F14T2A3 geg: Gruppe G

$\phi_h : G \to G,\ g \mapsto hgh^{-1}$ (für jedes $h \in G$)

$Inn(G) = \{\phi_h \mid h \in G\} \subseteq Aut(G)$

zu(a) bereits gezeigt: $Inn(G) \leq Aut(G)$

Nachweis der Normalteiler-Eigenschaft:

Sei $\sigma \in Aut(G)$ und $\tau \in Inn(G)$. z.zg.:

$\sigma \circ \tau \circ \sigma^{-1} \in Inn(G)$ $\tau \in Inn(G) \Rightarrow \exists h \in G$

mit $\tau = \phi_h$ Sei nun $g \in G$ vorgeg. Es gilt

$(\sigma \circ \tau \circ \sigma^{-1})(g) = \sigma(\tau(\sigma^{-1}(g))) =$

zu(i)

zu(ii)

zu(iii)

$\sigma(\phi_h(\sigma^{-1}(g))) = \sigma(h\sigma^{-1}(g)h^{-1}) =$

$\sigma(h)\sigma(\sigma^{-1}(g))\sigma(h^{-1}) = \sigma(h)g\sigma(h)^{-1} =$

$\phi_{\sigma(h)}(g)$ also: $\sigma \circ \tau \circ \sigma^{-1} = \phi_{\sigma(h)}$

$\Rightarrow \sigma \circ \tau \circ \sigma^{-1} \in Inn(G)$

zu (b) z.Zg: Die Abbildung $\phi: G \to Aut(G)$, $h \mapsto \phi_h$ induziert einen Isomorphismus $G/Z(G) \cong Inn(G)$

Damit der Homomorphiesatz den angeg. Isom. liefert, müssen wir überprüfen (i) ϕ ist ein Gruppenhom.

(ii) $im(\phi) = Inn(G)$ (iii) $ker(\phi) = Z(G)$

(Erinnerung: Zentrum von G $Z(G) = \{g \in G \mid \forall h \in G: gh = hg\}$)

zu (i) Seien $h, h' \in G$. z.Zg.: $\phi(hh') = \phi(h) \circ \phi(h')$

gleichbedeutend: $\phi_{hh'} = \phi_h \circ \phi_{h'}$ Sei $g \in G$.

$$\phi_{hh'}(g) = (hh')\, g\, (hh')^{-1} = hh' g (h')^{-1} h^{-1} =$$

$$= \phi_h(h' g (h')^{-1}) = \phi_h(\phi_{h'}(g)) = (\phi_h \circ \phi_{h'})(g).$$

Da g beliebig vorgeg. war, folgt daraus $\phi_{hh'} = \phi_h \circ \phi_{h'}$.

zu (ii) Für jedes $\sigma \in \mathrm{Aut}(G)$ gilt die Äquivalenz

$$\sigma \in \mathrm{im}(\phi) \iff \exists h \in G : \phi(h) = \sigma \iff \exists h \in G : \sigma = \phi_h$$

$$\iff \sigma \in \mathrm{Inn}(G)$$

zu (iii) Sei $h \in G$. Dann gilt die Äquivalenz

$h \in \ker(\phi) \Leftrightarrow \phi(h) = id_G \Leftrightarrow \phi_h = id_G \Leftrightarrow$

$\forall g \in G: \phi_h(g) = id_G(g) \Leftrightarrow \forall g \in G: hgh^{-1} = g$

$\Leftrightarrow \forall g \in G: hg = gh \Leftrightarrow g \in Z(G)$

Z4(c) Bestimmen Sie alle Automorphismen von $(\mathbb{Z}/7\mathbb{Z}, +)$ und zeigen Sie, dass es nur einen innere Automorphismus gibt.

