M. Künzer

Gruppentheorie, SoSe 25

Lösung 2

Hausaufgabe 5 Sei $G := \langle (1,4), (1,2,3)(4,5,6)\rangle \leqslant \mathrm{S}_7$.
Wir betrachten die G-Menge $M := [1,7]$.

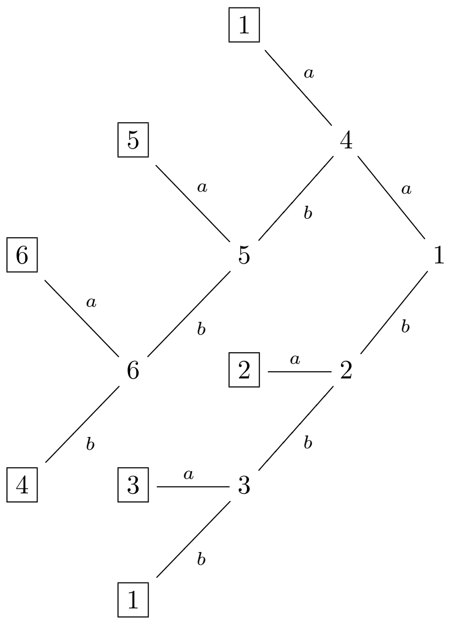
(1) Man berechne die Bahn $G \cdot 1$.

(2) Man berechne Erzeuger von $\mathrm{C}_G(1)$. Ist $\mathrm{C}_G(1)$ abelsch?

(3) Man verwende das Bahnenlemma und (1), (2), um $|G|$ zu berechnen.

(4) Ist $G \cdot 1$ eine primitive G-Menge? Kann man einen Block B mit $1 < |B| < |G \cdot 1|$ angeben?

Lösung.
Ad $(1,2)$. Wir schreiben $a := (1,4)$ und $b := (1,2,3)(4,5,6)$.
Wir erstellen folgenden Baum von rechts nach links.



Die Einträge nicht in Kästen geben $G \cdot 1 = \{1,2,3,4,5,6\}$.
Die Einträge in den Kästen geben, von rechts nach links:

$$
\begin{array}{lrcllcl}
\boxed{1}: & \tau(a \circ a)^- \circ (a \circ a) & = & \mathrm{id}^- \circ a^2 & & = & \mathrm{id} \\
\boxed{2}: & \tau(a \circ b)^- \circ (a \circ b) & = & b^- \circ (a \circ b) & & = & (3,6) \\
\boxed{5}: & \tau(a \circ b \circ a)^- \circ (a \circ b \circ a) & = & (b \circ a)^- \circ (a \circ b \circ a) & & = & (3,6) \\
\boxed{3}: & \tau(a \circ b \circ b)^- \circ (a \circ b \circ b) & = & b^{-2} \circ (a \circ b \circ b) & & = & (2,5) \\
\boxed{1}: & \tau(b \circ b \circ b)^- \circ (b \circ b \circ b) & = & \mathrm{id}^- \circ b^3 & & = & \mathrm{id} \\
\boxed{6}: & \tau(a \circ b^2 \circ a)^- \circ (a \circ b^2 \circ a) & = & (b^2 \circ a)^- \circ (a \circ b^2 \circ a) & & = & (2,5) \\
\boxed{4}: & \tau(b^3 \circ a)^- \circ (b^3 \circ a) & = & a^- \circ (b^3 \circ a) & & = & \mathrm{id}
\end{array}
$$

Folglich ist $\mathrm{C}_G(1) = \langle (2,5), (3,6)\rangle$. Da die Erzeuger kommutieren, ist $\mathrm{C}_G(1)$ abelsch.

Ad (3). Da $\mathrm{C}_G(1)$ abelsch ist, ist $\mathrm{C}_G(1) = \{\, (2,5)^k \circ (3,6)^\ell \, : \, k, \, \ell \in \mathbb{Z} \,\} = \{\mathrm{id}, (2,5), (3,6), (2,5)(3,6)\}$. Folglich ist $|\mathrm{C}_G(1)| = 4$.
Das Bahnenlemma gibt $|G| = |G \cdot 1| \cdot |\mathrm{C}_G(1)| = 6 \cdot 4 = 24$.

