Übungsblatt № 3

Aufgabe 3.1: Untergruppenverbände und Homomorphismen

Finden Sie Gruppen $(G, \circ)$ und $(H, *)$ sowie einen Gruppenhomomorphismus $f\colon G \to H$ derart, dass es Untergruppen $U_1, U_2 \leq G$ und $U_1', U_2' \leq H$, sodass f das folgende Abbildungsverhalten induziert

$$\begin{tikzcd}
G \arrow[r, "f"] & H \\
U_3 \arrow[r, "\nexists"] & U_2' \arrow[dl] \\
U_2 \arrow[dr, shift left] & \\
U_1 \arrow[r] & U_1' \arrow[ul, shift left]
\end{tikzcd}$$

Sei f der triviale Homomorphismus $f(x) = 1_H$ für $x \in G$. Sei $U_2' \leq H$ eine nicht-triviale Untergruppe, also $U_2' \neq \{1_H\}$. Dann $\exists y \in U_2' \setminus \{1_H\}\colon \ \nexists x \in G\colon f(x) = y$. Es gibt also keine Untergruppe $U_3 \leq G$, sodass $f[U_3] = U_2'$, da $f[U_3] = \{1_H\}$. Wir brauchen also noch $U_1, U_2 \leq G$ und $U_1' \leq H$, sodass das Abbildungsverhalten gegeben ist. Wir wählen $U_1' = \{1_H\}$, dann folgt für alle Untergruppen $U_1 \leq G\colon f[U_1] = \{1_H\} = U_1'$, und $f[U_2] = \{1_H\} = U_1'$. U_1 kann also eine beliebige Untergruppe von G sein. Zuletzt U_2:

$$\begin{aligned}
f^{-1}[U_2'] &= \{x \in G\colon f(x) \in U_2'\} = G \\
f^{-1}[U_1'] &= \{x \in G\colon f(x) = 1_H\} = G
\end{aligned}$$

Also folgt $U_2 = G$.

$$\begin{tikzcd}
G \arrow[r, "f"] & H \\
U_3 \arrow[r, "\nexists"] & H \arrow[dl] \\
G \arrow[dr, shift left] & \\
U_1 \arrow[r] & \{1_H\} \arrow[ul, shift left]
\end{tikzcd}$$

Beispielsweise betrachten wir $(\mathbb{Z}, +) \xrightarrow{f} (\mathbb{Z}/n\mathbb{Z}, +)$ mit $f(z) = [0]_n$ für $z \in \mathbb{Z}$. Als U_2' wählen wir einfach $\mathbb{Z}/n\mathbb{Z}$ und $U_1' = \{[0]_n\}$. Weiters seien $U_2 = \mathbb{Z}$ und $U_1 = 2\mathbb{Z}$.

Aufgabe 3.2: Mehr zum Komplexprodukt

Sei $(G, \circ)$ eine Gruppe und $U, V \leq G$. Zeigen Sie:

a) Die Menge UV ist genau dann eine Untergruppe von G, wenn $UV = VU$ gilt.

b) Ist U ein Normalteiler von G, so gilt $\langle U \cup V \rangle = UV = VU$

c) Sind U und V endlich, so gilt

$$|UV| = \frac{|U| \cdot |V|}{|U \cap V|}$$

Zu a):

$\Rightarrow$: Sei $UV \leq G$, es gilt also $1 \in UV$ und $\forall u, v \in UV : uv^{-1} \in UV$. Da UV eine Untergruppe ist, gilt $(uv)^{-1} \in UV$. Da U und V Untergruppen sind, gilt $1 \in U, V$, ergo insbesondere $\forall u \in U : u1 \in UV$ und $\forall v \in V : 1v \in UV$, ergo $U \subseteq UV$ und $V \subseteq UV$. insbesondere gilt also $\forall u \in U : u^{-1} \in UV$ bzw. $\forall v \in V : v^{-1} \in UV$. Somit existieren $u' \in U$ und $v' \in V$ mit

$$(uv)^{-1} = v^{-1}u^{-1} = u'v' \Leftrightarrow 1 = uvu'v' \Leftrightarrow (v')^{-1}(u')^{-1} = uv$$

Da $(v')^{-1} \in V$ und $(u')^{-1} \in V$ ist $(v')^{-1}(u')^{-1} \in VU$, somit also $uv \in VU$. Ergo $UV \subseteq VU$.

