G. Nebe, M. Künzer

Algebra I, WS 04/05

Lösung 1

Aufgabe 5.

(1) Wir wollen zeigen, daß $(\rho(a_1,\ldots,a_k)\rho^{-1})(b) = (\rho(a_1),\ldots,\rho(a_k))(b)$ für alle $b\in[1,n]$.
Falls $b\notin\{\rho(a_i),\ldots,\rho(a_k)\}$, dann ist auch $\rho^{-1}(b)\notin\{a_1,\ldots,a_k\}$, und auf beiden Seiten steht einfach b.
Falls $b=\rho(a_i)$ mit $i\in[1,k-1]$, so erhalten wir auf beiden Seiten $\rho(a_{i+1})$.
Falls $b=\rho(a_k)$, so erhalten wir auf beiden Seiten $\rho(a_1)$.

(2) Die Elemente von $[1,n]$ in die Zykeln vorgegebener Länge zu verteilen, dafür gibt es $n!$ Möglichkeiten. Jeden Zykel kann man zyklisch vertauschen, ohne die Permutation zu ändern, also müssen wir $\prod_{m\in[1,n]} m^{u_m}$ abdividieren. Ferner kann man noch die Zykel gleicher Länge untereinander vertauschen, ohne die Permutation zu ändern, und somit müssen wir noch einen Faktor $\prod_{m\in[1,n]} u_m!$ abdividieren. Die Länge der Konjugiertenklasse ergibt sich somit zu

$$\frac{n!}{\prod_{m\in[1,n]} m^{u_m}\cdot u_m!}\ .$$

(3) Wir listen die Konjugiertenklassen mit Repräsentant und Länge auf.

$(1,2,3,4,5)$	$\frac{5!}{5^1\cdot 1!}$	$=$	24
$(1,2,3,4)(5)$	$\frac{5!}{(4^1\cdot 1!)(1^1\cdot 1!)}$	$=$	30
$(1,2,3)(4,5)$	$\frac{5!}{(3^1\cdot 1!)(2^1\cdot 1!)}$	$=$	20
$(1,2,3)(4)(5)$	$\frac{5!}{(3^1\cdot 1!)(1^2\cdot 2!)}$	$=$	20
$(1,2)(3,4)(5)$	$\frac{5!}{(2^2\cdot 2!)(1^1\cdot 1!)}$	$=$	15
$(1,2)(3)(4)(5)$	$\frac{5!}{(2^1\cdot 1!)(1^3\cdot 3!)}$	$=$	10
$(1)(2)(3)(4)(5)$	$\frac{5!}{1^5\cdot 5!}$	$=$	1

Sei nochmals erwähnt, daß unter normalen Umständen die Zykel der Länge 1 nicht notiert werden.

(4) Wir geben jeweils ein Beispiel. Für Ordnung 4 und 8 gibt es noch weitere (isomorphe) Beispiele.

(Ordnung 4) Sei

$$V_4 \;=\; \langle(1,2)(3,4),(1,3)(2,4)\rangle \;=\; \{\mathrm{id},\,(1,2)(3,4),\,(1,3)(2,4),\,(1,4)(2,3)\} \qquad \text{(die \textit{Kleinsche Vierergruppe})}\ .$$

Wir erhalten $\mathrm{N}_{\mathcal{S}_4}(V_4)=\mathcal{S}_4$ (die Gruppe ist Vereinigung zweier Konjugiertenklassen!), $\mathrm{C}_{\mathcal{S}_4}(V_4)=V_4$ (wegen V_4 abelsch ist hier $\supseteq$ klar), und $\mathrm{Z}(V_4)=V_4$ (wegen V_4 abelsch).

(Ordnung 8) Sei

$$D_8 \;=\; \langle(1,3),(1,2,3,4)\rangle \;=\; \{\mathrm{id},\,(1,2,3,4),\,(1,3)(2,4),\,(1,4,3,2),\,(1,3),\,(1,4)(2,3),\,(2,4),\,(1,2)(3,4)\}$$
(die *Diedergruppe* der Ordnung 8) .

