Algebra I

Musterlösung 6

Permutationsgruppen, Semidirektes Produkt

---

37. (a) Zeige: Sind $\rho, \sigma \in S_n$ disjunkte Permutationen, dann gilt $(\rho\sigma)^k = \sigma^k \rho^k$ für alle $k \in \mathbb{N}$.

(b) Zeige: Ist ρ ein k-Zykel in S_n, dann ist $\operatorname{ord}(\rho) = k$.

(c) Zeige: Ist $\pi \in S_n$ ein Produkt paarweise disjunkter Zyklen der Länge $k_1, \ldots, k_r$, so ist $\operatorname{ord}(\pi) = \operatorname{kgV}(k_1, \ldots, k_r)$.

Lösung: Siehe Skript.

38. Zeige, dass für jedes $n \geqslant 1$ die Gruppe der orthogonalen Matrizen $\mathrm{O}(n, \mathbb{R})$ isomorph zum semidirekten Produkt $\mathrm{SO}(n, \mathbb{R}) \rtimes C_2$ ist.

Lösung: Since $\mathrm{SO}_n(\mathbb{R})$ is the kernel of the surjective homomorphism $\det : \mathrm{O}_n(\mathbb{R}) \to \{\pm 1\}$, it follows that $\mathrm{SO}_n(\mathbb{R})$ is normal of index 2 in $\mathrm{O}_n(\mathbb{R})$. Let $R \in \mathrm{O}_n(\mathbb{R})$ be of order 2 with determinant -1, for example, a diagonal matrix with entries in $\{1, -1\}$, such that -1 appears with odd multiplicity. Then $\langle R \rangle = \{I_n, R\} < \mathrm{O}_n(\mathbb{R})$. Since $[\mathrm{O}_n(\mathbb{R}) : \mathrm{SO}_n(\mathbb{R})] = 2$ and $R \notin \mathrm{SO}_n(\mathbb{R})$, it follows that $\mathrm{SO}_n(\mathbb{R}) \cdot \langle R \rangle = \mathrm{O}_n(\mathbb{R})$. Now $R \notin \mathrm{SO}_n(\mathbb{R})$ also implies that $\mathrm{SO}_n(\mathbb{R}) \cap \langle R \rangle = I_n$. It follows that $\mathrm{O}_n(\mathbb{R})$ is the inner semidirect product of $\mathrm{SO}_n(\mathbb{R})$ by $\langle R \rangle$. Identifying $\langle R \rangle$ with C_2 yields the desired result.

Remark: Observe that when n is odd, we may choose $R = -I_n$, in which case $\langle R \rangle$ is normal in $\mathrm{O}_n(\mathbb{R})$, the action is trivial, and $\mathrm{O}_n(\mathbb{R})$ is the inner direct product $\mathrm{SO}_n(\mathbb{R}) \times \{\pm I_n\}$.

39. Eine Folge von Gruppen und Homomorphismen der Form

$$\{e\} \to G' \xrightarrow{\beta} G \xrightarrow{\alpha} G'' \to \{e\}, \qquad (*)$$

heisst **kurze exakte Folge**, falls β injektiv und α surjektiv ist, und $\ker(\alpha) = \operatorname{Im}(\beta)$. Man sagt, dass die kurze exakte Folge $(*)$ **zerfällt**, falls es einen Homomorphismus $\gamma\colon G'' \to G$ gibt so, dass $\alpha \circ \gamma = id_{G''}$ ist.

(a) Seien N, H zwei Gruppen und sei $G = N \rtimes H$ das semidirekte Produkt von N und H. Zeige, dass es eine kurze exakte Folge

$$\{e\} \to N \xrightarrow{\beta} G \xrightarrow{\alpha} H \to \{e\}$$

gibt, die zerfällt.

(b) Sei

$$\{e\} \to N \xrightarrow{\beta} G \xrightarrow{\alpha} H \to \{e\}$$

eine kurze exakte Folge, die zerfällt.
Zeige, dass dann $G \cong N \rtimes_\varphi H$.