$\Leftarrow$: Sei $UV = VU$. Wir wollen zeigen, dass $ab^{-1} \in UV$. Seien $a, b \in UV$ mit $a = u_1v_1$ und $b = u_2v_2$:

$$\begin{aligned}
&ab^{-1} = (u_1v_1)(u_2v_2)^{-1} = (u_1v_1)(v_2^{-1}u_2^{-1}) = u_1(v_1v_2^{-1})u_2^{-1} \\
&\Rightarrow \exists v_3 \in V, u_3 \in U : u_1(v_1v_2^{-1}) = v_3u_3 \\
&\Rightarrow ab^{-1} = v_3 \underbrace{u_3u_2^{-1}}_{\in U} \in VU
\end{aligned}$$

1 ist trivialerweise in UV, da $1 \in U$ und $1 \in V$.

Zu b):

$$UV = \bigcup_{v \in V} Uv = \bigcup_{v \in V} vU = VU$$

Somit ist UV eine Untergruppe. U und V sind Untergruppen, daher ist $U \subseteq UV$ und $V \subseteq UV$, da $U = U1$ und $V = 1V$, womit auch $U \cup V \subseteq UV$. Da UV eine Untergruppe ist, kommt UV auch im Schnitt für $\langle U \cup V \rangle$ vor, womit $\langle U \cup V \rangle \subseteq UV$.

Zu $\supseteq$.

$$U, V \subseteq \langle U \cup V \rangle \Rightarrow \forall u \in U, v \in V : uv \in \langle U \cup V \rangle$$

Sei nun $x \in UV$, dann $\exists u \in U, v \in V$, sodass $x = uv$. Allerdings gilt $x = uv \in \langle U \cup V \rangle$. Damit haben wir $UV \subseteq \langle U \cup V \rangle$ und $\langle U \cup V \rangle \subseteq UV$, ergo $\langle U \cup V \rangle = UV = VU$.

Zu c): Wir zeigen zuerst, dass $U \cap V \leq U, V$. Es gilt natürlich $1 \in U \cap V$, da $1 \in U$ und $1 \in V$. Seien nun $a, b \in U \cap V$, dann gilt $ab \in U$ und $ab \in V$, daher auch $ab \in U \cap V$.

Wir wollen herausfinden, wie viele Linksnebenklassen es von $U \cap V$ gibt. Nach dem Satz von Lagrange

$$[U : U \cap V] = \frac{|U|}{|U \cap V|}$$

Somit ist U genau die disjunkte Vereinigung von $[U : U \cap V]$ Linksnebenklassen von $U \cap V$

$$\begin{aligned}
&U = \biguplus_{a \in \mathcal{R}} a(U \cap V) \Rightarrow UV = \left(\biguplus_{a \in \mathcal{R}} a(U \cap V) \right) V = \biguplus_{a \in \mathcal{R}} a(U \cap V)V = \biguplus_{a \in \mathcal{R}} aUV \\
&\Rightarrow |UV| = [U : U \cap V] \cdot |V| = \frac{|U| \cdot |V|}{|U \cap V|}
\end{aligned}$$

Wobei $\mathcal{R}$ ein geeignetes Repräsentantensystem für die Linksnebenklassen von $U \cap V$ ist.

Aufgabe 3.3: Einige Automorphismengruppen

Bestimmen Sie zu jeder der folgenden Gruppen jeweils eine „bekannte“ Gruppe, zu welcher diese isomorph ist:

a) $\mathrm{Aut}(C_2)$
b) $\mathrm{Aut}(C_4)$
c) $\mathrm{Aut}(C_2 \times C_2)$

Wir erinnern uns, dass $C_n = \{0, \ldots, n-1\}$ mit der folgenden inneren Verknüpfung:

$$(a, b) \mapsto \begin{cases} a+b & a+b < n \\ a+b-n & a+b \geq n \end{cases}$$

Wir wollen uns überlegen, wie Funktionen $f \in \mathrm{Aut}(C_2)$ „aussehen“. Damit $f \in \mathrm{Aut}(C_n)$, muss gelten, dass f ein Isomorphismus ist, also eine Funktion $g \in \mathrm{End}(C_2)$ existiert, sodass $f \circ g = \mathrm{id} = g \circ f$. Somit muss f eine bijektive Funktion auf C_n sein. Damit kommen aber nur Permutationen in Frage, welche genau die bijektiven Funktionen auf einer n-elementigen Menge darstellen. Wir haben jedoch die Einschränkung auf $f(0) = 0$, womit wir $n-1$ Elemente permutieren wollen. Daraus folgt $\mathrm{Aut}(C_2) \simeq \mathfrak{S}_1$ und $\mathrm{Aut}(C_4) \simeq \mathfrak{S}_3$.