Wir erhalten $\mathrm{N}_{\mathcal{S}_4}(D_8)=D_8$ (da z.B. $(1,2)$ die Gruppe D_8 nicht normalisiert, da also $D_8\le\mathrm{N}_{\mathcal{S}_4}(D_8)<\mathcal{S}_4$), $\mathrm{C}_{\mathcal{S}_4}(D_8)=\langle(1,3)(2,4)\rangle$ (da $\mathrm{C}_{\mathcal{S}_4}(D_8)\le\mathrm{N}_{\mathcal{S}_4}(D_8)$ und da ein Element eine Untergruppe zentralisiert genau dann, wenn es gewählte Erzeuger zentralisiert), sowie $\mathrm{Z}(D_8)=\mathrm{C}_{\mathcal{S}_4}(D_8)\cap D_8=\langle(1,3)(2,4)\rangle$.

(Ordnung 12) Sei

$$\begin{aligned}\mathcal{A}_4 \;&=\; \langle(1,2,3),(1,2,4)\rangle\\ &=\; \{\mathrm{id},\,(1,2)(3,4),\,(1,3)(2,4),\,(1,4)(2,3),\,(1,2,3),\,(1,2,4),\,(1,3,2),\,(1,3,4),\,(1,4,2),\,(1,4,3)\}\end{aligned}$$
(die *alternierende Gruppe* auf $[1,4]$)

Wir erhalten $\mathrm{N}_{\mathcal{S}_4}(\mathcal{A}_4)=\mathcal{S}_4$ (die Gruppe ist Vereinigung dreier Konjugiertenklassen!), $\mathrm{C}_{\mathcal{S}_4}(\mathcal{A}_4)=1$ (da ein Element eine Untergruppe zentralisiert genau dann, wenn es gewählte Erzeuger zentralisiert, und da etwa $(1,2,3)$ nur von $\langle(1,2,3)\rangle$ zentralisiert wird), und $\mathrm{Z}(\mathcal{A}_4)=\mathrm{C}_{\mathcal{S}_4}(\mathcal{A}_4)\cap 1=1$.

Aufgabe 6.

(1) Sei $g \in G$. Wir wollen zeigen, daß $c(g) : G \longrightarrow G$, $x \longmapsto {}^g x$, ein Automorphismus von G ist. Zunächst wird $(c(g))(xy) = {}^g xy = g^{-1}xyg = g^{-1}xgg^{-1}yg = {}^g x\, {}^g y = (c(g))(x)(c(g))(y)$ für $x,\, y \in G$, was zeigt, daß $c(g)$ ein Morphismus von Gruppen ist. Ferner ist $(c(g^{-1}) \circ c(g))(x) = {}^{g^{-1}}({}^g x) = g^{-1}gxgg^{-1} = x$, also $c(g^{-1}) \circ c(g) = \mathrm{id}_G$. Genauso folgt $c(g) \circ c(g^{-1}) = \mathrm{id}_G$. Mithin ist $c(g)$ invertierbar, und insgesamt also ein Automorphismus.

(2) Wir wollen zeigen, daß $c(gh) = c(g) \circ c(h)$ für $g,\, h \in G$. In der Tat erhalten wir bei $x \in G$

$$(c(gh))(x) \;=\; {}^{gh}x \;=\; ghxh^{-1}g^{-1} \;=\; {}^g({}^h x) \;=\; (c(g) \circ c(h))(x)\ .$$

(3) Wir wollen zeigen, daß $\mathrm{Kern}\, c = \mathrm{Z}(G)$. In der Tat ist

$$g \in \mathrm{Kern}\, c \iff c(g) \;=\; \mathrm{id}_G \iff {}^g x = x \text{ für alle } x \in G \iff g \in \mathrm{Z}(G)\ .$$

(4) Wir behaupten, daß $\mathrm{N}_{\mathrm{Aut}\, G}(\mathrm{Inn}\, G) = \mathrm{Aut}\, G$, i.e. daß für alle $\alpha \in \mathrm{Aut}\, G$ gilt, daß $\alpha \circ (\mathrm{Inn}\, G) \circ \alpha^{-1} = \mathrm{Inn}\, G$.

