \psi_1$ und $\varphi(g) = \psi_6$. Im ersten Fall ist $G = C_4 \times C_7$ und im zweiten Fall ist $G = C_4 \ltimes_\varphi C_7$ ein nichttriviales semidirektes Produkt.

Sei nun $H = C_2 \times C_2$. Weil die Elemente (g, e) und (e, g) Ordnung 2 haben, kommt für $\varphi(g, e)$ und $\varphi(e, g)$ jeweils auch nur ψ_1 oder ψ_6 infrage. Es gibt demnach 4 mögliche Homomorphismen $\varphi_0, \varphi_1, \varphi_2, \varphi_3\colon C_2 \times C_2 \to \mathrm{Aut}(C_7)$, wobei

(a) $\varphi_0(g, e) = \psi_1,\ \varphi_0(e, g) = \psi_1$

(b) $\varphi_1(g, e) = \psi_1,\ \varphi_1(e, g) = \psi_6$

(c) $\varphi_2(g, e) = \psi_6,\ \varphi_2(e, g) = \psi_1$

(d) $\varphi_3(g, e) = \psi_6,\ \varphi_3(e, g) = \psi_6$.

Die letzten drei Möglichkeiten geben nach Aufgabe 47 jedoch bis auf Isomorphie dasselbe Gruppe G, denn die drei nichttrivialen Elemente von $C_2 \times C_2$ lassen sich mit Isomorphismen von $C_2 \times C_2$ beliebig permutieren. Somit sind die zwei Möglichkeiten $G = C_2 \times C_2 \times C_7$ und $G = (C_2 \times C_2) \ltimes_{\varphi_1} C_7$. Da letzteres die einzige nichtabelsche Gruppe ist, die kein Element der Ordnung 4 enthält, gilt $(C_2 \times C_2) \ltimes_{\varphi_1} C_7 \cong D_{14}$.