Ad (4). Wir behaupten, daß $B := \{1,4\}$ ein Block ist.

Wir berechnen seine Bahn in der Potenzmenge von M mittels folgendem Baum.

$$\begin{tikzcd}
\boxed{\{3,6\}} \arrow[dr, dash, "a"] & \boxed{\{2,5\}} \arrow[dr, dash, "a"] & \boxed{\{1,4\}} \arrow[dr, dash, "a"] & \\
\boxed{\{1,4\}} \arrow[r, dash, "b"] & \{3,6\} \arrow[r, dash, "b"] & \{2,5\} \arrow[r, dash, "b"] & \{1,4\}
\end{tikzcd}$$

Somit ist tatsächlich $g \cdot B = B$ oder $g \cdot B \cap B = \emptyset$ für $g \in G$. Also ist B ein Block.
Da B mehr als ein Element, aber weniger als $|G \cdot 1| = 6$ Elemente hat, folgt aus dem Vorhandensein dieses Blocks, daß M eine nicht-primitive G-Menge ist.

Hausaufgabe 6 (A7, A4) Man zeige.

(1) Sei p prim. Sei P eine p-*Gruppe,* i.e. sei P eine endliche Gruppe und p der einzige Primteiler von $|P|$. Sei M eine endliche P-Menge. Dann ist $|\mathrm{Fix}_P(M)| \equiv_p |M|$.

(2) Sei G eine endliche Gruppe. Sei p ein Primteiler von $|G|$.
Dann gibt es in G ein Element von Ordnung p.
(Hinweis: Es ist $M := \{\, (g_i)_i \in G^{\times p} \;:\; g_1 g_2 \cdot \ldots \cdot g_p = 1 \,\}$ eine C_p-Menge.
Wieso ist $|\mathrm{Fix}_{\mathrm{C}_p}(M)| \geqslant p\,$?)

(3) Sei G eine Gruppe. Sei $U \leqslant G$. Sei $\mathrm{N}_G(U) := \{\, g \in G \;:\; {}^gU = U \,\}$ der *Normalisator* von U in G. Dann ist $\mathrm{C}_G(U) \trianglelefteqslant \mathrm{N}_G(U)$ und $U \trianglelefteqslant \mathrm{N}_G(U)$.

Lösung.
Ad (1). Sei $k := |\{\, Pm \;:\; m \in M \,\}|$. Seien $k \geqslant 1$ und $m_i \in M$ für $i \in [1,k]$ so gewählt, daß $M = \bigsqcup_{i \in [1,k]} Pm_i$ ist. Es ist $\mathrm{Fix}_P(M) = \{\, m_i \;:\; i \in [1,k],\ |Pm_i| = 1 \,\}$. Folglich ist

$$M \smallsetminus \mathrm{Fix}_P(M) \;=\; \bigsqcup_{i \in [1,k],\ |Pm_i| > 1} Pm_i \;.$$