Zu $\subseteq$. Sei $\beta \in \mathrm{Inn}\, G$, i.e. sei ein $g \in G$ gegeben mit $\beta = c(g)$. Wir behaupten, daß $\alpha \circ c(g) \circ \alpha^{-1} = c(\alpha(g))$ ist, und so insbesondere $\alpha \circ c(g) \circ \alpha^{-1} \in \mathrm{Inn}\, G$ folgt. Tatsächlich wird für $x \in G$

$$(\alpha \circ c(g) \circ \alpha^{-1})(x) \;=\; \alpha(g\alpha^{-1}(x)g^{-1}) \;=\; \alpha(g)x\alpha(g)^{-1} \;=\; (c(\alpha(g)))(x)\ .$$

Zu $\supseteq$. Da auch $\alpha^{-1} \in \mathrm{Aut}\, G$, folgt mit dem eben Gezeigten, daß $\alpha^{-1} \circ (\mathrm{Inn}\, G) \circ \alpha \subseteq \mathrm{Inn}\, G$, und also $\mathrm{Inn}\, G \subseteq \alpha \circ (\mathrm{Inn}\, G) \circ \alpha^{-1}$.

(5, 6, 7) Zeigen wir zunächst die Injektivität, und zwar gleich für alle $\mathcal{S}_n$ mit $n \geq 3$.

Wir schreiben $[a, b] := \{z \in \mathbf{Z} \;:\; a \leq z \leq b\}$ für $a, b \in \mathbf{Z}$.

Allgemein gilt für einen Morphismus von Gruppen $K \xrightarrow{f} H$, daß er injektiv ist genau dann, wenn $\mathrm{Kern}\, f = \{1\} =: 1$. Denn ist er injektiv, so ist $|f^{-1}(1)| = 1$. Und umgekehrt, ist $\mathrm{Kern}\, f = 1$, und sind $g,\, g' \in G$ gegeben mit $f(g) = f(g')$, dann ist $f(gg'^{-1}) = f(g)f(g')^{-1} = 1$, und also $gg'^{-1} \in \mathrm{Kern}\, f = 1$, und somit $g = g'$.

Wir haben zu zeigen, daß $\mathrm{Z}(\mathcal{S}_n) = 1$. Sei $\sigma \in \mathcal{S}_n$, und sei $\sigma(i) = j$, mit $i,\, j \in [1, n]$, und $i \neq j$. Wir haben zu zeigen, daß σ nicht im Zentrum von $\mathcal{S}_n$ liegt. Sei $k \in [1, n] \smallsetminus \{i, j\}$, was wegen $n \geq 3$ gefunden werden kann. Es wird

$$({}^{(j,k)}\sigma)(i) \;=\; ((j, k) \circ \sigma \circ (j, k))(i) \;=\; (j, k)(\sigma(i)) \;=\; k \;\neq\; \sigma(i)\ ,$$

und somit ${}^{(j,k)}\sigma \neq \sigma$.

Zeigen wir nun die Surjektivität von c in den einzelnen Fällen.

