Modul Algebra 2
SoSe 2006

Einige Lösungen zum 1. und 2. Aufgabenblatt

(2) Zu zeigen: Eine endliche Gruppe G gerader Ordnung enthält ein Element g mit den Eigenschaften $g \neq 1$ und $g^2 = 1$.
Annahme: Es gibt kein Element mit obigen Eigenschaften, d.h. für alle $g \in G \backslash \{1\}$ gilt: $g \neq g^{-1}$. Man kann G also schreiben als $G = \{g_0, g_1, \ldots, g_n\}$, $g_0, \ldots, g_n$ paarweise verschieden, o.E. $g_0 = 1, g_1^{-1} = g_2, g_3^{-1} = g_4, \ldots, g_{n-1}^{-1} = g_n$. Dabei werden die Eindeutigkeit der Inversen sowie die Eigenschaft $(h^{-1})^{-1} = h$ ausgenutzt. Damit ist n gerade, also $|G| = n + 1$ ungerade.

(3) (a) Zu zeigen: Ist $\varphi : G \longrightarrow H$ ein Gruppenmorphismus und $a \in G$, dann gilt: $\varphi(\langle a \rangle) = \langle \varphi(a) \rangle$.
$\subseteq$: Sei $b \in \langle a \rangle$, d.h. $b = a^k$ für ein $k \in \mathbb{Z}$, dann ist $\varphi(b) = \varphi(a^k) = \varphi(a)^k \in \langle \varphi(a) \rangle$.
$\supseteq$: Sei $b \in \langle \varphi(a) \rangle$, d.h. $b = \varphi(a)^k$ für ein $k \in \mathbb{Z}$, dann ist $b = \varphi(a)^k = \varphi(a^k) \in \varphi(\langle a \rangle)$.

(b) Ist $(\mathbb{Z}, +, 0)$ isomorph zu $(\mathbb{Q}, +, 0)$?
Es ist $\mathbb{Z} = \langle 1 \rangle_+$, d.h. für alle Gruppenmorphismen $\varphi : \mathbb{Z} \longrightarrow \mathbb{Q}$ gilt:

$$\varphi(\mathbb{Z}) = \varphi(\langle 1 \rangle_+) = \langle \varphi(1) \rangle_+ \neq \mathbb{Q},$$

da $\mathbb{Q}$ bzgl. $+$ nicht von einem Element erzeugt werden kann, weil für alle $a \in \mathbb{Q}$ gilt: $\frac{a}{2} \in \mathbb{Q}$, aber $\frac{a}{2} \notin \langle a \rangle_+$.

(c) Ist $(\mathbb{Q}, +, 0)$ isomorph zu $(\mathbb{Q}\backslash\{0\}, \cdot, 1)$?
Annahme: Es existiert ein Isomorphismus

$$\varphi : (\mathbb{Q}, +, 0) \longrightarrow (\mathbb{Q}\backslash\{0\}, \cdot, 1).$$

Dann ist φ insbesondere surjektiv, also existiert ein $a \in \mathbb{Q}$ mit $\varphi(a) = 2$. Mit $b := \frac{a}{2}$ ist $2 = \varphi(a) = \varphi(b + b) = \varphi(b)\varphi(b) = \varphi(b)^2$, also $\varphi(b) \in \{\sqrt{2}, -\sqrt{2}\}$. Die Zahl $\sqrt{2}$ ist aber nicht rational. Daher existiert kein solcher Isomorphismus.

(6) Sei G eine Gruppe, D eine nichtleere Menge und $\sigma : G \longrightarrow S(D)$ ein Gruppenmorphismus. Dabei sei $\sigma_g := \sigma(g)$.

(a) Sei $D = G$ und für $g \in G$ sei σ_g die Abbildung mit $\sigma_g(x) = gxg^{-1}$ für alle $x \in G$.
Zu zeigen: Für alle $g \in G$ ist σ_g ein Automorphismus von G:
Für alle $x, y \in G$ gilt:

$$\sigma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \sigma_g(x)\sigma_g(y)$$

Injektivität: Seien $x, y \in G$ mit $\sigma_g(x) = \sigma_g(y)$, dann folgt durch Multiplikation mit g^{-1} von links und mit g von rechts $x = y$.
Surjektivität: Sei $x \in G$, dann ist $\sigma_g(g^{-1}xg) = x$ und damit ist σ_g surjektiv.
Insgesamt ist σ_g ein Automorphismus.

Zu zeigen: $\sigma : G \longrightarrow S(G)$ ist ein Gruppenmorphismus:
Für alle $g, h \in G$ und für alle $x \in G$ gilt:

$$\sigma_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g\sigma_h(x)g^{-1} = (\sigma_g \circ \sigma_h)(x)$$

und damit $\sigma_{gh} = \sigma_g \circ \sigma_h$. Also ist σ ein Gruppenmorphismus.

Zu zeigen: σ ist nicht in jedem Fall injektiv.
σ ist nicht injektiv, sobald $|G| \geq 2$ und G kommutativ ist, weil dann für alle $g \in G$ gilt: $\sigma_g = id_G$, also z.B. für $G = \mathbb{Z}_3$.

(b) Zu zeigen: Für alle $x \in D$ ist $G_x := \{g \in G : \sigma_g(x) = x\}$ eine Untergruppe von G.

G_x ist abgeschlossen bzgl. Verknüpfung, da für alle $g, h \in G_x$ gilt:

$$\sigma_{gh}(x) = (\sigma_g \circ \sigma_h)(x) = \sigma_g(\sigma_h(x)) = \sigma_g(x) = x,$$

also ist $gh \in G_x$.

G_x enthält das Einselement e von G, da $\sigma_e = id_G$.

Damit ist G_x Untergruppe von G.

(c) Zu zeigen: Mit $G(x) := \{\sigma_g(x) : g \in G\}$ ist $|G(x)| = [G : G_x]$.
Da G_x nach (b) Untergruppe von G ist, gilt nach Lagrange:

$$|G| = |G_x|[G : G_x] \quad \text{bzw.} \quad \frac{|G|}{|G_x|} = [G : G_x]$$

Also reicht es zu zeigen: $|G(x)| = \dfrac{|G|}{|G_x|}$
Für $g, h \in G$ gilt:

$$g^{-1}h \in G_x \Leftrightarrow \sigma_{g^{-1}h}(x) = x \Leftrightarrow (\sigma_{g^{-1}} \circ \sigma_h)(x) = x \Leftrightarrow \sigma_h(x) = \sigma_g(x)$$

Also ist $|G| = |G_x||\{\sigma_g(x) : g \in G\}| = |G_x||G(x)|$.