Lösung: (a) Wir wählen für $\beta\colon N \to G$ die Einbettung $n \mapsto (n, e_H)$ und für $\alpha\colon G \to H$ die Projektion $(n,h) \mapsto h$. Dann gilt

$$\beta(n_1) \circ_\varphi \beta(n_2) = (n_1, e_H) \circ_\varphi (n_2, e_H) = (n_1 \underbrace{\varphi_{e_H}}_{id_N}(n_2), e_H) = (n_1 n_2, e_H) = \beta(n_1 n_2),$$

da φ ein Gruppenhomomorphismus ist, wird e_H auf id_N abgebildet. Weiter gilt

$$\alpha(n_1, h_1)\alpha(n_1, h_1) = h_1 h_2 = \alpha(n_1 \varphi_{h_1}(n_2), h_1 h_2) = \alpha((n_1, h_1) \circ_\varphi (n_2, h_2)).$$

Somit sind α und β Gruppenhomomorphismen. Es ist klar, dass β injektv ($\ker \beta = e_H$) und α surjektiv ist (für jedes $h \in H$ ist $(e_N, h) \in G$ mit $\alpha((e_N, h)) = h$).

Wählen wir weiter für $\gamma\colon H \to G$ die Einbettung $h \mapsto (e_N, h)$. Dann gilt

$$\gamma(h_1) \circ_\varphi \gamma(h_2) = (e_N, h_1) \circ_\varphi (e_N, h_2) = (e_N \varphi_{h_1}(e_N), h_1 h_2) = (e_N, h_1 h_2) = \gamma(h_1 h_2).$$

Also ist γ ein Gruppenhomomophismus und es gilt für alle $h \in H$

$$\alpha(\gamma(h)) = \alpha((e_N, h)) = h,$$

das heisst $\alpha \circ \gamma = id_H$. Somit ist

$$\{e\} \to N \xrightarrow{\beta} G \xrightarrow{\alpha} H \to \{e\}$$

eine kurze exakte Folge, die zerfällt.

(b) Sei $\tilde{N} := \operatorname{Im} \beta$. Dann ist $\tilde{N} \leqslant G$ und wegen $\tilde{N} = \operatorname{Im} \beta = \ker \alpha$ folgt $\tilde{N} \trianglelefteq G$. Da β injektiv ist gilt $N \cong \tilde{N}$. Weiter sei $\tilde{H} := \operatorname{Im} \gamma \leqslant G$, wobei $\gamma\colon H \to G$ der Homomorphismus ist, der $\gamma \circ \alpha = id_H$ erfüllt. Dann existiert für jedes $g \in \tilde{N} \cap \tilde{H}$ ein $h \in H$ mit $\gamma(h) = g$ und es gilt

$$\alpha(g) = e_H \Leftrightarrow \alpha(\gamma(h)) = e_H \Leftrightarrow h = e_H \Leftrightarrow \gamma(h) = \gamma(e_H) \Leftrightarrow g = e_G.$$

Daher ist $\tilde{N} \cap \tilde{H} = \{e_G\}$. Da α surjektiv ist, muss γ injektiv sein und wir haben $H \cong \tilde{H}$.

Sei nun $g \in G$ und $h := \gamma(\alpha(g)) \in \tilde{H}$. Dann ist $\alpha(gh^{-1}) = \alpha(g) \cdot \alpha(\gamma(\alpha(g)))^{-1} = e_H$ und somit $gh^{-1} \in \tilde{N}$. Sei $n := gh^{-1}$, dann folgt $g = nh$. Somit gibt es für jedes $g \in G$ ein $n \in \tilde{N}$ und ein $h \in \tilde{H}$ mit $g = nh$. Also ist $G = \tilde{N}\tilde{H}$ und wie erhalten

$$G \cong \tilde{N} \rtimes \tilde{H} \cong N \rtimes H.$$

40. Sei $p > 2$ eine Primzahl und sei G eine Gruppe mit Ordnung $|G| = 2p$.

Zeige, dass G entweder zyklisch oder isomorph zur Diedergruppe D_{2p} ist.

Lösung: Mit dem ersten Sylowsatz oder Cauchy's Theorem folgt, dass die Gruppe G Elemente x und y mit $\operatorname{ord}(x) = 2$ und $\operatorname{ord}(y) = p$ enthählt. 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

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

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 $\frac{2\pi}{p}$.

