Übungsaufgaben und Musterlösungen
zur Einführung in die Algebra im Sommersemester 2004

Aufgabe (4). *Konjugation. Sei G eine Gruppe. $a, b \in G$ heißen konjugiert (oder ähnlich) in Zeichen $a \approx b$, wenn mit einem $c \in G$ gilt: $ca = bc$.*

(a) Zeigen Sie: $\approx$ ist eine Äquivalenzrelation. Die Äquivalenzklassen heißen Konjugiertenklassen oder Ähnlichkeitsklassen.

(b) Zu festem $a \in G$ betrachten wir die Abbildung $\varphi_a : G \to G$ mit $\varphi_a(x) = axa^{-1}$ für alle $x \in G$. Zeigen Sie: φ_a ist ein Gruppenautomorphismus.

(c) Zeigen Sie: Die Abbildung $\varphi : G \to S(G)$, $a \mapsto \varphi_a$ ist ein Gruppenmorphismus und Kern $\varphi = Z(G)$.

Lösung.

(a) $\approx$ ist eine Äquivalenzrelation, denn: Für alle $a, b \in G$ gilt $a \approx b$, falls ein $c \in G$ existiert mit $ca = bc$.

(i) Reflexivität: Insbesondere gilt $a \approx a$, denn sei $c = e \in G$ (neutrales Element), dann gilt:

$$c \cdot a = e \cdot a \underset{G\ Gruppe}{=} a \cdot c\,.$$

(ii) Symmetrie: Außerdem gilt falls $a \approx b$: $ca = bc$ (für $c \in G$), d.h. es existiert $c^{-1} \in G$, da G Gruppe, so dass:

$$c \cdot c^{-1} = e = c^{-1} \cdot c \text{ und}$$

$$a \cdot c^{-1} = \underbrace{(c^{-1} \cdot c)}_{neutr.\,Elem.} a \cdot c^{-1} \underset{Ass.Gesetz}{=} c^{-1}(c \cdot a)c^{-1} \underset{Def.\,\approx}{=} c^{-1}(b \cdot c)c^{-1} \underset{Ass.Gesetz}{=} (c^{-1} \cdot b)(c \cdot c^{-1}) = c^{-1} \cdot b$$

$$\text{d.h. a} \approx \text{b} \Leftrightarrow \text{b} \approx \text{a}\,.$$

(iii) Transitivität: Für alle $a, b, c \in G$ mit $a \approx b$ und $b \approx c$ gilt: Es existieren $g_1, g_2 \in G$, so dass $g_1 \cdot a = b \cdot g_1$ und $g_2 \cdot b = c \cdot g_2$, d.h. es gilt: $\underbrace{(g_2 \cdot g_1)}_{\in G} \cdot a = g_2 \cdot (g_1 \cdot a) = g_2 \cdot (b \cdot g_1)$

$$\underset{Ass.Gesetz}{=} (g_2 \cdot b) \cdot g_1 = (c \cdot g_2) \cdot g_1 = c \cdot \underbrace{(g_2 \cdot g_1)}_{\in G}\,.$$

Damit folgt, dass ein $\tilde{g} \in G$ existiert, so dass $\tilde{g} \cdot a = c \cdot \tilde{g}$. Somit folgt $a \approx c$ und damit ist $\approx$ eine Äquivalenzrelation.

(b) $\varphi_a : G \to G$ ist Gruppenhomomorphismus, denn für alle $x, y \in G$ gilt:

$$\begin{aligned}\varphi_a(x) \cdot \varphi_a(y) &= (axa^{-1}) \cdot (aya^{-1}) \underset{Ass.Gesetz}{=} (a \cdot x) \cdot \underbrace{(a^{-1} \cdot a)}_{inv./neutr.\,Element} \cdot (y \cdot a^{-1}) \\ &= (a \cdot x) \cdot e \cdot (y \cdot a^{-1}) \underset{Ass.Gesetz}{=} a \cdot (x \cdot y) \cdot a^{-1} = \varphi_a(x \cdot y)\end{aligned}$$