Zu c):

$$C_2 \times C_2 = \{(0,0), (1,0), (0,1), (1,1)\}$$

Wir zeigen $C_2 \times C_2 \simeq C_4$. Sei $f\colon C_2 \times C_2 \to C_4$ mit $f(z_1, z_2) = 2z_1 + z_2$. Da $z_1, z_2 \in C_2$ gilt $2z_1 + z_2 \leq 3$. Wir sehen, dass f bijektiv ist. Es verbleibt zu zeigen, dass $f \in \mathrm{Hom}(C_2 \times C_2, C_4)$.

$$\begin{array}{lll} f(0,1) + f(0,1) = 2 & f(0,1) + f(1,0) = 3 & f(0,1) + f(1,1) = 0 \\ f(1,0) + f(0,1) = 3 & f(1,0) + f(1,0) = 0 & f(1,0) + f(1,1) = 1 \\ f(1,1) + f(0,1) = 0 & f(1,1) + f(1,0) = 1 & f(1,1) + f(1,1) = 2 \end{array}$$

Somit folgt $C_2 \times C_2 \simeq C_4$, womit auch $\mathrm{Aut}(C_2 \times C_2) \simeq \mathrm{Aut}(C_4) \simeq \mathfrak{S}_3$.

Aufgabe 3.4: Semidirekte Produkte

Seien $(G, \bullet)$ und $(H, *)$ Gruppen und $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(G))$. Wir betrachten die binäre innere Verknüpfung

$$\star\colon (G \times H)^2 \to G \times H \qquad ((g, h), (g', h')) \mapsto (g \bullet \varphi(h)(g'), h * h')$$

auf $G \times H$. Zeigen Sie:

a) Die Menge $G \times H$ bildet zusammen mit $\star$ eine Gruppe, das sogenannte **semidirekte innere Produkt** von G mit H bezüglich[1] φ.
b) Es gilt $G \times \{1_H\} \trianglelefteq G \rtimes H$ und $\{1_G\} \times H \leq G \rtimes H$
c) $\{1_G\} \times H \trianglelefteq G \rtimes H$ genau dann wenn $\varphi(h) = \mathrm{id}_G$ für alle $h \in H$ ist.
d) Ist $N \trianglelefteq G$ und $U \leq G$ mit $N \cap U = \{1_G\}$, so ist $NU \simeq N \rtimes_\varphi U$ für $\varphi \in \mathrm{Hom}(U, \mathrm{Aut}(N))$ gegeben durch $\varphi(u) = n \mapsto unu^{-1}$.

Zu a): Wir wollen zuerst zeigen, dass $\exists 1 \in G \rtimes H\colon 1 \star (g, h) = (g, h) = (g, h) \star 1$. Sei dazu $1 = (\widetilde{g}, \widetilde{h})$, dann folgt $\widetilde{h} = 1_H$. Für $\widetilde{g}$:

$$g \bullet \varphi(h)(\widetilde{g}) = g \Leftrightarrow \varphi(h)(\widetilde{g}) = 1_G$$

Bekannt ist, dass für $f \in \mathrm{Hom}(G, H)$ gelten muss $f(1_G) = 1_H$. Da wir fordern, dass $\varphi(h)$ ein Automorphismus von G ist, kann also nur $\varphi(h)(1_G) = 1_G$ gelten. Damit ist unser neutrales Element in $G \rtimes H$ gegeben durch $(1_G, 1_H)$. Weiters suchen wir inverse Elemente $(\widetilde{g}, \widetilde{h})$ zu (g, h). Aus der Definition von $\star$ folgt direkt $\widetilde{h} = h^{-1}$. Für $\widetilde{g}$ gehen wir analog zum neutralen Element vor:

$$g \bullet \varphi(h)(\widetilde{g}) = 1 \Leftrightarrow \varphi(h)(\widetilde{g}) = g^{-1}$$

Da $\varphi(h)$ ein Automorphismus ist, gibt es eine Abbildung $\psi\colon G \to G$, sodass $\psi \circ \varphi(h) = \mathrm{id}_G = \varphi(h) \circ \psi$. Es gilt natürlich $\psi = \varphi(h^{-1})$ nach Lemma 2.1 aus dem Vorlesungsskript (Seite 19). Somit

$$\varphi(h)(\widetilde{g}) = g^{-1} \Leftrightarrow \widetilde{g} = \varphi(h^{-1})(g^{-1})$$

Damit sind die inversen Elemente gegeben durch $(\varphi(h^{-1})(g^{-1}), h^{-1})$. Das $\star$ assoziativ ist, folgt direkt daraus, dass $\varphi(h)$ ein Automorphismus ist, bzw. φ ein Homomorphismus.