Wir haben $|M \smallsetminus \mathrm{Fix}_P(M)| \overset{!}{\equiv}_p 0$ zu zeigen. Es genügt, $|Pm_i| \overset{!}{\equiv}_p 0$ für $i \in [1,k]$ mit $|Pm_i| > 1$ zu zeigen. Aber $|Pm_i|$ ist ein Teiler von $|P|$. Da $|P|$ eine Potenz von p ist und da $|Pm_i| \neq 1$ ist, folgt $|Pm_i| \equiv_p 0$.
Ad (2). Es operiert S_p auf $G^{\times p}$ via $\sigma \cdot (g_i)_i := (g_{\sigma^-(i)})_i$ für $(g_i)_i \in G^{\times p}$. Sei $\sigma := (1, 2, \ldots, p) \in \mathrm{S}_p$. Durch Einschränkung operiert auch $\langle \sigma \rangle$ auf $G^{\times p}$. Ist nun $(g_i)_i$ in M, dann ist auch $\sigma \cdot (g_i)_i$ in M, da aus $g_1 g_2 \cdots g_p = 1$ durch Konjugation mit g_p folgt, daß $g_p g_1 g_2 \cdots g_{p-1} = 1$ ist.
Es ist $(1, 1, \ldots, 1) \in \mathrm{Fix}_{\mathrm{C}_p}(M)$, mithin $|\mathrm{Fix}_{\mathrm{C}_p}(M)| \geqslant 1$.
Es ist $|M| = |G|^{p-1} \equiv_p 0$, da wir eine Bijektion $G^{\times (p-1)} \to M$, $(g_i)_i \mapsto (g_1\,, \ldots\,, g_{p-1}\,, (g_1 \cdots g_{p-1})^-)$ haben.
Dank (1) ist nun $|\mathrm{Fix}_{\mathrm{C}_p}(M)| \equiv_p |M| \equiv_p 0$, also $|\mathrm{Fix}_{\mathrm{C}_p}(M)| > 1$. Sei $(g_i)_i \in \mathrm{Fix}_{\mathrm{C}_p}(M) \smallsetminus \{(1, 1, \ldots, 1)\}$. Dann ist zum einen $x := g_1 = g_2 = \cdots = g_p$, aber $x \neq 1$, zum anderen $x^p = g_1 g_2 \cdots g_p = 1$. Also ist x ein Element in G mit $1 < |\langle x \rangle| \mid p$. Wegen p prim ist x also von Ordnung $|\langle x \rangle| = p$.

> *Alternative Lösung (von Maximilan Kotte):* Induktion über $|G|$. Sei die Aussage für Gruppen von Ordnung kleiner als $|G|$ bekannt. Seien $x_1, \ldots, x_k$ Repräsentanten der Konjugationsklassen von G von Kardinalität > 1. Dann ist $G = \mathrm{Z}(G) \sqcup \bigsqcup_{i \in [1,k]} {}^G x_i$. Also $|G| = |\mathrm{Z}(G)| + \sum_{i \in [1,k]} |G|/|\mathrm{C}_G(x_i)|$. Falls $|\mathrm{C}_G(x_i)| \equiv_p 0$ für ein $i \in [1,k]$, dann finden wir nach Induktionsvoraussetzung in einer dieser Gruppen und damit auch in G ein Element der Ordnung p. Falls $|\mathrm{C}_G(x_i)| \not\equiv_p 0$ für $i \in [1,k]$, dann ist $|\mathrm{Z}(G)| \equiv_p 0$. In der endlichen abelschen Gruppe $\mathrm{Z}(G)$ findet sich ein Element der Ordnung p.

Ad (3). Es ist

$$\begin{array}{rcl} \mathrm{N}_G(U) & = & \{\, g \in G \;:\; {}^gU = U \,\} \\ \mathrm{C}_G(U) & = & \{\, g \in G \;:\; {}^gu = u \text{ für } u \in U \,\}\,. \end{array}$$

Also ist $\mathrm{C}_G(U) \leqslant \mathrm{N}_G(U)$.
Ist $x \in \mathrm{N}_G(U)$, dann ist ${}^x\mathrm{C}_G(U) = \mathrm{C}_G({}^xU) = \mathrm{C}_G(U)$. Also ist $\mathrm{C}_G(U) \trianglelefteqslant \mathrm{N}_G(U)$.
Ist $x \in \mathrm{N}_G(U)$, dann ist ${}^xU = U$. Also ist $U \trianglelefteqslant \mathrm{N}_G(U)$.

Hausaufgabe 7 (A12) Sei G eine Gruppe. Seien $U, V \leqslant G$. Man zeige.

(1) Seien U und V endlich. Es ist $|UV| = |U| \cdot |V| / |U \cap V|$.