Für $1 \leq a \leq 6$ ist $\partial_a: \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$, $\bar{b} \mapsto a \cdot \bar{b}$ ein Automorphismus, denn: Für alle $\bar{b}, \bar{c} \in \mathbb{Z}/7\mathbb{Z}$ gilt $\partial_a(\bar{b} + \bar{c}) = a \cdot (\bar{b} + \bar{c}) = a\bar{b} + a \cdot \bar{c} =$ $\partial_a(\bar{b}) + \partial_a(\bar{c})$, d.h. jedes ∂_a $(1 \leq a \leq 6)$ ist jeden-

falls ein Endomorphismus von $(\mathbb{Z}/7\mathbb{Z}, +)$
Jedes ∂_a ist injektiv, denn: $ggT(a, 7)$
$= 1 \Rightarrow a + 7\mathbb{Z} \in (\mathbb{Z}/7\mathbb{Z})^\times \Rightarrow$
$\exists b \in \mathbb{Z}, ggT(b, 7) = 1$ mit $(a + 7\mathbb{Z}) \cdot$
$(b + 7\mathbb{Z}) = 1$ Sei nun $\bar{c} \in \ker(\partial_a)$,
$\bar{c} = c + 7\mathbb{Z}$ mit $c \in \mathbb{Z}, ggT(7, c) = 1$
$\rightarrow \partial_a(\bar{c}) = \bar{0} \Rightarrow a(c + 7\mathbb{Z}) =$
$0 + 7\mathbb{Z} \Rightarrow ac + 7\mathbb{Z} = 0 + 7\mathbb{Z} \Rightarrow$
$(a + 7\mathbb{Z}) \cdot (c + 7\mathbb{Z}) = 0 + 7\mathbb{Z} \Rightarrow$
$c + 7\mathbb{Z} = (1 + 7\mathbb{Z}) \cdot (c + 7\mathbb{Z}) =$
$(b + 7\mathbb{Z}) \cdot (a + 7\mathbb{Z}) \cdot (c + 7\mathbb{Z}) =$
$(b + 7\mathbb{Z}) \cdot 0 + 7\mathbb{Z} = 0 + 7\mathbb{Z}$

Da $\mathbb{Z}/7\mathbb{Z}$ eine endliche Menge ist, folgt aus der Injektivität von σ_a auch die Surjektivität, insg. also $\sigma_a \in \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$

noch z.zg.:

(1) Es gibt keine weiteren Automorphismen von $(\mathbb{Z}/7\mathbb{Z}, +)$

(2) Nur eines der σ_a $(1 \leq a \leq 6)$ ist ein innerer Automorphismus.

<u>zu (1)</u> Sei $\sigma \in \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$

$\sigma(1+7\mathbb{Z}) \in \mathbb{Z}/7\mathbb{Z} \Rightarrow \exists a \in \{0, 1, \dots, 6\}$ mit $\sigma(1+7\mathbb{Z}) = a + 7\mathbb{Z}$. Dabei ist $a = 0$ ausgeschlossen, da sonst $1+7\mathbb{Z} \in \ker(\sigma)$, im Widerspruch zu $\ker(\sigma) = \{0+7\mathbb{Z}\}$ auf-

gew

Es g

$= \sigma($

folgt

<u>zu (2)</u>

$\Rightarrow 7 b$

$a + 7\mathbb{Z}$

$(b + 7\mathbb{Z})$

$(b + 1 + ($

Tatsäch

denn es

$= 1 + 7\mathbb{Z}$

grund der Injektivität von σ.

Es gilt $\sigma_a(1+7\mathbb{Z}) = a\cdot(1+7\mathbb{Z}) = a+7\mathbb{Z}$
$= \sigma(1+7\mathbb{Z})$. Wegen $\mathbb{Z}/7\mathbb{Z} = \langle 1+7\mathbb{Z}\rangle$
folgt daraus $\sigma = \sigma_a$.

zu (2) Sei $a \in \{1,\dots,6\}$. Ang., $\sigma_a \in \mathrm{Inn}(\mathbb{Z}/7\mathbb{Z})$.
$\Rightarrow 7 \in b \in \mathbb{Z}$ mit $\sigma_a = \phi_{b+7\mathbb{Z}} \Rightarrow$
$a+7\mathbb{Z} = \sigma_a(1+7\mathbb{Z}) = \phi_{b+7\mathbb{Z}}(1+7\mathbb{Z}) =$
$(b+7\mathbb{Z}) + (1+7\mathbb{Z}) + (-(b+7\mathbb{Z})) =$
$(b+1+(-b)) + 7\mathbb{Z} = 1+7\mathbb{Z} \Rightarrow a = 1$
Tatsächlich ist σ_1 ein innerer Automorphismus,
denn es gilt z.B. $\sigma_1 = \phi_{0+7\mathbb{Z}}$ wegen $\sigma_1(1+7\mathbb{Z})$
$= 1+7\mathbb{Z} = (0+7\mathbb{Z}) + (1+7\mathbb{Z}) + (-(0+7\mathbb{Z})) = \phi_{0+7\mathbb{Z}}(1+7\mathbb{Z})$ □

