Algebra - Blatt 6 Lösungsvorschlag

A1 <u>Beh:</u> $\mathbb{Z}/15\mathbb{Z}$ ist die einzige Gruppe der Ordnung 15 (bis auf Isomorphie).

<u>Bew:</u> Sei G eine Gruppe mit $\#G = 15 = 3\cdot 5$.
Es bezeichne s_3 die Anzahl der 3-Sylowgr. und s_5 die Anzahl der 5-Sylowgr. von G.
Dann ist $s_5 \equiv 1 \mod 5$, $s_5 | 3$,
also $s_5 = 1$ und $s_3 \equiv 1 \mod 3$, $s_3 | 5$,
also $s_3 = 1$. Sei $A \leq G$ die 3-Sylowgr. und $B \leq G$ die 5-Sylowgr. Sei $g \in G \setminus (A \cup B)$.
(Das ex., da $\#(A\cup B) \leq \#A + \#B - 1 = 7 < 15 = \#G$.)

Sei $H := \langle g \rangle$. Dann ist $\#H = \operatorname{ord}(g)$ ein Teiler von 15; wegen $g \notin A\cup B$ ist $H \neq A$, $H \neq B$, also $\#H \neq 3$, $\#H \neq 5$.
Außerdem $\#H \neq 1$ (denn $1 \in A \cup B \not\ni g$),
also $H = G$, d.h. G ist zyklisch. Also $G \cong \mathbb{Z}/15\mathbb{Z}$.

A2 $(a,b)\cdot(a',b') := (a\lambda_b(a'), bb')$ für $(a,b), (a',b') \in G_1 \times G_2$

a) $G_1 \times G_2 \neq \emptyset$ ✓

"$\cdot$" <u>assoziativ:</u> $(a,b)\cdot((a',b')\cdot(a'',b''))$

$= (a,b)\cdot(a'\lambda_{b'}(a''), b'b'')$

$= (a\lambda_b(a'\lambda_{b'}(a'')), b(b'b''))$

$= (a\lambda_b(a')\lambda_b\lambda_{b'}(a''), (bb')b'')$

$b \mapsto \lambda_b$ ist Homom.

$\overset{\downarrow}{=} (a\lambda_b(a')\lambda_{bb'}(a''), (bb')b'')$

$= (a\lambda_b(a'), bb')\cdot(a'',b'')$

$= ((a,b)\cdot(a',b'))\cdot(a'',b'')$ ✓

$(1,1)$ ist <u>Neutralelement</u>: $(1,1)\cdot(a,b) = (1\cdot\lambda_1(a), 1b)$
$= (1a, 1b) = (a,b)$
und $(a,b)\cdot(1,1) = (a\lambda_b(1), b1) = (a1, b1)$
$= (a,b)$. ✓

$(\lambda_{b^{-1}}(a^{-1}), b^{-1})$ ist zu (a,b) <u>Inverses</u>:

$(a,b)\cdot(\lambda_{b^{-1}}(a^{-1}), b^{-1}) = (a\lambda_b(\lambda_{b^{-1}}(a^{-1})), bb^{-1}) = (a\lambda_{bb^{-1}}(a^{-1}), 1)$
$= (aa^{-1}, 1) = (1,1)$

und

$(\lambda_{b^{-1}}(a^{-1}), b^{-1})\cdot(a,b) = (\lambda_{b^{-1}}(a^{-1})\lambda_{b^{-1}}(a), b^{-1}b)$
$= (\lambda_{b^{-1}}(a^{-1}a), 1) = (\lambda_{b^{-1}}(1), 1) = (1,1)$ ✓

b) $G_1 \to G_1 \rtimes_\lambda G_2$, $a \mapsto (a,1)$:

~~Zz ist~~ $(a,1)\cdot(a',1) = (aa',1)$.

Es ist $(a,1)\cdot(a',1) = (a\lambda_1(a'), 1\cdot 1) = (aa',1)$ ✓

$G_2 \to G_1 \rtimes_\lambda G_2$, $b \mapsto (1,b)$:

analog: $(1,b)\cdot(1,b') = (1\cdot\underbrace{\lambda_b(1)}_{=1}, bb') = (1,bb')$ ✓

$\mathrm{im}(G_1 \to G_1 \rtimes_\lambda G_2) \trianglelefteq G_1 \rtimes_\lambda G_2$:

Seien $(a,1) \in G_1 \times \{1\} = \mathrm{im}(G_1 \to G_1 \rtimes_\lambda G_2)$ (d.h. $a \in G_1$)
und $(g,h) \in G_1 \rtimes_\lambda G_2$ beliebig.
Nach (a) ist $(g,h)^{-1} = (\lambda_{h^{-1}}(g^{-1}), h^{-1})$, also

$$(g,h)^{-1}\cdot(a,1)\cdot(g,h) = (\lambda_{h^{-1}}(g^{-1}), h^{-1})\cdot(a,1)\cdot(g,h)$$
$$= (\lambda_{h^{-1}}(g^{-1})\,\lambda_{h^{-1}}(a), h^{-1}1)\cdot(g,h)$$
$$= (\lambda_{h^{-1}}(g^{-1})\,\lambda_{h^{-1}}(a)\,\lambda_{h^{-1}}(g), h^{-1}h)$$
$$= (\lambda_{h^{-1}}(g^{-1}ag), 1) \in G_1 \times \{1\},$$

also ist $G_1 \times \{1\} \trianglelefteq G_1 \rtimes_\lambda G_2$.

Bem: Das sieht man auch einfacher ohne viel Rechnung: $(g,h)^{-1}(a,1)\cdot(g,h) =$

$$(*, h^{-1})\cdot(*,1)\cdot(*,h) = (*,h^{-1})\cdot(*,h) = (*, h^{-1}h) = (*,1) \in G_1 \times \{1\}$$

c) Betrachte $\lambda: H \to \mathrm{Aut}(N)$, $b \mapsto \varphi_b$ wobei

$\varphi_b : N \to N$, $a \mapsto bab^{-1}$ d.h. λ ist die Konjugationsoperation von H auf N.

Beh: $\Psi: N \rtimes_\lambda H \to G$, $(a,b) \mapsto ab$ ist ein Isomorphismus.

Bew: Bijektivität ist klar, da jedes Element von G sich eindeutig in der Form ab mit $a \in N$, $b \in H$ schreiben lässt.
Außerdem ist

$$\Psi((a,b)\cdot(a',b')) = \Psi(a\lambda_b(a'), bb') = \Psi(aba'b^{-1}, bb') = aba'b' = \Psi(a,b)\Psi(a',b')$$

d.h. Ψ ein Homom.

d) Sei G eine Gruppe mit $\#G = p \cdot q$, p, q zwei verschiedene Primzahlen.

oE sei $p > q$. Dann gilt für s_p = Anzahl der p-Sylowgr. von G und s_q = Anz. der q-Sylowgr. von G, dass $s_p \equiv 1 \mod p$ und $s_p | q$,

also $s_p = 1$. ($s_p = q$ ist ausgeschlossen, da $q \not\equiv 1 \pmod p$)

Sei also $P \leq G$ die p-Sylowgr., diese ist dann ein Normalteiler. (Da gPg^{-1} wieder eine p-Sylowgr. ist (für jedes $g \in G$), also $gPg^{-1} = P$.)

Sei Q eine beliebige q-Sylowgr. von G.

Dann ist $\#P = p$, $\#Q = q$; also gilt: $g \in P \cap Q \Rightarrow \mathrm{ord}(g) | p$ und $\mathrm{ord}(g) | q \Rightarrow \mathrm{ord}(g) = 1 \Rightarrow g = 1$.

D.h. $P \cap Q = \{1\}$. Seien nun $a, a' \in P$, $b, b' \in Q$ mit $ab = a'b'$. Wir zeigen $a = a'$ und $b = b'$, d.h. die Darstellung von Elementen von G in dieser Form ist eindeutig. Daraus folgern wir dann die Beh.

Zur Eindeutigkeit: $ab = a'b' \Rightarrow \underbrace{a'^{-1}a}_{\in P} = \underbrace{b'b^{-1}}_{\in Q}$,

also $a'^{-1}a = b'b^{-1} = 1$, d.h. $a = a'$ und $b = b'$.

Zur Existenz: Betrachte nun $\{ab \mid a \in P, b \in Q\} =: M$

Es ist $M \subseteq G$ mit $\#M \underset{\text{Eindeutigkeit}}{=} \#P \cdot \#Q = p \cdot q \underset{\text{Voraussetzung}}{=} \#G$,

also $M = G$.

Wir haben also gesehen: $P \trianglelefteq G$, $Q \leq G$, jedes Element von G lässt sich eindeutig als $a \cdot b$ schreiben mit $a \in P$, $b \in Q$.

Damit sind die Voraussetzungen in A2(c) erfüllt, d.h. $G \cong P \rtimes_\lambda Q$ für geeignetes λ.

Weiter sind P, Q Gruppen mit Primzahlordnung, also zyklisch (jedes Element $\neq 1$ hat Ordnung $\#P$ bzw. $\#Q$, d.h. ist ein Erzeuger), d.h.

