11. Übungsblatt

Anmerkungen und Musterlösungen

Aufgabe 44 a) In den Übungsgruppen wurde bewiesen:
Für einen Gruppenhomomorphismus $f : G \longrightarrow H$ gilt

$$f^{-1}(f(U)) = U \cdot \mathrm{Kern}(f) \quad (\forall\, U \leq G) \quad , \quad f(f^{-1}(V)) = V \cap \mathrm{Bild}(f) \quad (\forall\, V \leq H)$$

Ist f surjektiv, so wird durch die Vorschrift $U \longmapsto f(U)$ eine bijektive Abbildung

$$\alpha : \{\, U \,|\, \mathrm{Kern}(f) \subseteq U \leq G \,\} \longrightarrow \{\, V \,|\, V \leq H \,\}$$

definiert. Wendet man dieses Ergebnis auf den natürlichen Gruppenhomomorphismus $\nu : G \longrightarrow G/N$ an, so folgt, da ν surjektiv ist und $\mathrm{Kern}(\nu) = N$ gilt, daß ν eine bijektive Abbildung

$$\alpha : \{\, U \,|\, \mathrm{Kern}(\nu) \subseteq U \leq G \,\} \longrightarrow \{\, V \,|\, V \leq G/N \,\}$$

definiert. Die Zuordnungsvorschrift lautet $U \longmapsto \nu(U) = \{\, [a]_n |\, a \in U \,\} = U/V$. Zu jeder Untergruppe V von G/N gibt es also genau eine Untergruppe U von G mit $N \subseteq U$ und $V = U/N$.

b) Nach a) ist jede Untergruppe V von $\mathbb{Z}_{12}$ von der Form $V = U/\mathbb{Z}12$ mit $\mathbb{Z}12 \subseteq U$. Nun gilt $U = \mathbb{Z}n$ für ein geeignetes $n \in \mathbb{N}_0$ und $\mathbb{Z}12 \subseteq \mathbb{Z}n \iff n \,|\, 12$. Die Menge der positiven Teiler von 12 ist $\{1, 2, 3, 4, 6, 12\}$. Folglich gibt es in $\mathbb{Z}_{12}$ genau die 6 Untergruppen

$$\mathbb{Z}1/\mathbb{Z}12 = \mathbb{Z}_{12}, \mathbb{Z}2/\mathbb{Z}12, \mathbb{Z}3/\mathbb{Z}12, \mathbb{Z}4/\mathbb{Z}12, \mathbb{Z}6/\mathbb{Z}12, \mathbb{Z}12/\mathbb{Z}12 = \{0\}$$

c) Wegen $m \,|\, n$ gilt $\mathbb{Z}n \subseteq \mathbb{Z}m$. Es ist $\mathbb{Z}m/\mathbb{Z}n \subseteq \mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, also

$$\mathbb{Z}m/\mathbb{Z}n = \{\, [km]_n \,|\, k \in \mathbb{N}_0, 0 \leq km < n \,\}$$

Wegen $0 \leq km < n \iff 0 \leq k < \frac{n}{m}$ gibt es genau $\frac{n}{m}$ Nebenklassen von Elementen aus $\mathbb{Z}m$ nach $\mathbb{Z}n$ (beachte $\frac{n}{m} \in \mathbb{N}$!!) , d.h.

$$(\mathbb{Z}m : \mathbb{Z}n) \;=\; \frac{n}{m} \, .$$

45. Aufgabe: Die Kongruenzrelation modulo n auf $\mathbb{Z}$ ist nach a) **reflexiv**, nach b) **symmetrisch** und nach c) **transitiv** , insgesamt also eine **Äquivalenzrelation auf $\mathbb{Z}$** .

e) besagt, daß die Nebenklasse $[a]_n$ von $a \in \mathbb{Z}$ nach dem Normalteiler $\mathbb{Z}n$ gleich der Menge aller ganzen Zahlen ist, die bei Division durch n denselben Rest wie a haben. Daher nennt man $[a]_n$ auch die **Restklasse von a modulo n** .

f) Dies ist der sog. **Chinesische Restsatz**

<u>1. Beweis:</u> In (9.4) wird gezeigt, daß die Abbildung

$$f^\star : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \quad , \quad [a]_{mn} \longmapsto ([a]_m, [a]_n)$$

ein Gruppenisomorphismus ist. Die Surjektivität von $f^\star$ liefert daher die Existenz einer simultanen Lösung von $(\star)$, und die Injektivität die Eindeutigkeit (modulo mn).