Der Korrespondenzsatz für Gruppen

Satz

Sei G eine Gruppe, N ein Normalteiler, $\bar{G} = G/N$ und $\pi_N : G \to \bar{G}$ der kanonische Epimorphismus. Ferner sei $\bar{\mathcal{G}}$ die Menge der Untergruppen von $\bar{G}$ und $\mathcal{G}_N$ die Menge der Untergruppen U von G mit $U \supseteq N$. Dann sind die beiden Abbildungen

$$\mathcal{G}_N \to \bar{\mathcal{G}} \ , \ U \mapsto \pi_N(U) \quad \text{und} \quad \bar{\mathcal{G}} \to \mathcal{G}_N \ , \ \bar{U} \mapsto \pi_N^{-1}(\bar{U})$$

bijektiv und zueinander invers. Außerdem gilt:

- Für $U, V \in \mathcal{G}_N$ gilt $U \subseteq V$ genau dann, wenn $\pi_N(U) \subseteq \pi_N(V)$ erfüllt ist.
- Genau dann ist $U \in \mathcal{G}_N$ ein Normalteiler von G, wenn $\pi_N(U)$ ein Normalteiler von $\bar{G}$ ist.
- Ist $U \in \mathcal{G}_N$ von endlichem Index in G und $\bar{U} = \pi_N(U)$, dann gilt $(G : U) = (\bar{G} : \bar{U})$.

F23T2A2

Sei G eine Gruppe der Ordnung 30, U_3 eine 3- und U_5 eine 5-Sylowgruppe.

(a) Zeigen Sie: $U_3 \trianglelefteq G$ oder $U_5 \trianglelefteq G$

$|G| = 2^1 \cdot 3^1 \cdot 5^1 \Rightarrow$ Die 3-Sylowgr. sind genau die Untergr. der Ordnung 3, und die 5-Sylowgruppen sind genau die Untergr. der Ordnung 5 von G. Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgr. von G. Aufgrund des 2. Sylowsatzes genügt es z.zg.

$\nu_3 = 1$ oder $\nu_5 = 1$

3. Sylowsatz $\Rightarrow \nu_5 \mid 6 \Rightarrow \nu_5 \in \{1, 2, 3, 6\}$

außerdem $\nu_5 \equiv 1 \bmod 5$ $\overset{(*)}{\Rightarrow}$ $\nu_5 \in \{1, 6\}$

ebenso: $\nu_3 \mid 10 \Rightarrow \nu_3 \in \{1, 2, 5, 10\}$,

außerdem $\nu_3 \equiv 1 \bmod 3$, $2 \not\equiv 1 \bmod 3$, $5 \equiv 2 \not\equiv 1 \bmod 3 \Rightarrow \nu_3 \in \{1, 10\}$ [(*) und $2, 3 \not\equiv 1 \bmod 5$]

Ang. $\nu_5 \neq 1$ und $\nu_3 \neq 1$. $\Rightarrow \nu_5 = 6$ und $\nu_3 = 10$

Allgemein gilt: Ist G eine endliche Gruppe und p eine Primzahl, dann ist die Anzahl der Elemente der Ordnung p genau $(p-1)$-mal so groß wie die Anzahl der Untergr. der Ordn. p (denn: ... siehe letzte Woche) Aus $\nu_5 = 6$ folgt also, dass G $6 \cdot 4 = 24$ Elemente der Ordnung 5 enthält, und aus $\nu_3 = 10$ entsprechend, dass es $10 \cdot 2 = 20$ Ele-

$\{1, 2, 3, 6\}$

$\in \{1, 6\}$

$5, 10\}$,

od 3, $5 \equiv 2$

und $2, 3 \not\equiv 1 \bmod 5$]

und $\nu_3 = 10$

ch Gruppe und

nzahl der Elemente

so groß wie die

(denn: ... siehe

gt also, dass G

5 enthält, und

es $10 \cdot 2 = 20$ Ele-

mente der Ordnung 3 in G gibt.

aber: $24 + 20 = 44 > |G|$ ↯

zu (b) Zeigen Sie: Ist U_3 Normalteiler von G, dann hat G/U_3 eine Untergruppe vom Index 2. Ebenso hat G/U_5 im Fall G/U_5 eine Untergruppe von Index 2.

