Einführung in Algebra und Zahlentheorie – Übungsblatt 3

Aufgabe 1 (4 Punkte)
Seien G, H endliche Gruppen und $\varphi : G \to H$ ein Gruppenhomomorphismus.

a) Zeige, dass für $g \in G$ die Ordnung $\mathrm{ord}(\varphi(g))$ ein Teiler der Ordnung $\mathrm{ord}(g)$ ist.

b) Sei nun konkret $G = S_n$ für ein $n \in \mathbb{N}$, H eine Gruppe ungerader Ordnung. Zeige, dass φ der triviale Homomorphismus ist.

Lösung Aufgabe 1

a) $g \in G$ habe Ordnung $n \in \mathbb{N}$. Dann ist wegen $\varphi(g)^n = \varphi(g) \cdot ... \cdot \varphi(g) = \varphi(g^n) = \varphi(e_G) = e_H$ die Ordnung m von $\varphi(g)$ sicher kleinergleich n.
Wir können n durch m mit Rest teilen, also $n = km + r$ für ein $k \in \mathbb{N}$ und einen Rest $0 \leq r < m$. (Wir lernen dies später genauer, aber das haben wir ja in der Schule schon gelernt, dass das geht.)
Dann aber ist $e_H = \varphi(g)^n = (\varphi(g)^m)^k \cdot \varphi(g)^r = \varphi(g)^r$, aber da $r < m$ und m die kleinste natürliche Zahl $\neq 0$ mit der Eigenschaft $\varphi(g)^m = e_H$ ist, muss $r = 0$ gelten.
Aber dann ist $n = km$, also m ein Teiler von n.

b) Transpositionen haben Ordnung 2, werden also unter φ nach a) auf Elemente der Ordnung 1 (Da gibt es nur e_H.) oder 2 abgebildet. Nach dem Satz von Lagrange gibt es aber keine Elemente der Ordnung 2, denn $2 \nmid |H|$, also wird jede Transposition auf e_H abgebildet.
Da jedes Element in S_n als Produkt von Transpositionen geschrieben werden kann, wird jedes Element auf e_H abgebildet, φ ist trivial.

Aufgabe 2 (4 Punkte)

a) Beweise die beiden folgenden Aussagen aus Beispiel 1.3.9 der Vorlesung:
Für eine Gruppe G und $g \in G$ ist die Konjugation mit g ein Gruppenautomorphimus von G.
Die Zuordnung $G \mapsto \mathrm{Aut}(G)$, $g \mapsto (h \mapsto ghg^{-1})$ ist ein Gruppenhomomorphismus.

b) Zeige $\mathrm{Aut}(S_3) \cong S_3$.
(*Hinweis: Zeige, dass der Homomorphismus aus a) injektiv ist. Wieso ist er auch surjektiv? Hier könnte ein Mächtigkeitsargument helfen.*)

Lösung Aufgabe 2

a) Für $g \in G$ sei Ω_g die Konjugation mit g. Dann ist Ω_g sicher bijektiv, denn $\Omega_{g^{-1}}$ ist invers dazu, wie man leicht nachrechnet, etwa $(\Omega_g \circ \Omega_{g^{-1}})(h) = \Omega_g(g^{-1}hg) = gg^{-1}hgg^{-1} = h$ für alle $h \in H$, analog bei Vertauschung von Ω_g und $\Omega_{g^{-1}}$.
Desweiteren ist $\Omega_g(h_1h_2) = gh_1h_2g^{-1} = gh_1(g^{-1}g)h_2g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \Omega_g(h_1)\Omega_g(h_2)$, also Ω_g ein Homomorphismus, also ein Automorphismus.

Schließlich bleibt zu zeigen, dass die Zuordnung $g \mapsto \Omega_g$ selbst ein Homomorphismus ist, also $\Omega_{g_1g_2} = \Omega_{g_1} \circ \Omega_{g_2}$. Für $h \in G$ gilt
$\Omega_{g_1g_2}(h) = g_1g_2h(g_1g_2)^{-1} = g_1g_2hg_2^{-1}g_1^{-1} = \Omega_{g_1}(\Omega_{g_2}(h)) = (\Omega_{g_1} \circ \Omega_{g_2})(h)$.

b) Wir zeigen, dass für eine Permutation $\sigma \neq 1$ die zugehörige Konjugation nichttrivial ist.
$\Omega_{(12)}$ (mit Inversem $(12)^{-1} = (12)$) ist nichttrivial wegen $\Omega_{(12)}(13) = (12)(13)(12) = (23)$.
Analog ist $\Omega_{(13)}(12) = (23)$, $\Omega_{(23)}(12) = (13)$.
$\Omega_{(123)}$ (mit Inversem $(123)^{-1} = (132)$) ist nichttrivial wegen $\Omega_{(123)}(12) = (123)(12)(132) = (23)$ und wieder analog $\Omega_{(132)}(12) = (13)$.
Insgesamt folgt, dass die Zuordnung aus a) injektiv ist.

Insbesondere gibt es mindestens $|S_3| = 6$ Automorphismen, es reicht zu zeigen, dass es auch höchstens 6 solche gibt, dann muss die Zuordnung ein Isomorphismus sein.

S_3 wird von Transpositionen erzeugt, insbesondere ist jeder Automorphismus (Die Aussage gilt natürlich sogar für jeden Homomorpshimus.) eindeutig durch Angabe der Bilder der Transpositionen festgelegt.
Aber jede Transposition wird durch einen Automorphismus ordnungserhaltend auf eine Transposition abgebildet. Da er zusätzlich bijektiv sein muss, entspricht jeder Automorphimus einer Permutation der Transpositionen (wobei wir noch nicht wissen, dass jede Permutation einen Automorphismus gibt...).
Es gibt 3 Transpositionen, also $3! = 6$ Permutationen, also höchstens 6 Automorphismen, was zu zeigen war.