Zu b): Wir wollen zeigen, dass $G \times \{1_H\}$ ein Normalteiler von $G \rtimes H$ ist. Sei $(g_0, h_0) \in G \rtimes H$:

$$\begin{aligned}
&(g_0, h_0) \star G \times \{1_H\} \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) = (g_0, h_0) \star \{(g, 1_H), g \in G\} \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) \\
&= \{(g_0, h_0) \star (g, 1_H) | g \in G\} \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) \\
&= \{(g_0 \bullet \varphi(h_0)(g), h_0) | g \in G\} \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) \\
&= \{(g_0 \bullet \varphi(h_0)(g), h_0) \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) | g \in G\} \\
&= \{(g_0 \bullet \varphi(h_0)(g) \bullet \varphi(h_0)(\varphi(h_0^{-1})(g_0^{-1})), 1_H) | g \in G\} \\
&= \{(g_0 \bullet \varphi(h_0)(g) \bullet g_0^{-1}, 1_H) | g \in G\} \subseteq G \times \{1_H\}
\end{aligned}$$

Da $g_0 \bullet \varphi(h_0)(g) \bullet g_0^{-1} \in G$ für $g, g_0 \in G$ und $h_0 \in H$. Somit gilt $G \times \{1_H\} \trianglelefteq G \rtimes H$.

Für $\{1_G\} \times H$ verwenden wir das Untergruppenkriterium. Wir sehen direkt, dass $(1_G, 1_H) \in \{1_G\} \times H$. Wir müssen also noch zeigen, dass $\forall a, b \in H\colon (1_G, a) \star (1_G, b)^{-1} \in \{1_G\} \times H$. Ausgehen von unseren Überlegungen zum inversen Element folgt $(1_G, b)^{-1} = (1_G, b^{-1})$, womit:

$$(1_G, a) \star (1_G, b^{-1}) = (1_G \bullet \varphi(a)(1_G), a * b^{-1}) = (1_G, a * b^{-1}) \in \{1_G\} \times H$$

Somit ist $\{1_G\} \times H \leq G \rtimes H$.

Zu c): Sei $(g_0, h_0) \in G \rtimes H$:

$$\begin{aligned}
&(g_0, h_0) \star \{1_G\} \times H \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) \\
&= \{(g_0, h_0) \star (1_G, h) | h \in H\} \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1})
\end{aligned}$$

[1] Man schreibt dafür auch $G \rtimes_\varphi H$, oder kurz $G \rtimes H$, falls der Bezug auf φ klar ist.

$$
\begin{aligned}
&= \{(g_0 \bullet \varphi(h_0)(1_G), h_0 * h) | h \in H\} \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) \\
&= \{(g_0, h_0 * h) \star (\varphi(h_0^{-1})(g_0^{-1}), h_0^{-1}) | h \in H\} \\
&= \{(g_0 \bullet \varphi(h_0 * h)(\varphi(h_0^{-1})(g_0^{-1})), h_0 * h * h_0^{-1}) | h \in H\} \\
&= \{(g_0 \bullet \varphi(h_0)(\varphi(h)(\varphi(h_0^{-1})(g_0^{-1}))), h_0 * h * h_0^{-1}) | h \in H\}
\end{aligned}
$$

Damit $(g_0, h_0) \star \{1_G\} \times H \star (g_0, h_0)^{-1} \subseteq \{1_G\} \times H$ gilt, muss also $\varphi(h_0)(\varphi(h)(\varphi(h_0^{-1})(g_0^{-1}))) = g_0^{-1}$ gelten:

$$
\varphi(h_0)(\varphi(h)(\varphi(h_0^{-1})(g_0^{-1}))) = g_0^{-1} \Leftrightarrow \varphi(h)(\varphi(h_0^{-1})(g_0^{-1})) = \varphi(h_0^{-1})(g_0^{-1})
$$

Der einzige Automorphismus f von G, für den gilt $\forall g \in G\colon f(g^{-1}) = g^{-1}$ ist genau $f = \mathrm{id}$. Damit folgt $\varphi = \mathrm{id}_G$.
$\Leftarrow$. Sei $\varphi = \mathrm{id}_G$, dann folgt direkt:

$$
\begin{aligned}
&\{(g_0 \bullet \varphi(h_0)(\varphi(h)(\varphi(h_0^{-1})(g_0^{-1}))), h_0 * h * h_0^{-1}) | h \in H\} \\
&= \{(g_0 \bullet g_0^{-1}, h_0 * h * h_0^{-1}) | h \in H\} = \{(1_G, h_0 * h * h_0^{-1}) | h \in H\} \subseteq \{1_G\} \times H
\end{aligned}
$$