Es gilt: φ_a bijektiv genau dann wenn ein $\tilde{\varphi} : G \to G$ existiert mit $\varphi_a \circ \tilde{\varphi} = id = \tilde{\varphi} \circ \varphi_a$.
$\varphi_a \circ \varphi_{a^{-1}} = id_G$, denn für alle $x \in G$ gilt:

$$\varphi_a(\varphi_{a^{-1}}(x)) = \varphi_a(a^{-1} \cdot x \cdot (a^{-1})^{-1}) = \varphi_a(a^{-1} \cdot x \cdot a) = a(a^{-1} \cdot x \cdot a)a^{-1} \underset{Ass.Gesetz}{=} (a \cdot a^{-1})x(a \cdot a^{-1}) = x$$

und

$$\varphi_{a^{-1}}(\varphi_a(x)) = \varphi_{a^{-1}}(a \cdot x \cdot a^{-1}) = a^{-1}(a \cdot x \cdot a^{-1})a \underset{Ass.Gesetz}{=} (a^{-1} \cdot a)x(a^{-1} \cdot a) = x$$

(c) Kern $\varphi = \{x \in G | \varphi_x = id_G\}$. Es ist $Z(G) \subseteq$ Kern φ, denn:

Für alle $a \in Z(G)$, für alle $g \in G$ gilt: $a \cdot g = g \cdot a$, d.h. also für alle $z \in G$:

$\varphi_a(z) = a \cdot z \cdot a^{-1} = a(z \cdot a^{-1}) = (a \cdot a^{-1}) \cdot z = z = id_G(z)$.

Weiterhin ist Kern $\varphi \subseteq Z(G)$, denn:

Für alle $x \in$ Kern φ gilt: $\varphi_x = id_G$, also für alle $g \in G$:

$$g \cdot x = \varphi_x(g) \cdot x = (x \cdot g \cdot x^{-1}) \cdot x \underset{Ass.Gesetz}{=} (x \cdot g) \cdot \underbrace{(x^{-1} \cdot x)}_{neutr.\,Element} = x \cdot g.$$

Damit folgt: $x \in Z(G)$.

$\varphi : a \mapsto \varphi_a$ ist ein Gruppenhomomorphismus, denn für alle $a \in G$ gilt:

$\varphi_{ab}(g) = (ab) \cdot g \cdot (ab)^{-1} = a \cdot (bg) \cdot b^{-1} \cdot a^{-1} = a \cdot \varphi_b(g) \cdot a^{-1} = \varphi_a(\varphi_b(g))$.

Somit folgt $\varphi_{ab} = \varphi_a \circ \varphi_b$ und es gilt $\varphi_e = id_G$.

Aufgabe (7). *Sei G eine Gruppe, und seien $a, b \in G$ mit $\operatorname{ord} a < \infty$ und $\operatorname{ord} b < \infty$. Es gelte weiterhin $\langle a \rangle \cap \langle b \rangle = \{1\}$. Dann gilt $\operatorname{ord}(\langle a, b \rangle) \geq \operatorname{ord} a \cdot \operatorname{ord} b$, wobei sowohl Gleichheit als auch Ungleichheit gelten kann.*

Lösung. Setze

$$H := \{a^i b^j \mid 0 \leq i < \operatorname{ord} a,\ 0 \leq j < \operatorname{ord} b\}.$$

Es gilt $|H| \leq \operatorname{ord} a \cdot \operatorname{ord} b$ und $H \subseteq \langle a, b \rangle$. Wir zeigen nun, dass je zwei Elemente mit verschiedenen Exponenten aus H paarweise verschieden sind, woraus $|H| = \operatorname{ord} a \cdot \operatorname{ord} b$ folgt. Dann muss auch $\langle a, b \rangle$ mindestens $\operatorname{ord} a \cdot \operatorname{ord} b$ Elemente enthalten, was zu zeigen war.

