Gruppentheorie

FSU Jena - SS 2009

Übungsserie 05 - Lösungen

Stilianos Louca

May 22, 2009

Aufgabe 18

(i) O.B.d.A $k \in \mathbb{N}$ (da auch $g^{-k} = 1$ und der Fall $k = 0$ trivial ist). Offensichtlich ist $k \geq m$, so dass aus $m \nmid k$ folgen würde $k = n \cdot m + r$ mit $m > r \in \mathbb{N}$, $n \in \mathbb{N}_0$, das heißt

$$g^r = g^{k-nm} = \underbrace{g^k}_{1} \cdot \underbrace{(g^m)^{-n}}_{1} = 1$$

ein Widerspruch zu $m = \min \left\{ l \in \mathbb{N} : g^l = 1 \right\}$.

(ii) Nach (i) ist $g^{kl} = 1$ äquivalent zu $m \mid kl$. Unter Verwendung von

$$\mathrm{kgV}(m,k) = \frac{mk}{\mathrm{ggT}(m,k)}$$

schreiben wir

$$\frac{m}{\mathrm{ggT}(m,k)} = \frac{1}{k}\,\mathrm{kgV}(m,k) = \frac{1}{k}\min\{l \in \mathbb{N} : m \mid l \ \wedge \ k \mid l\} = \frac{1}{k}\min\{kl : m \mid kl \ \wedge \ l \in \mathbb{N}\}$$

$$= \min\{l \in \mathbb{N} : m \mid kl\} = \min\left\{l \in \mathbb{N} : g^{kl} = 1\right\} = \left|\left\langle g^k \right\rangle\right|$$

(iii) Wegen $h^n = 1$ ist

$$g^n = g^n h^n \overset{gh=hg}{=} (gh)^n \in \langle gh \rangle$$

ist $\langle g^n \rangle \leq \langle gh \rangle$, das heißt

$$\underbrace{|\langle g^n \rangle|}_{\frac{m}{\mathrm{ggT}(m,n)}=m} \Big| \, |\langle gh \rangle|$$

Analog auch $n \big| \, |\langle gh \rangle|$. Anderseits ist

$$(gh)^{\mathrm{kgV}(m,n)} = \underbrace{g^{\mathrm{kgV}(m,n)}}_{1} \underbrace{h^{\mathrm{kgV}(m,n)}}_{1} = 1$$

das heißt $\mathrm{kgV}(m,n) \geq |\langle gh \rangle| \geq \mathrm{kgV}(m,n)$, also

$$|\langle gh \rangle| = \mathrm{kgV}(m,n) = \frac{mn}{\mathrm{ggT}(m,n)} = mn$$

□

Aufgabe 19

Gruppeneigenschaften

Für

$$(g_1, .., g_n; \sigma),\ (h_1, .., h_n; \tau),\ (q_1, .., q_n; \rho) \in G \wr H$$

ist

$$\begin{aligned}(g_1, .., g_n; \sigma)\,[(h_1, .., h_n; \tau)(q_1, .., q_n; \rho)] &= (g_1, .., g_n; \sigma)\left(h_1 q_{\tau^{-1}(1)}, .., h_n q_{\tau^{-1}(n)}; \tau\rho\right)\\ &= \left(g_1 h_{\sigma^{-1}(1)} q_{\tau^{-1}(\sigma^{-1}(1))}, .., g_n h_{\sigma^{-1}(1)} q_{\tau^{-1}(\sigma^{-1}(n)}; \sigma\tau\rho\right)\\ &= \left(g_1 h_{\sigma^{-1}(1)} q_{(\sigma\tau)^{-1}(1)}, .., g_n h_{\sigma^{-1}(n)} q_{(\sigma\tau)^{-1}(n)}; \sigma\tau\rho\right)\\ &= \underbrace{\left(g_1 h_{\sigma^{-1}(1)}, .., g_n h_{\sigma^{-1}(n)}; \sigma\tau\right)(q_1, .., q_n; \rho)}_{[(g_1, .., g_n; \sigma)(h_1, .., h_n; \tau)](q_1, .., q_n; \rho)}\end{aligned}$$