$P \cong \mathbb{Z}/p\mathbb{Z}$, $Q \cong \mathbb{Z}/q\mathbb{Z}$

A3 (a) $g_1 = id$ und $g_2 : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$

$$x + p\mathbb{Z} \longmapsto -x + p\mathbb{Z}$$

sind Automorphismen von $\mathbb{Z}/p\mathbb{Z}$ mit $g_i^2 = id$.

Sei nun $g \in Aut(\mathbb{Z}/p\mathbb{Z})$ mit $g^2 = id$ beliebig. Setze $\bar{k} := g(\bar{1})$. Dann ist $\bar{k}^2 = g(\bar{1}) \cdot \bar{k}$

$$= g(\underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{k \text{ mal}}) = g(\bar{k}) = g^2(\bar{1}) = id(\bar{1}) = \bar{1}.$$

Dies ($\bar{k}^2 = \bar{1}$) ist eine Gleichg in $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ und hat dort die Lösungen $\bar{k} = \bar{1}$ und $\bar{k} = -\bar{1}$.

Also ist $g(\bar{1}) = \bar{1}$ oder $g(\bar{1}) = -\bar{1}$.

Für $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ beliebig $(x \in \mathbb{N})$ folgt nun

$$g(\bar{x}) = g(\underbrace{\bar{1} + \dots + \bar{1}}_{x \text{ mal}}) = \underbrace{g(\bar{1}) + \dots + g(\bar{1})}_{x \text{ mal}} = \begin{cases} \bar{1} + \dots + \bar{1} \\ -\bar{1} + \dots + (-\bar{1}) \end{cases}$$

$$= \begin{cases} \bar{x} & \text{falls } g(\bar{1}) = \bar{1} \\ -\bar{x} & \text{falls } g(\bar{1}) = -\bar{1} \end{cases}$$

Also ist $g = g_1$ oder $g = g_2$.

b) $f_1 : \bar{0} \longmapsto id$ und $f_2 : \bar{0} \longmapsto id$

$\bar{1} \longmapsto id$ $\quad$ $\bar{1} \longmapsto g_2 = -id$

sind Gruppenhomomorphismen von $\mathbb{Z}/2\mathbb{Z}$ nach $Aut(\mathbb{Z}/p)$

Sei nun $f : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/p\mathbb{Z})$ ein beliebiger Gruppenhom. Dann ist $f(\underset{\text{Neutralelement von } \mathbb{Z}/2\mathbb{Z}}{\bar{0}}) = id$ ← Neutralelement von $Aut(\mathbb{Z}/p\mathbb{Z})$

und $f(\bar{1}) \in Aut(\mathbb{Z}/p\mathbb{Z})$ mit $f(\bar{1})^2 = f(\bar{1} + \bar{1}) = f(\bar{0}) = id$

also $f(\bar{1}) = g_1$ oder $f(\bar{1}) = g_2$ nach (a), d.h. $f = f_1$ oder $f = f_2$.

---

c) Nach A2(d) mit $q = 2$ ist $G \cong \mathbb{Z}/p \rtimes_\lambda \mathbb{Z}/2$ für einen geeigneten Gruppenhomomorphismus $\lambda : \mathbb{Z}/2 \longrightarrow Aut(\mathbb{Z}/p)$. Nach (b) gibt es genau zwei Möglichkeiten dieses λ zu wählen.

$\lambda = f_1$ ergibt $G \overset{\circledast}{\cong} \mathbb{Z}/p \times \mathbb{Z}/2 \cong \mathbb{Z}/2p$ und

$\lambda = f_2$ ergibt $G \cong D_p$ nach Definition von D_p.

⊛ Nachrechnen: $(\bar{x}, \bar{y}) \cdot (\bar{x}', \bar{y}') = (\bar{x} + \underbrace{f_1(\bar{y})}_{= id}(\bar{x}'), \bar{y} + \bar{y}')$

$= (\bar{x} + \bar{x}', \bar{y} + \bar{y}')$

A4 a) $a + 0\cdot a \overset{\text{1 NE bzgl} \cdot}{=} 1\cdot a + 0\cdot a \overset{\text{Distributiv}}{=} (1+0)\cdot a$

$\underset{\text{0 NE bzgl +}}{=} 1\cdot a \underset{\text{1 NE bzgl} \cdot}{=} a$, d.h. $a + 0\cdot a = a$.

Also $\underbrace{\underbrace{-a+a}_{=0} + 0\cdot a} = -a + a \overset{\text{$-a$ invers zu a bzgl +}}{=} 0$

$= 0\cdot a$ d.h. $0\cdot a = 0$.

b) Ist $0 = 1$, so gilt

$0 \underset{(a)}{=} 0\cdot a = 1\cdot a \underset{\text{1 NE bzgl} \cdot}{=} a$

für jedes $a \in R$, d.h. $R = \{0\}$.