Setze zunächst $U_3 \trianglelefteq G$ voraus. Dann gilt

$$|G/U_3| = (G : U_3) = \frac{|G|}{|U_3|} = \frac{30}{3} = 10.$$

5 ist Primteiler von $|G/U_3|$, Lemma von Cauchy $\Rightarrow \exists\, \bar{g} \in G/U_3$ mit $\operatorname{ord}(\bar{g}) = 5 \Rightarrow \bar{U} = \langle \bar{g} \rangle$ ist Untergruppe von G/U_3 von Ordnung 5 und $(G/U_3 : \bar{U}) = \frac{|G/U_3|}{|\bar{U}|} = \frac{10}{5} = 2$

Im Fall $U_5 \trianglelefteq G$ läuft die Argumentation analog (Anstatt U_3 als Übung).

(c) Zeigen Sie, dass G eine Untergruppe U_{15} von Ordnung 15 besitzt.

Nach Teil (a) gilt $U_3 \trianglelefteq G$ oder $U_5 \trianglelefteq G$.

1. Fall: $U_3 \trianglelefteq G$.

Nach Teil (b) besitzt G/U_3 eine Untergruppe $\bar{U}$ vom Index 2. Sei $\pi_3 : G \to G/U_3$ der kanonische Epimorphismus. Laut Korrespondenzsatz ist $U_{15} = \pi_3^{-1}(\bar{U})$ in G eine Untergr. mit $(G : U_{15}) = 2$. Es gilt $|U_{15}| = \frac{|G|}{(G : U_{15})}$

(c) Zeigen Sie, dass es in G nur eine 3- und nur eine 5-Sylowgruppe gibt.

$= \frac{30}{2} = 15$. 2. Fall: $U_5 \not\trianglelefteq G$ (läuft analog. Übung)

(d) Zeigen Sie, dass alle 3- und alle 5-Sylowgruppen in U_{15} enthalten sind.

Führe das Argument hier nur für $p=3$ aus (Für $p=5$ läuft es wieder analog.)

Da 3 ein Primteiler von $|U_{15}| = 15$ ist, gibt es in U_{15} nach dem Lemma von Cauchy ein Element der Ordnung 3, und damit auch eine Untergr. $P' \leq U_{15}$ mit $|P'| = 3$. Dieses P' ist dann auch eine 3-Sylowg. von G. Sei nun P' eine beliebige 3-Sylowgr. von G. z.zg: $P' \subseteq U_{15}$ 2 Sylowsatz $\Rightarrow \exists g \in G$ mit $P' = gPg^{-1}$. $(G : U_{15}) = \frac{|G|}{|U_{15}|} = 2 \Rightarrow U_{15} \trianglelefteq G$

$\Rightarrow gU_{15}g^{-1} = U_{15}$ $\quad P \leq U_{15} \Rightarrow P' = gPg^{-1} \in$

$gU_{15}g^{-1} = U_{15}$

(e) Zeigen Sie, dass es in G nur eine 3- und nur eine 5-Sylowgruppe gibt.

Jede 3- und jede 5-Sylowgruppe liegt nach Teil (d) in U_{15}. Wegen $|U_{15}| = 15$ ist U_{15} lt. Vl. eine zyklische Gruppe, besitzt also nur eine Untergruppe der Ordnung 3, und nur eine Untergr. der Ordnung 5. Alle 3- bzw. 5-Sylowgr. stimmen also mit dieser eind. bestimmten Untergr. der Ordnung 3 bzw. 5 überein, d.h. es gilt $r_3 = 1$ und $r_5 = 1$. $\square$

Hinweis:

Teil (c) von Aufgabe H24T1A2 liefert ein Anwendungsbeispiel für den Korrespondenzsatz. Verwendet werden muss hierzu das Ergebnis von Teil (a), aber das Ergebnis von Teil (b) wird für Teil (c) nicht benötigt. Teil (b) verwendet die Theorie der Gruppenoperationen und ist nicht auch nicht ganz leicht. Eventuell ist es ratsam, mit der Bearbeitung von Teil (b) bis Ende nächster Woche zu warten.