Aufgabe 3 (4 Punkte)
Sei G eine Gruppe.

a) G und die triviale Gruppe seien die einzigen Untergruppen von G. Welche Form hat G?

b) G ist genau dann endlich, wenn G endlich viele Untergruppen besitzt.

Lösung Aufgabe 3

a) Wir zeigen, dass G entweder trivial oder isomorph zu $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p ist.
Klar ist, dass diese beiden Fälle auftreten können, denn beide erfüllen die Voraussetzung: Im Fall $\mathbb{Z}/p\mathbb{Z}$ sieht man dies direkt ein mit Hilfe des Satzes von Lagrange, denn jedes nichttriviale Element erzeugt eine Untergruppe der Ordnung p, wovon es nicht allzu viele gibt.

Wir zeigen nun also, dass nur diese beiden Gruppentypen die Voraussetzung erfüllen. Ohne Einschränkung sei G also nicht die triviale Gruppe, $x \in G \setminus \{e\}$ beliebig.

- Nach der Voraussetzung muss $\langle x \rangle = G$ gelten, also ist G in jedem Fall zyklisch.
- Offensichtlich kann G aber nicht isomorph zu $\mathbb{Z}$ sein, denn $\mathbb{Z}$ hat ja bekannterweise nichttriviale Untergruppen. G ist also isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$.
- Wäre nun aber $n = km$ nicht prim, d.h. $k, m \neq 1$, so erzeugt x^k eine Untergruppe, die wieder zwischen $\{e\}$ und G liegt, was nicht sein kann.

Dies zeigt die Behauptung.

b) „$\Rightarrow$“ ist trivial, da für endliche G bereits die Potenzmenge $\mathcal{P}(G)$ endlich ist.
„$\Leftarrow$“ ist interessanter: Habe G nur endlich viele Untergruppen.
Da G keine zu $\mathbb{Z}$ isomorphe Untergruppe haben kann (diese hätte ja unendlich viele Untergruppen, die wiederum Untergruppen von G wären), muss jedes Element endliche Ordnung haben.
Da jedes $x \in G$ in seinem eigenen Erzeugnis liegt, können wir G schreiben als $G = \bigcup_{x \in G} \langle x \rangle$, wobei auf der rechten Seite nach Voraussetzung nur endlich viele verschiedene Gruppen stehen, die nach Voraussetzung alle endlich sind. G ist also als endliche Vereinigung endlicher Mengen selbst endlich.

Aufgabe 4 (4 Punkte)
Seien G eine Gruppe, $U, V \leq G$ Untergruppen.

a) Zeige, dass $UV := \{uv \mid u \in U, v \in V\}$ genau dann eine Untergruppe ist, wenn $UV = VU$.

b) Zeige, dass $U \cup V$ genau dann eine Untergruppe ist, wenn $U \subseteq V$ oder $V \subseteq U$ gilt.

Lösung Aufgabe 4
In dieser Lösung seien u, v - gegebenenfalls mit Indizes versehen - stets aus U bzw. V.

a) „$\Rightarrow$“ Sei $uv \in UV$. Dann ist uv das Inverse von $u'v' \in UV$, denn UV ist eine Gruppe, also $uv = (u'v')^{-1} = v'^{-1}u'^{-1} \in VU$. Dies zeigt $UV \subseteq VU$.
Sei $vu \in VU$. Dann ist $vu = (u^{-1}v^{-1})^{-1} \in UV$, da UV eine Gruppe, also das Inverse von $u^{-1}v^{-1} \in UV$ auch in UV liegt. Dies zeigt $VU \subseteq UV$.
„$\Leftarrow$“ Wir verwenden das Untergruppenkriterium. Wegen $U, V \neq \emptyset$ ist auch $UV \neq \emptyset$, konkret ist $ee = e \in UV$.

Seien $uv, u'v' \in UV$, dann ist $(uv)(u'v')^{-1} = (uvv'^{-1}u'^{-1}) \overset{(1)}{=} uv''u'^{-1} \overset{(2)}{=} uu''v''' \overset{(3)}{=} u'''v''' \in UV$, wobei die gestrichelten u, v jeweils fest berechnete Elemente sind. Nutze dazu
$vv'^{-1} \in V$ an der Stelle (1),
$v''u^{-1} \in VU = UV$ an der Stelle (2),
$uu'' \in U$ an der Stelle (3).
Damit ist alles für das Untergruppenkriterium gezeigt, UV ist eine Untergruppe.

b) „$\Leftarrow$„ ist trivial, denn die Vereinigung ist dann U beziehungsweise V.

"$\Rightarrow$„ Sei nun $U \cup V$ eine Gruppe, $U \subsetneq V$, es gibt also $u \in U, u \notin V$. Wir müssen $V \overset{(!)}{\subseteq} U$ zeigen. Sei dazu $v \in V$ beliebig.
Es ist $u \in U \subseteq U \cup V$, $v \in V \subseteq U \cup V$ und da $U \cup V$ eine Gruppe ist, gilt auch $uv \in U \cup V$.
Wäre nun $uv \in V$, so wäre auch $u = (uv)v^{-1} \in V$ (denn V ist ja abgeschlossen), was aber ausgeschlossen wurde.
Also ist $uv \in U$ und damit $v = u^{-1}(uv) \in U$, was zu zeigen war.

Abgabe der Übungsblätter:
Bitte wirf deine Lösung bis Dienstag, 8. Mai, 9:30 Uhr, in den entsprechenden Abgabekasten im 1C-Teil des Allianzgebäudes oder gib sie direkt vor der großen Übung deinem Übungsleiter.