<u>2. Beweis:</u> Es wird eine Lösung explizit angegeben.

Da m und n teilerfremd sind, gibt es $x, y \in \mathbb{Z}$ mit $xm + yn = 1$. Definiere

$$x_0 := bxm + ayn$$

Dann ist $x_0 \in \mathbb{Z}$ und es folgt

$$\left.\begin{array}{l} x_0 \equiv ayn \pmod m \\ axm + ayn = a \quad \Longrightarrow \quad ayn \equiv a \pmod m \end{array}\right\} \Longrightarrow \quad x_0 \equiv a \pmod m$$

Analog beweist man $x_0 \equiv b \pmod n$. Damit ist x_0 eine Lösung von $(\star)$.

Ist x_1 eine weitere Lösung von $(\star)$, so folgt

$$\begin{array}{l} x_0 \equiv x_1 \pmod m \\ x_0 \equiv x_1 \pmod n \end{array} ,$$

woraus sich wegen $\mathrm{ggT}(m, n) = 1$ ergibt:

$$x_0 \equiv x_1 \pmod{m \cdot n} .$$

46. Aufgabe: Ein Gruppenisomorphismus $G \longrightarrow G$ einer Gruppe G auf sich heißt auch ein **Gruppenautomorphismus**. Der spezielle Gruppenautomorphismus $\tau_a : G \longrightarrow G$ $(a \in G)$ wird als **innerer Gruppenautomorphismus von** G bezeichnet.

47. Aufgabe: b) $Z(\mathrm{GL}_2(\mathbb{R})) = \{ rE \mid r \in \mathbb{R}^\star \}$ (Dabei ist E die (2×2)–Einheitsmatrix).

Achtung!! Die Nullmatrix gehört **nicht** zu $\mathrm{GL}_2(\mathbb{R})$.

48*. Aufgabe: a) $UN \leq G$ gilt nach Aufg. 40a).

b) Klar ist $N \leq UN$. Da N Normalteiler in G ist, ist N auch Normalteiler in UN.

c) Sei
$$\mu := \nu \mid U : U \longrightarrow UN/N \quad , \quad a \longmapsto [a]_N$$
die Einschränkung des natürlichen Homomorphismus $\nu : G \longrightarrow G/N$ auf U. Dann ist μ ist ein Gruppenhomomorphismus mit

$$\mathrm{Kern}(\mu) = \mathrm{Kern}(\nu \mid U) = U \cap \mathrm{Kern}(\nu) = U \cap N$$

Als Kern eines Gruppenhomomorphismus ist $U \cap N$ Normalteiler in U.

d) Dieses Ergebnis wird in der Literatur häufig als **1. Isomorphiesatz** bezeichnet.

Der Homomorphismus μ aus c) ist surjektiv. Nach dem Homomorphiesatz (8.12) induziert μ einen Isomorphismus

$$\mu^\star : U/\mathrm{Kern}(\mu) = U/U \cap N \xrightarrow{\cong} UN/N \quad , \quad [a]_{U\cap N} \longmapsto [a]_N \quad (a \in U)$$

e) Seien $m, n \in \mathbb{N}$. Wende d) auf die Untergruppen $U := \mathbb{Z}m$ und $N := \mathbb{Z}n$ von $(\mathbb{Z}, +)$ an. Man erhält

$$\mathbb{Z}m/\mathbb{Z}m \cap \mathbb{Z}n \;\cong\; \mathbb{Z}m + \mathbb{Z}n/\mathbb{Z}n\,.$$

Nach dem Beweis von (3.6) ist $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}g$ mit $g = \mathrm{ggT}(m, n)$, und nach dem Beweis von (3.13) ist $\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}k$ mit $k = \mathrm{kgV}(m, n)$. Also gilt $\mathbb{Z}m/\mathbb{Z}k \;\cong\; \mathbb{Z}g/\mathbb{Z}n$, woraus sich

$$|\,\mathbb{Z}m/\mathbb{Z}k\,| = |\,\mathbb{Z}g/\mathbb{Z}n\,|$$

ergibt, d.h.

$$(\mathbb{Z}m : \mathbb{Z}k) \;=\; (\mathbb{Z}g : \mathbb{Z}n)\,.$$

Mit Aufg. 44c) folgt $\dfrac{k}{m} \;=\; \dfrac{n}{g}$, d.h. $g \cdot k = m \cdot n$, womit (3.14) noch einmal für natürliche Zahlen bewiesen worden ist:

$$\mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n) \;=\; m \cdot n$$