Seien $a^i b^j \in H$ und $a^k b^\ell \in H$ mit $a^i b^j = a^k b^\ell$. Multiplizieren von Links mit a^{-k} und von Rechts mit b^{-j} liefert

$$a^{i-k} = b^{\ell-j},$$

was wegen der Voraussetzung $\langle a \rangle \cap \langle b \rangle = \{1\}$ gerade

$$a^{i-k} = 1 \qquad \text{und} \qquad b^{\ell-j} = 1$$

liefert. Nun ist

$$-\operatorname{ord} a < i - k < \operatorname{ord} a \qquad \text{und} \qquad -\operatorname{ord} b < \ell - j < \operatorname{ord} b,$$

womit $i - k = 0 = \ell - j$ sein muss, also ist $i = k$ und $\ell = j$.

Damit ist $|H| = \operatorname{ord} a \cdot \operatorname{ord} b$ gezeigt, und somit der erste Teil der Behauptung.

Als Beispiel für Gleichheit betrachte die triviale Gruppe $\{1\}$ mit $a = b = 1$. (Die Voraussetzungen sind dann natürlich erfüllt.)

Als Beispiel für Ungleichheit betrachte die Gruppe $\langle A, B \rangle$ aus Aufgabe (5).

Aufgabe (8). *Seien U, V Untergruppen und K ein Normalteiler der Gruppe G. Zeigen Sie:*

(a) Wenn die Menge der Linksnebenklassen von H dieselbe ist wie die Menge der Rechttsnebenklassen, dann ist H ein Normalteiler.

(b) $\forall a, b \in G\ :\ (aK) \cdot (bK) = (ab)K$.

(c) $U \cdot K = K \cdot U$

(d) $\forall a \in G\ :\ a(U \cap V) = aU \cap aV$.

(e) Sind $[G : U]$, $[G : V]$, $[G : U \cap V]$ die (möglicherweise unendlichen) Anzahlen der Linksnebenklassen von U, V, bzw. $U \cap V$ in G, dann gilt:

$$[G : U] < \infty \text{ und } [G : V] < \infty \ \Rightarrow \ \text{(Satz von Poincaré).}$$

Bei (b) soll nur die Definition 6 von §4 benutzt werden.

Lösung.

(a) Für alle $a, b \in G$ gilt: Aus $aK = Kb$ folgt $b \in aH$ (da K ein neutrales Element hat), also $bK = aK = Kb$ wegen der Disjunktheit der Linksnebenklassen.

(b) Zeige: $\forall a, b \in G : (aK)(bK) = (ab)K$
Seien $a, b \in G$ Zeige zunächst: $(aK)(bK) \subseteq (ab)K$
Beweis:

Sei $x \in (aK)(bK)$
$\Rightarrow akbk' = x$, wobei $k, k' \in K$ geeignet
$\Rightarrow abk''k' = x$, weil K Normalteiler, $k'' \in K$
$\Rightarrow abk^{neu} = x$, mit $k^{neu} = k''k'$
$\Rightarrow x \in (ab)K$

Zeige nun: $(ab)K \subseteq (aK)(bK)$ Beweis:

Sei $x \in (ab)K$
$\Rightarrow \exists k \in K : x = abk$
$\Rightarrow \exists k \in K : x = a1bk$
$\Rightarrow x \in (aK)(bK)$

(c) Zeige: $UK = KU$
Beweis mit Lemma:

Sei $x \in UK$
$\Leftrightarrow \exists u \in U : x = uK$
$\Leftrightarrow \exists u \in U : x = Ku$
$\Leftrightarrow x \in KU$

Beweis ohne Lemma:
Zeige: $UK \subseteq KU$
Beweis:

Sei $x \in UK$
$\Rightarrow x = uk, u \in U$ und $k \in K$ geeignet
$\Rightarrow xu^{-1} = uku^{-1}$
$\Rightarrow xu^{-1} = k'$, weil K Normalteiler, $k' \in K$
$\Rightarrow x = k'u$
$\Rightarrow x \in KU$

Zeige: $KU \subseteq UK$
Beweis:

Sei $x \in KU$
$\Rightarrow x = ku, u \in U$ und $k \in K$ geeignet
$\Rightarrow u^{-1}x = u^{-1}ku$
$\Rightarrow u^{-1}x = u^{-1}k(u^{-1})^{-1}$
$\Rightarrow u^{-1}x = k'$, weil K Normalteiler, $k' \in K$
$\Rightarrow x = uk'$
$\Rightarrow x \in UK$

(d) Zeige: $\forall a \in G : a(U \cap V) = aU \cap aV$
Sei $a \in G$
Zeige zunächst: $a(U \cap V) \subseteq aU \cap aV$
Beweis:

Sei $x \in a(U \cap V)$
$\Rightarrow \exists t \in U \cap V : x = at$
$\Rightarrow \exists t \in U : x = at$ und $\exists t \in V : x = at$
$\Rightarrow x \in aU$ und $x \in aV$
$\Rightarrow x \in aU \cap aV$

Zeige nun: $aU \cap aV \subseteq a(U \cap V)$
Beweis:

Sei $x \in aU \cap aV$
$\Rightarrow \exists u \in U : x = au$ und $\exists v \in V : x = av$
$\Rightarrow au = av = x$
$\Rightarrow u = v$
$\Rightarrow \exists u = v \in (U \cap V) : x = au$
$\Rightarrow x \in a(U \cap V)$

(e) Zeige: $[G:U] < \infty$ und $[G:V] < \infty \Rightarrow [G:U \cap V] < \infty$
Beweis:

Sei $[G:U] < \infty$ und $[G:V] < \infty$
$\Rightarrow$ Anzahl der Linksnebenklassen, die als Schnitt von Linksnebenklassen von U mit Linksnebenklassen von V entstehen ist endlich
$|\{aU \cap aV \mid a \in G\}| < \infty$ (höchstens $[G:U] \cdot [G:V] < \infty$ Stück)
$\Rightarrow [G:U \cap V] = |\{a(U \cap V) \mid a \in G\}| \overset{(d)}{=} |\{aU \cap aV \mid a \in G\}| < \infty.$

Aufgabe (9). *Für $a, b \in \mathbb{Z}$ sei $a \circ b = a + b - ab$. Weisen Sie nach, dass $(\mathbb{Z}, \circ, 0)$ ein Monoid ist und dass die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}$ mit $\varphi(a) = 1 - a$ ein Monoidisomorphismus ist mit dem Monoid $(\mathbb{Z}, \cdot, 1)$.*

Lösung.

(i) Gegeben: $a, b \in \mathbb{Z}, a \circ b = a + b - ab$. Zu zeigen: $(\mathbb{Z}, \circ, 0)$ ist Monoid, also zu zeigen: Assoziativität sowie neutrales Element.
Zum neutralen Element:
$a \circ 0 = a + 0 - a \cdot 0 = a = 0 + a - 0 \cdot a = 0 \circ a$, also ist 0 das neutrale Element.
Zur Assoziativität:

$$\begin{aligned}
a \circ (b \circ c) &= a \circ (b + c - bc) \\
&= a + b + c - bc - (a(b + c - bc)) \\
&= a + b + c - bc - (ab + ac - abc) \\
&= a + b + c - bc - ab - ac + abc \\
(a \circ b) \circ c &= (a + b - ab) \circ c \\
&= a + b - ab + c - ((a + b - ab)c) \\
&= a + b - ab + c - (ac + bc - abc) \\
&= a + b + c - ab - ac - bc + abc
\end{aligned}$$

also $a \circ (b \circ c) = (a \circ b) \circ c$.