das heißt $G \wr H$ ist eine Halbgruppe. Dabei ist

$$1 := (1, .., 1; 1)$$

das neutrale Element, und zu $(g_1, .., g_n; \sigma) \in G \wr H$

$$\left(g_{\sigma(1)}^{-1}, .., g_{\sigma(n)}^{-1}; \sigma^{-1}\right) \overset{\sigma^{-1} \in H}{\in} G \wr H$$

das inverse, das heißt $G \wr H$ ist tatsächlich eine Gruppe.

Konstruktion von N

Setzen

$$N := \{(g_1, .., g_n; 1) : g_i \in G\}$$

Dann ist offensichtlich $N \leq G \wr H$ und $N \cong \underbrace{G \times \cdots \times G}_{\times n}$. Es ist sogar $N \trianglelefteq G$, denn für $(h_1, .., h_n; \sigma) \in G \wr H$ ist

$$(h_1, .., h_n; \sigma)N = \left\{\left(h_1 g_{\sigma^{-1}(1)}, .., h_n g_{\sigma^{-1}(n)}; \sigma\right) : g_i \in G\right\} = \{(h_1 g_1, .., h_n g_n; \sigma) : g_i \in G\}$$

$$\overset{G \trianglelefteq G}{=} \{(g_1 h_1, .., g_n h_n; \sigma) : g_i \in G\} = N(h_1, .., h_n; \sigma)$$

Konstruktion von U

Setzen

$$U := \{(1, .., 1; \sigma) : \sigma \in H\}$$

Dann ist $U \leq G \wr H$ denn $1 \in U$ und für $(1, .., 1; \sigma),\ (1, .., 1; \tau) \in U$ ist auch

$$(1, .., 1; \sigma)(1, .., 1; \tau)^{-1} = (1, .., 1; \sigma\tau^{-1}) \overset{H \leq \mathrm{Sym}(n)}{\in} U$$

Natürlich ist $U \cong H$.

Eigenschaften von N und U

Einerseits ist

$$NU = \{(g_1, .., g_n; 1)(1, .., 1; \sigma) : g_i \in G,\ \sigma \in H\} = \{(g_1, .., g_n; \sigma) : g_i \in G,\ \sigma \in H\} = G \wr H$$

$N \cap U = \{1\}$ ist klar.

Variante

Wir zeigen dass $G \wr H$ ein semi-direktes Produkt der form $(\overbrace{\underbrace{G \times \cdots \times G}_{\times n}}^{G^n}) \rtimes_\varphi H$ ist. Dafür sei

$$\varphi : H \to \mathrm{Aut}(G^n) \quad , \quad h \mapsto \varphi_h$$

mit

$$\varphi_h(g_1, .., g_n) := \big(g_{h^{-1}(1)}, .., g_{h^{-1}(n)}\big)$$

Dann ist für $(g_1, .., g_n),\ (g'_1, .., g'_n) \in G^n$:

$$\varphi_h(g_1g'_1, .., g_ng'_n) = \Big(g_{h^{-1}(1)}g'_{h^{-1}(1)}, .., g_{h^{-1}(n)}g'_{h^{-1}(n)}\Big) = \varphi_h(g_1, .., g_n)\varphi_h(g'_1, .., g'_n)$$

das heißt φ_h ist homomorph. Bijektivität von φ_h ist klar, so dass tatsächlich $\varphi_h \in \mathrm{Aut}(G^n)$ ist.