41. 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 $\varphi'_h = \alpha \circ \varphi_h \circ \alpha^{-1}$. 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,

$$\begin{aligned} \gamma(n_1,h_1) \circ_{\varphi'} \gamma(n_2,h_2) &= (\alpha(n_1),h_1) \circ_{\varphi'} (\alpha(n_2),h_2) = (\alpha(n_1) \cdot \varphi'_{h_1}(\alpha(n_2)), h_1h_2) \\ &= (\alpha(n_1) \cdot (\alpha \circ \varphi_{h_1} \circ \alpha^{-1})(\alpha(n_2)), h_1h_2) \\ &= (\alpha(n_1) \cdot \alpha(\varphi_{h_1}(n_2)), h_1h_2) = (\alpha(n_1 \cdot \varphi_{h_1}(n_2)), h_1h_2) \\ &= \gamma(n_1 \cdot \varphi_{h_1}(n_2), h_1h_2) = \gamma((n_1,h_1) \circ_\varphi (n_2,h_2)) \end{aligned}$$

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 $(n_1,h_1),(n_2,h_2) \in N \rtimes_\varphi H$

$$\begin{aligned} \delta(n_1,h_1) \circ_{\varphi'} \delta(n_2,h_2) &= (n_1,\beta(h_1)) \circ_{\varphi'} (n_2,\beta(h_2)) = (n_1 \cdot \varphi'_{\beta(h_1)}(n_2), \beta(h_1) \cdot \beta(h_2)) \\ &= (n_1 \cdot (\varphi \circ \beta^{-1})(\beta(h_1))(n_2), \beta(h_1h_2)) = (n_1 \cdot \varphi_{h_1}(n_2), \beta(h_1h_2)) \\ &= \delta(n_1 \cdot \varphi_{h_1}(n_2), h_1h_2) = \delta((n_1,h_1) \circ_\varphi (n_2,h_2)) \end{aligned}$$

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

42. Bestimme, bis auf Isomorphie, alle Gruppen der Ordnung 28.

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 $C_7 \trianglelefteq H$ ist gilt $C_7H = HC_7$ und somit ist C_7H nach Aufgabe 15(b) eine Untergruppe von G. Wegen $C_7 \leqslant C_7H$ und $H \leqslant C_7H$ gilt 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 Zaheln 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 27(a) haben wir $\mathrm{Aut}(C_7)$ bestimmt. Es ist

$$(\{k + 7\mathbb{Z} : \mathrm{ggT}(k,7) = 1\}, \cdot) = (\{1 + 7\mathbb{Z}, \ldots, 6 + 7\mathbb{Z}\}, \cdot),$$

also eine abelsche Gruppe mit 6 Elementen. Somit muss $\mathrm{Aut}(C_7) \cong C_6$ gelten. Wir machen nur 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 $\mathrm{ord}(\varphi(g))|\,\mathrm{ord}(g)$ gibt es nur die beiden Möglichkeiten $\varphi(g) = e$ und $\varphi(g) = 7 + 7\mathbb{Z}$. 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 $H = C_2 \times C_2$. Alle möglichen Homomorphismen $\varphi\colon C_2 \times C_2 \to \mathrm{Aut}(C_7)$ sind

(a) $\varphi_0(g,e) = 1 + 7\mathbb{Z}, \varphi(e,g) = 1 + 7\mathbb{Z}$

(b) $\varphi_1(g,e) = 3 + 7\mathbb{Z}, \varphi(e,g) = 1 + 7\mathbb{Z}$

(c) $\varphi_2(g,e) = 1 + 7\mathbb{Z}, \varphi(e,g) = 3 + 7\mathbb{Z}$

(d) $\varphi_3(g,e) = 3 + 7\mathbb{Z}, \varphi(e,g) = 3 + 7\mathbb{Z}$.

Die letzeten drei Möglichkeiten geben nach Aufgabe 24(b) jedoch bis auf Isomorphie dasselbe 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 $(C_2 \times C_2) \ltimes_{\varphi_1} C_7 \cong D_{14}$.