(ii) Gegeben: $\varphi : \mathbb{Z} \to \mathbb{Z}$ mit $\varphi(a) = 1 - a$. Zu zeigen: φ ist Monoidisomorphismus. Für Monoidmorphismus ist zu zeigen:

- $\varphi(1) = 0$, wobei 1 das neutrale Element in $(\mathbb{Z}, \cdot, 1)$ und 0 das neutrale Element in $(\mathbb{Z}, \circ, 0)$ ist.
- $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$

Das erste ist klar, denn $\varphi(1) = 1 - 1 = 0$ nach Definition von φ. Zum zweiten:

$$\begin{aligned}
\varphi(a) \circ \varphi(b) &= (1 - a) \circ (1 - b) \\
&= (1 - a) + (1 - b) - ((1 - a)(1 - b)) \\
&= 1 - a + 1 - b - (1 - b - a + ab) \\
&= 2 - a - b - 1 + b + a - ab \\
&= 1 - ab \\
&= \varphi(a \cdot b)
\end{aligned}$$

Zu zeigen bleibt jetzt noch, dass φ bijektiv ist:
Injektivität: $\varphi(a) = \varphi(b) \Leftrightarrow (1 - a) = (1 - b) \Leftrightarrow a = b$
Surjektivität: ist erfüllt, da es eine Abbildung gibt, so dass $\varphi(1 - a) = 1 - (1 - a) = a$.
Somit ist φ ein Monoidisomorphismus.

Aufgabe (10). *Sei K ein Körper mit mindestens 5 Elementen. Sei $D = K \setminus \{0,1\}$ und seien $f, g \in S(D)$ gegeben durch die Vorschrift $f(x) = 1 - x$ und $g(x) = \frac{1}{x}$ für $x \in D$.*

Betrachte die Untergruppe $\langle f, g\rangle$ und bestimme die Ordnung, die Untergruppen, die Normalteiler und das Zentrum.

Lösung. Es ist $f^2 = g^2 = \mathrm{id}$. Wir brauchen daher nur die folgenden Kompositionen betrachten[1]: $(gf)(x) = \frac{1}{1-x}$, $(fg)(x) = \frac{x-1}{x}$, $(fgf)(x) = \frac{x}{x-1} = (gfg)(x)$ und da $gfgf = fg$ und $fgfg = gf$ ist, haben wir $\langle f, g\rangle = \{\mathrm{id}, f, g, fg, gf, gfg\}$.

Diese sind nun auch paarweise verschieden: Setzen wir $\varphi(x) = \psi(x)$ für $\varphi, \psi \in \langle f, g\rangle$, so erhalten wir nach Umformen immer eine Gleichung der Form $ax^2 + bx + c = 0$ mit $a, b, c \in K$, nicht alle gleich Null. Diese kann nicht für alle $x \in D$ erfüllt sein, da von 0 verschiedene Polynome vom Grad kleinergleich zwei höchstens zwei Nullstellen haben, jedoch $|D| \geq 3$ vorausgesetzt war.

Als Untergruppen hat man zunächst die trivialen $\{id\}$ und $\langle f, g\rangle$, sowie die zyklischen $\{id, f\}$, $\{id, g\}$, $\{id, fg, gf\}$ und $\{id, fgf\}$. Da jede weitere echte Untergruppe maximal 3 Elemente haben kann, braucht man nur $\langle fgf, f\rangle$ und $\langle fgf, g\rangle$ betrachten. Beide sind jedoch gleich $\langle f, g\rangle$.

Neben den trivialen Normalteilern $\{id\}$ und $\langle f, g\rangle$ ist $\{id, fg, gf\}$ nach Präsenzaufgabe P6 ein Normalteiler. Für die anderen Untergruppen findet man leicht Gegenbeispiele. So folgt aus $gf \neq fg$, dass weder $\{id, f\}$ noch $\{id, g\}$ Normalteiler ist und $\{id, fgf\}$ ist auch keiner, da $f\{id, fgf\} = \{f, gf\} \neq \{f, fg\} = \{id, fgf\}f$.

Wir zeigen, dass das Zentrum nur aus der Identität besteht: f und g liegen nicht im Zentrum, da $fg \neq gf$. $fg \neq Z(\langle f, g\rangle)$, da $ffg = g \neq fgf$ und $gf \neq Z(\langle f, g\rangle)$, da $fgf \neq gff = g$. Ebenso $fgf \neq Z(\langle f, g\rangle)$, da $ffgf = gf \neq fg = fgff$.

[1] Wir lassen das Kompositionszeichen weg, da keine Verwechselungen mit der Multiplikation zu befürchten sind.