Anderseits ist für $h_1, h_2 \in H$ und $(g_1, .., g_n) \in G^n$:

$$(\varphi_{h_1} \circ \varphi_{h_2})(g_1, .., g_n) = \varphi_{h_1^{-1}}\Big(g_{h_2^{-1}(1)}, .., g_{h_2^{-1}(n)}\Big) = \Big(g_{h_2^{-1}(h_1^{-1}(1))}, .., g_{h_2^{-1}(h_1^{-1}(n))}\Big)$$

$$= \big(g_{(h_1h_2)^{-1}(1)}, .., g_{(h_1h_2)^{-1}(n)}\big) = \varphi_{h_1h_2}(g_1, .., g_n)$$

das heißt φ ist homomorph. Somit existiert $G^n \rtimes_\varphi H$.

Wegen

$$(g_1, .., g_n, h) \circ_{G^n \rtimes_\varphi H} (g'_1, .., g'_n, h') = ((g_1, .., g_n)\, \varphi_h(g'_1, .., g'_n),\ hh') = \Big(g_1g'_{h^{-1}(1)}, .., g_ng'_{h^{-1}(n)},\ hh'\Big)$$

$$= (g_1, .., g_n, h) \circ_{G \rtimes H} (g'_1, .., g'_n, h')$$

ist tatsächlich $G^n \rtimes_\varphi H = G \wr H$. Die restlichen Aussagen folgen aus den Eigenschaften des Semiprodukts (vgl. Übungsaufgabe 14).
□

Aufgabe 20

(i) $Z(G) \trianglelefteq G$ und G einfach ist, ist $Z(G) = G$ oder $Z(G) = \{1_G\}$. Da jedoch G nicht abelsch ist ($G \neq Z(G)$) ist $Z(G) = \{1\}$. Demnach
$$\mathrm{Inn}(G) \cong G/Z(G) \cong G$$
Zu beliebigen $A \in \mathrm{Aut}(\mathrm{Aut}(G))$ sei nun $I_A := A(\mathrm{Inn}(G)) \cap \mathrm{Inn}(G)$. Da $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ ist auch $A(\mathrm{Inn}(G)) \trianglelefteq A(\mathrm{Aut}(G)) = \mathrm{Aut}(G)$ bzw. $I_A \trianglelefteq \mathrm{Aut}(G)$. Insbesondere $I_A \trianglelefteq \mathrm{Inn}(G)$. Nach obiger Überlegung ist jedoch $\mathrm{Inn}(G)$ einfach (da Einfachheit Isomorphieinvariant), das heißt $I_A = \{1\}$ oder $I_A = \mathrm{Inn}(G)$.

O.B.d.A sei also $I_A = \{1\}$ (sonst wären wir fertig). Dann kommutiert jedes Element von $A(\mathrm{Inn}(G))$ mit $\mathrm{Inn}(G)$, das heißt
$$A(\mathrm{Inn}(G)) \subset C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) \overset{\substack{\text{ÜA}\\(15)}}{=} \{1\}$$
das heißt in jedem Fall $A(\mathrm{Inn}(G)) \subset \mathrm{Inn}(G)$. Da A beliebig war, ist $\mathrm{Inn}(G)$ charakteristisch in $\mathrm{Aut}(G)$.

(ii) Betrachtet sei der Homomorphismus
$$\mathrm{ad} : G \to \mathrm{Inn}(G) \quad , \quad g \mapsto \mathrm{ad}_g$$
Nach dem Homomorphiesatz ist
$$F : G/\ker(\mathrm{ad}) \to \mathrm{ad}(G) = \mathrm{Inn}(G) \quad , \quad \underbrace{g\ker(\mathrm{ad})}_{g\{1\}} \mapsto \mathrm{ad}_g,\ g \in G$$