(2) Ist $U \leqslant \mathrm{N}_G(V)$, dann ist $V \trianglelefteq UV = VU \leqslant G$ und $U \cap V \trianglelefteq U$ und $U/(U \cap V) \xrightarrow{\sim} (UV)/V$, $u(U \cap V) \mapsto uV$ ein Gruppenisomorphismus.

(3) Sind $U, V \trianglelefteq G$, dann ist $UV \trianglelefteq G$.

(4) Sei $N \trianglelefteq G$. Sei $N \trianglelefteq H \trianglelefteq G$. Dann haben wir den Isomorphismus $G/H \xrightarrow{\sim} (G/N)/(H/N)$, $gH \mapsto (gN)(H/N)$.

Lösung.
Ad (1). Betrachte die surjektive Abbildung

$$\begin{array}{ccccc} U & \times & V & \xrightarrow{f} & UV \\ (u & , & v) & \mapsto & uv\,. \end{array}$$

Sei $x \in UV$. Wir haben zu zeigen, daß das Urbild $f^{-1}(\{x\})$ in Bijektion steht zu $U \cap V$, da dann die disjunkte Zerlegung $U \times V = \bigsqcup_{x \in UV} f^{-1}(\{x\})$ die Gleichheit $|U \times V| = |UV| \cdot |U \cap V|$ nach sich zieht, wie verlangt.

Schreibe $x = u_0 v_0$. Wir *behaupten* $f^{-1}(\{x\}) \overset{!}{=} \{\, (u_0 t, t^- v_0) \;:\; t \in U \cap V \,\}$; was dann auch die benötigte Bijektion liefert, nämlich $U \cap V \to \{\, u_0 t v_0 \;:\; t \in U \cap V \,\}$, $t \mapsto u_0 t v_0$.

Zu zeigen ist nur $f^{-1}(\{x\}) \overset{!}{\subseteq} \{\, (u_0 t, t^- v_0) \;:\; t \in U \cap V \,\}$. Sei $(u, v) \in f^{-1}(\{x\})$. Es folgt $uv = x = u_0 v_0$ und also $t := u_0^- u = v_0 v^- \in U \cap V$ sowie $(u, v) = (u_0 u_0^- u, v v_0^- v_0) = (u_0 t, t^- v_0)$. Dies zeigt die *Behauptung*.

Ad (2). Wir zeigen $UV \overset{!}{=} VU$.

Wir zeigen $UV \overset{!}{\subseteq} VU$. Sei $u \in U$ und $v \in V$. Es ist $uv = (uvu^-)u = {}^{u}v \cdot u \in VU$, da $u \in \mathrm{N}_G(V)$.

Wir zeigen $UV \overset{!}{\supseteq} VU$. Sei $u \in U$ und $v \in V$. Es ist $vu = u(u^- vu) = u \cdot {}^{u^-}v \in UV$, da $u^- \in \mathrm{N}_G(V)$.
Nun ist $UV = VU$ erreicht.

Wir zeigen $UV \overset{!}{\leqslant} G$. Für $u, \tilde{u} \in U$ und $v, \tilde{v} \in V$ ist $uv(\tilde{u}\tilde{v})^- = uv\tilde{v}^-\tilde{u}^- = {}^{u}(v\tilde{v}^-)u\tilde{u}^- \in VU = UV$, da $u \in \mathrm{N}_G(V)$.

Wir zeigen $V \overset{!}{\trianglelefteq} UV$. Für $v, \tilde{v} \in V$ und $u \in U$ ist ${}^{uv}\tilde{v} = {}^{u}({}^{v}\tilde{v}) \in V$, da $u \in \mathrm{N}_G(V)$.

Wir zeigen $U \cap V \overset{!}{\trianglelefteq} U$. Für $t \in U \cap V$ und $u \in U$ ist ${}^{u}t \in U$, da $t \in U$, und ${}^{u}t \in V$, da $t \in V$ und $u \in \mathrm{N}_G(V)$.