Wir machen dazu Gebrauch von folgenden beiden Tatsachen. Ist G eine endliche Gruppe, $G \xrightarrow[\sim]{\alpha} G$ ein Automorphismus und $g \in G$, so haben g und $\alpha(g)$ dieselbe Ordnung, $\mathrm{o}(g) = \mathrm{o}(\alpha(g))$. Ferner sind die Konjugiertenklassen gleich lang, genauer, es gibt eine Bijektion

$$\begin{array}{ccc} {}^G g & \xrightarrow{\sim} & {}^G\alpha(x) \\ x & \longmapsto & \alpha(x)\ . \end{array}$$

(5) Fall $G = \mathcal{S}_3$. Es ist $\mathcal{S}_3 = \langle (1, 2), (1, 2, 3) \rangle$. Ein Automorphismus ist also durch die Bilder von $(1, 2)$ und von $(1, 2, 3)$ bestimmt. Mögliche Bilder von $(1, 2)$ sind, wegen Ordnung 2, aus $\{(1, 2), (1, 3), (2, 3)\}$. Mögliche Bilder von $(1, 2, 3)$ sind, wegen Ordnung 3, aus $\{(1, 2, 3), (1, 3, 2)\}$. Nun folgt aus

$$6 \;=\; |\,\mathrm{Inn}\, \mathcal{S}_3| \;\leq\; |\,\mathrm{Aut}\, \mathcal{S}_3| \;\leq\; 2 \cdot 3 \;=\; 6\ ,$$

daß $\mathrm{Inn}\, \mathcal{S}_3 = \mathrm{Aut}\, \mathcal{S}_3$.

(6) Fall $G = \mathcal{S}_4$. Es ist $\mathcal{S}_4 = \langle (1, 2), (1, 2, 3, 4) \rangle$.

Konjugiertenklassen der Ordnung 2 in $\mathcal{S}_4$ haben wir die von $(1, 2)$, welche 6 Elemente umfaßt, und die von $(1, 2)(3, 4)$, welche 3 Elemente umfaßt. Somit bildet ein Automorphismus das Element $(1, 2)$ auf ein Element von ${}^{\mathcal{S}_4}(1, 2)$ ab.

Konjugiertenklassen der Ordnung 4 in $\mathcal{S}_4$ haben wir die von $(1, 2, 3, 4)$, welche 6 Elemente umfaßt. Somit bildet ein Automorphismus das Element $(1, 2, 3, 4)$ auf ein Element von ${}^{\mathcal{S}_4}(1, 2, 3, 4)$ ab.

Damit haben wir maximal 36 Automorphismen. Da aber $|\,\mathrm{Inn}\, \mathcal{S}_4|$ ein Teiler von $|\,\mathrm{Aut}\, \mathcal{S}_4|$ ist, ist $\mathrm{Inn}\, \mathcal{S}_4 = \mathrm{Aut}\, \mathcal{S}_4$.

(7) Fall $G = \mathcal{S}_5$. Es ist $\mathcal{S}_5 = \langle (1,2), (1,2,3,4,5) \rangle$.

Konjugiertenklassen der Ordnung 2 in $\mathcal{S}_4$ haben wir die von $(1,2)$, welche 10 Elemente umfaßt, und die von $(1,2)(3,4)$, welche 15 Elemente umfaßt. Somit bildet ein Automorphismus das Element $(1,2)$ auf ein Element von ${}^{\mathcal{S}_4}(1,2)$ ab.

Konjugiertenklassen der Ordnung 5 in $\mathcal{S}_5$ haben wir die von $(1,2,3,4,5)$, welche 24 Elemente umfaßt. Somit bildet ein Automorphismus das Element $(1,2,3,4,5)$ auf ein Element von ${}^{\mathcal{S}_5}(1,2,3,4,5)$ ab.

An dieser Stelle wissen wir $|\operatorname{Aut}\mathcal{S}_5| \leq 240$. Wir müssen also noch gewisse Wahlen für die Bilder von $(1,2)$ und von $(1,2,3,4,5)$ ausschließen.

Sei $\alpha \in \operatorname{Aut}\mathcal{S}_5$, und sei $\alpha((1,2)) = (a,b)$ mit $a,\ b \in [1,5]$, $|\{a,b\}| = 2$, sowie $\alpha((1,2,3,4,5)) = (a,d,e,f,g)$ mit $d,\ e,\ f,\ g \in [1,5]$, $|\{d,e,f,g\}| = 4$. Es ist $b \in \{d,e,f,g\}$. Das liefert 4 Fälle, von denen wir nun ein paar ausschließen wollen.