(und somit auch ad) ein Isomorphismus.Sei nun $A \in \mathrm{Aut}(\mathrm{Aut}(G))$ beliebig, dann ist nach Teil (i) $A(\mathrm{Inn}(G)) = \mathrm{Inn}(G)$ und somit

$$A\big|_{\mathrm{Inn}(G)} \in \mathrm{Aut}(\mathrm{Inn}(G))$$

Setzen $g := \mathrm{ad}^{-1} \circ A\big|_{\mathrm{Inn}(G)} \circ \mathrm{ad} \in \mathrm{Aut}(G)$.
Behauptung: $\mathrm{ad}_g\big|_{\mathrm{Inn}(G)} = A\big|_{\mathrm{Inn}(G)}$. Tatsächlich gilt für $x, y \in G$:

$$\begin{aligned}
[\mathrm{ad}_g(\mathrm{ad}_x)](y) &= \left(g \circ \mathrm{ad}_x \circ g^{-1}\right)(y) = g\left(xg^{-1}(y)x^{-1}\right) = g(x)yg(x^{-1}) \\
&= \mathrm{ad}^{-1}\left(A\left(\mathrm{ad}_x\right)\right) y\, \mathrm{ad}^{-1}(A(\underbrace{\mathrm{ad}_{x^{-1}}}_{\mathrm{ad}_x^{-1}})) = \mathrm{ad}^{-1}\left[A(\mathrm{ad}_x)\,\mathrm{ad}_y\, A(\mathrm{ad}_x)^{-1}\right] \\
&= \mathrm{ad}^{-1}\left[\mathrm{ad}_{A(\mathrm{ad}_x)(y)}\right] = A(\mathrm{ad}_x)(y)
\end{aligned}$$

$$\Rightarrow \quad \mathrm{ad}_g(\mathrm{ad}_x) = A(\mathrm{ad}_x) \quad \Rightarrow \quad \mathrm{ad}_g\big|_{\mathrm{Inn}(G)} = A\big|_{\mathrm{Inn}(G)}$$

Behauptung: Es ist sogar $\mathrm{ad}_g = A$. Tatsächlich, nach obigen Überlegungen ist

$$\underbrace{\left(A^{-1} \circ \mathrm{ad}_g\right)}_{\mathrm{Id}_{\mathrm{Inn}(G)}}(\mathrm{ad}_x) = \mathrm{ad}_x$$

Für beliebigen $\alpha \in \mathrm{Aut}(G)$ gilt nun

$$\alpha \circ \mathrm{ad}_x \circ \alpha^{-1} = \mathrm{ad}_{\alpha(x)} \in \mathrm{Inn}(G)$$

$$\Rightarrow \quad \alpha \circ \mathrm{ad}_x \circ \alpha^{-1} = (A^{-1} \circ \mathrm{ad}_g)(\alpha \circ \mathrm{ad}_x \circ \alpha^{-1}) = A^{-1}\left(\mathrm{ad}_g(\alpha)\right) \mathrm{ad}_x\, A^{-1}\left(\mathrm{ad}_g(\alpha)\right)^{-1}$$

$$\Rightarrow \quad \alpha^{-1}A^{-1}(\mathrm{ad}_g(\alpha))\,\mathrm{ad}_x = \mathrm{ad}_x\, \alpha^{-1}A^{-1}(\mathrm{ad}_g(\alpha)) \quad \forall\, x \in G$$

das heißt

$$\alpha^{-1}A^{-1}(\mathrm{ad}_g(\alpha)) \in C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) \overset{\substack{\text{ÜA} \\ (15)}}{=} \{1\}$$

bzw.

$$A^{-1}(\mathrm{ad}_g(\alpha)) = \alpha \quad \Rightarrow \quad A^{-1} \circ \mathrm{ad}_g = \mathrm{Id}_{\mathrm{Aut}(G)}$$

Demnach ist $A = \mathrm{ad}_g \in \mathrm{Inn}(\mathrm{Aut}(G))$. Da A allgemein war, ist $\mathrm{Aut}(\mathrm{Aut}(G)) \subset \mathrm{Inn}(\mathrm{Aut}(G))$. Die andere Inklusion ist trivial.

□

Aufgabe 21

(i)

(ii) Sei G eine Gruppe der Ordnung 6 und $1 \neq q \in G$. Nach Lagrange ist $|\langle q\rangle| \mid 6$, das heißt $|\langle q\rangle| \in \{2, 3, 6\}$.