Ad (3). Aus (2) wissen wir $UV \leqslant G$, da $U \leqslant G = \mathrm{N}_G(V)$. Wir zeigen $UV \overset{!}{\trianglelefteq} G$. Sei $g \in G$, $u \in U$ und $v \in V$. Es wird ${}^{g}(uv) = {}^{g}u \cdot {}^{g}v \in UV$, da $U \trianglelefteq G$ und $V \trianglelefteq G$.

Ad (4). Der surjektive Gruppenmorphismus $f : G \to (G/N)/(H/N)$, $g \mapsto (gN)(H/N)$, induziert den surjektiven Gruppenmorphismus $\bar{f} : G/H \xrightarrow{\sim} (G/N)/(H/N)$, $gH \mapsto (gN)(H/N)$, da $(hN)(H/N) = 1_{(G/N)/(H/N)}$ für $h \in H$.

Wir müssen zeigen, daß $\bar{f}$ injektiv ist. Für $g \in G$ ist $(gN)(H/N)$ genau dann gleich $1_{(G/N)/(H/N)}$, wenn $gN \in H/N$, i.e. $g \in H$, i.e. $gH = 1_{G/H}$ ist.

Hausaufgabe 8 (A5) Sei $n \geqslant 3$. Wir betrachten die A_n-Menge $[1, n]$.

(1) Man weise $[1, n]$ als $(n-2)$-fach transitive, aber nicht $(n-1)$-fach transitive A_n-Menge nach.

(2) Ist $[1, n]$ eine primitive A_n-Menge?

Lösung.
Ad (1). Um zu zeigen, daß $[1, n]$ eine $(n-2)$-fach transitive A_n-Menge ist, ist die A_n-Menge $[1, n]^{\times(n-2), \neq}$ als transitiv nachzuweisen.
Sei $(\, a_1\,, \ldots, a_{n-2}\,) \in [1, n]^{\times(n-2), \neq}$. Seien $k, \ell \in [1, n]$ die beiden nicht in diesem Tupel auftretenden Elemente. Sei $\sigma \in \mathrm{S}_n$ durch $\sigma(i) := a_i$ für $i \in [1, n]$, $\sigma(n-1) := k$ und $\sigma(n) := \ell$ festgelegt.
Falls $\sigma \in \mathrm{A}_n$ liegt, dann ist $\sigma \cdot (1, \ldots, n-2) = (\, a_1\,, \ldots, a_{n-2}\,)$.

Falls $\sigma \in \mathrm{S}_n \setminus \mathrm{A}_n$ liegt, dann ist $\sigma' := \sigma \circ (n-1, n) \in \mathrm{A}_n$ und $\sigma' \cdot (1, \dots, n-2) = (\, a_1 \,, \, \dots \,, \, a_{n-2} \,)$.

Um zu zeigen, daß $[1, n]$ keine $(n-1)$-fach transitive A_n-Menge ist, ist die A_n-Menge $[1, n]^{\times(n-1), \neq}$ als nicht-transitiv nachzuweisen.
Die einzige Permutation, die $(\, 1 \,, 2 \,, \, 3 \,, \, \dots \,, \, n-1)$ auf $(\, 2 \,, 1 \,, \, 3 \,, \, \dots \,, \, n-1)$, und also auch n auf n, abbildet, ist $(1, 2)$, und diese liegt in $\mathrm{S}_n \setminus \mathrm{A}_n$. Folglich liegen diese beiden Elemente von $[1, n]^{\times(n-1), \neq}$ in zwei verschiedenen A_n-Bahnen.

Ad (2). Ist $n \geqslant 4$, dann ist $[1, n]$ als $n-2$-fach transitive A_n-Menge wegen $n - 2 \geqslant 2$ auch primitiv.

Falls $n = 3$ ist, dann ist $[1, 3]$ eine primitive A_3-Menge, da $\mathrm{C}_{\mathrm{A}_3}(1) = 1$ eine maximale Untergruppe in $\mathrm{A}_3 = \langle (1, 2, 3) \rangle$ ist.