Es ist ${}^{(1,2,3,4,5)^2}(1,2) = (3,4)$, welches mit $(1,2)$ vertauscht, und daher muß auch ${}^{\alpha((1,2,3,4,5))^2}\alpha((1,2))$ mit $\alpha((1,2))$ vertauschen. Nun ist aber

$$ {}^{\alpha((1,2,3,4,5))^2}\alpha((1,2)) \;=\; {}^{(a,e,g,d,f)}(a,b) \;=\; (e,h)\ , $$

mit noch zu spezifizierendem $h \in [1,5]$. Dieses Element (e,h) vertauscht nun mit $\alpha((1,2)) = (a,b)$ genau dann, wenn $\{a,b\} \cap \{e,h\} = \emptyset$. Dies schließt nun aus, daß $h \in \{a,b\}$, d.h. daß $b = f$. Ferner schließt es aus, daß $e \in \{a,b\}$, d.h. daß $b = e$. Bei beliebiger Wahl von (a,b), wofür wir 10 Möglichkeiten haben, verbleiben also noch $2 \cdot 3 \cdot 2 = 12$ Möglichkeiten für das Bild von $(1,2,3,4)$, wobei der erste Faktor 2 die beiden Möglichkeiten aufzählt, b in den Zykel einzusortieren, nämlich an dritter oder an vierter Stelle.

Also

$$ 120 \;=\; |\operatorname{Inn}\mathcal{S}_5| \;\leq\; |\operatorname{Aut}\mathcal{S}_5| \;\leq\; 10 \cdot 12 \;=\; 120\ , $$

und somit $\operatorname{Inn}\mathcal{S}_5 = \operatorname{Aut}\mathcal{S}_5$.

Und für $\mathcal{S}_6$? Und für $\mathcal{S}_n$ mit $n \geq 7$?

(8) Wir können etwa $G = C_3 = \langle a \rangle$ nehmen. Wegen $\mathrm{Z}(C_3) = C_3 \neq 1$ ist c nicht injektiv. Da $C_3 \xrightarrow[\sim]{\alpha} C_3,\ x \longmapsto x^2$ ein Automorphismus ist, welcher wegen C_3 abelsch nicht inner ist, ist c auch nicht surjektiv.

Aufgabe 7.

(1) Aussage ist falsch. Z.B. ist in $\mathcal{S}_3$ auf der einen Seite $|\langle (1,2), (2,3) \rangle| = 6$, aber auf der anderen Seite $|\langle (1,2) \rangle| \cdot |\langle (2,3) \rangle| = 4$, und 6 ist kein Teiler von 4.

(2) Aussage ist richtig. In der Tat ist ein Automorphismus einer endlichen Gruppe G eine spezielle Bijektion von G in sich, und solche Bijektionen gibt es nur endlich viele, viz. $|G|!$ Stück.

(3) Aussage ist richtig. Ist nämlich $g \in G$ ein Element, für welches ${}^{g}v = v$ für alle $v \in V$ gilt, so gilt dies a fortiori auch für alle $v \in U \leq V$.

(4) Aussage ist falsch. Z.B. ist in $\mathcal{S}_3$ für $U := \langle (1,2) \rangle \leq \mathcal{S}_3 =: V$ der Normalisator von U gleich U, und der Normalisator von V gleich V, und somit ist letzterer keiner Untergruppe von ersterem.

(5) Aussage ist falsch. Betrachte etwa den Morphismus p von $C_4 = \langle a \rangle$ auf $C_2 = \langle b \rangle$, welcher a^m auf b^m schickt für $m \in [0,3]$. Ein Morphismus i wie verlangt müßte also b entweder auf a oder aber auf a^3 schicken. Dies hätte aber in beiden Fällen zur Folge, daß b^2 von i auf $a^2 = a^6 \neq 1$ geschickt würde, was wegen $b^2 = 1$ nicht möglich ist.