- Fall $|\langle q\rangle| = 6$ für ein $q \in G$, dann ist $G = \langle q\rangle$. Solch eine Gruppe existiert tatsächlich, z.B. $\mathbb{Z}/6\mathbb{Z}$. Ferner sind alle zyklischen Gruppen der Ordnung 6 isomorph.
- Fall $\langle q\rangle \neq G \;\; \forall\, q \in G$. Sei also $1 \neq q$, dazu $p \notin \langle q\rangle$. Bemerke dass dann auch $q \notin \langle p\rangle$ gilt, da per Wahl $q \notin \{1, p\}$ und aus $q = p^2$ folgen würde $q = 1$ (falls $|\langle p\rangle| = 2$) oder $q^2 = p$ (falls $|\langle p\rangle| = 3$ da $q^2 = p^3p$).
  Dabei kann nicht $|\langle q\rangle| = |\langle p\rangle| = 3$ gelten, denn sonst $qp \notin \left\{1, q, p, q^2, p^2\right\}$ also $G = \left\{1, q, q^2, p, p^2, qp\right\}$, doch anderseits $q^2p \notin \left\{1, q, p, q^2, p^2, qp\right\}$, ein Widerspruch.
  Somit:

- Fall $|\langle q\rangle| = 2,\ |\langle p\rangle| = 3$ (beachte dass q,p vollkommen gleichbedeutend sind). Dann $qp \notin \{1,q,p,p^2\}$ (da sonst $q = p^{-1}$ oder $p = 1$ oder $q = 1$ oder $q = p$). Außerdem $qp^2 \notin \{1,q,p,p^2,qp\}$ (da sonst $p^2 = q$ oder $p^2 = 1$ oder $q = p^{-1}$ oder $q = 1$ oder $p = 1$), somit

$$G = \{1,q,p,p^2,qp,qp^2\}$$

Dabei ist $pq \notin \{1,q,p,p^2\}$ und somit $pq = qp^2$ (im Fall $pq = qp$ ist $G = \langle qp^2\rangle$ was dem oben diskutierten Fall entspricht).
Somit Verknüpfungstabelle:

	1	q	p	p^2	qp	qp^2
1	1	q	p	p^2	qp	qp^2
q	q	1	qp	qp^2	p	p^2
p	p	qp^2	p^2	1	q	qp
p^2	p^2	qp	1	p	qp^2	q
qp	qp	p^2	qp^2	q	1	p
qp^2	qp^2	p	q	qp	p^2	1

Beispiel: $q := (1\ 2),\ p := (1\ 2\ 3)$ also $G = \mathrm{Sym}(3)$.

- Fall $|\langle q\rangle| = |\langle p\rangle| = 2$. Dann ist $qp \notin \{1,q,p\}$ (da sonst $q = p^{-1}$ oder $p = 1$ oder. $q = 1$) und $pq \notin \{1,q,p,qp\}$ (da sonst $q = p^{-1}$ oder $q = 1$ oder $p = 1$ oder $\{1,q,p,qp\} \leq G$ ein Widerspruch zu Lagrange). Außerdem ist $qpq \notin \{1,q,p,qp,pq\}$ (da sonst $qp = q$ oder $qp = 1$ oder $qp = pq$ oder $q = 1$ oder $q = 1$), somit
$$G = \{1,q,p,qp,pq,qpq\}$$
(analoges gilt auch für pqp, also $qpq = pqp$). Setzen nun $\tilde{p} := qp$ und $\tilde{q} := q$. Dann
$$\tilde{p} \notin \langle\tilde{q}\rangle \quad , \quad |\langle\tilde{q}\rangle| = 2$$
und außerdem
$$\tilde{p}^3 = (qpq)\underbrace{(pqp)}_{qpq} = 1 \ \Rightarrow\ \tilde{p}^2 \neq 1 \quad \Rightarrow \quad |\langle\tilde{p}\rangle| = 3$$
Somit ist dieser Fall gleich dem Fall $|\langle q\rangle| = 2,\ |\langle p\rangle| = 3$.