Übung zur Vorlesung Einführung in die Algebra

Prof. Dr. J. H. Bruinier
Stephan Ehlen

TECHNISCHE UNIVERSITÄT DARMSTADT

Sommersemester 2009
Lösungshinweise zu Übungsblatt 2

Aufgabe G2.1 Abelsche Gruppen

Es sei G eine endliche abelsche Gruppe mit $|G| = n$ und $G = \{g_1, \dots, g_n\}$. Da G abelsch ist, kann man das Produkt beliebig neu ordnen und da jedes Element zwei mal vorkommt, kann man es auch so ordnen, dass sich ergibt:

$$\prod_{g \in G} g^2 = g_1^2 \cdots g_n^2 = g_1 g_1^{-1} \cdots g_n g_n^{-1} = 1 \cdots 1 = 1.$$

Aufgabe G2.2 Prüfen der Gruppenaxiome

Für $r, s \in (-1,1)$ ist $1 + rs > 0$ und daher

$$\frac{r+s}{1+rs} < 1 \quad \Leftrightarrow \quad r+s < 1+rs \quad \Leftrightarrow \quad 0 < (1-r)(1-s);$$

die Bedingung ganz rechts ist offensichtlich erfüllt, also auch die linke. Somit $r \circ s < 1$. Analog ist $-1 < r \circ s$, da

$$-1 < \frac{r+s}{1+rs} \quad \Leftrightarrow \quad -1-rs < r+s \quad \Leftrightarrow \quad 0 < (1+r)(1+s),$$

wobei die Bedingung rechts offensichtlich erfüllt ist. Es ist also $r \circ s \in (-1,1)$.

Die Verknüpfung $\circ$ ist assoziativ: Für $r, s, t \in (-1,1)$ berechnen wir:

$$\begin{aligned} r \circ (s \circ t) &= r \circ \left(\frac{s+t}{1+st}\right) = \frac{r + \frac{s+t}{1+st}}{1 + r\frac{s+t}{1+st}} = \frac{r + rst + s + t}{1 + st + rs + rt} \\ (r \circ s) \circ t &= \left(\frac{r+s}{1+rs}\right) \circ t = \frac{\frac{r+s}{1+rs} + t}{1 + \frac{r+s}{1+rs} t} = \frac{r+s+t+rst}{1+rs+rt+st}, \end{aligned}$$

durch Erweitern mit $1 + st$ bzw. $1 + rs$. Die rechten Seiten stimmen überein.

0 *ist neutrales Element*: denn $0 \circ s = \frac{0+s}{1+0s} = s$ und analog $s \circ 0 = s$.

$-s$ *ist invers zu* s: Denn $(-s) \circ s = \frac{-s+s}{1+(-s)s} = 0$ und analog $s \circ (-s) = 0$.

Also ist $((-1,1), \circ, 0)$ eine Gruppe.

Aufgabe G2.3 Charakterisierungen von Untergruppen

(a) Die Notwendigkeit der Bedingung ist klar. Ist sie erfüllt, so ist $1 \in H$. Gegeben $y \in H$, erhalten wir mit $x := 1 \in H$

$$H \ni xy^{-1} = 1y^{-1} = y^{-1};$$

H ist also unter der Inversion von G abgeschlossen. Gegeben $x, y \in H$ ist $y^{-1} \in H$ nach dem Vorigen, also $xy = x(y^{-1})^{-1} \in H$ per Voraussetzung: H ist abgeschlossen in G unter der Multiplikation von G.

(b) Die Notwendigkeit der Bedingung ist klar. Ist sie erfüllt, so existiert ein $x \in H$. Mit $y := x$ folgt $1 = xx^{-1} = xy^{-1} \in H$. Daher ist die Bedingung aus (a) erfüllt, somit H Untergruppe von G.

Aufgabe G2.4 Eigenschaften von Gruppenhomomorphismen

Siehe Skript Neeb, Lemma I.2.2.

Aufgabe G2.5 Allgemeine Potenzen

(a) Ist ein Spezialfall von Aufgabe G2.2.

(b) zeigen wir durch Induktion über $n \in \mathbb{N}$.

Induktionsanfang: Es ist $g^1 g^{-1} = gg^{-1} = 1$.

Induktionsschritt: Da $g^{n+1} = gg^n$ nach (a) und $g^{-(n+1)} = g^{-n}g^{-1}$ per Definition, gilt

$$g^{n+1}g^{-(n+1)} = gg^n g^{-n} g^{-1} = gg^{-1} = 1\,,$$

wie behauptet.

(Aus $g^n g^{-n} = 1$ folgt durch Multiplikation mit $(g^n)^{-1}$ von links übrigens tatsächlich $g^{-n} = (g^n)^{-1}$).

(c) Für $n, m \geq 0$ ist die Aussage bereits in (a) gezeigt worden, und es gilt folglich auch

$$g^{-n}g^{-m} = (g^{-1})^n (g^{-1})^m = (g^{-1})^{n+m} = g^{-(n+m)}.$$

Ist $n \geq 0$, $m \leq 0$ und $n + m \geq 0$, so haben wir wegen $n = (n+m) + (-m)$ mit $n + m, -m \geq 0$ nach (a) und (b)

$$g^n g^m = g^{(n+m)+(-m)} g^m = g^{n+m} g^{-m} g^m = g^{n+m}\,.$$

Analog gilt $g^m g^n = g^m g^{-m} g^{m+n} = g^{m+n}$.

Ist $n \geq 0$, $m \leq 0$ und $n + m \leq 0$, so ist $(-n) + (-m) \geq 0$ und somit nach dem vorigen Fall

$$g^n g^m = (g^{-1})^{-n} (g^{-1})^{-m} = (g^{-1})^{(-n)+(-m)} = (g^{-1})^{-(n+m)} = g^{n+m}$$

sowie analog $g^m g^n = g^{m+n}$.

Aufgabe H2.1 Abelsche Gruppen

(a) Seien $a, b \in G$. Es gilt $(ab)^2 = 1$ und $a^2 = b^2 = 1$ nach Voraussetzung. Dies liefert $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

(b) Sei $G = \langle g \rangle$. Die Potenzabbildung $p_G : \mathbb{Z} \to G,\ n \mapsto g^n$ liefert einen surjektiven Gruppenhomomorphismus (nachrechnen!). Außerdem ist das Bild einer abelschen Gruppe unter einem Gruppenhomomorphismus abelsch.

(c) *Abgeschlossenheit*: Seien $f, g \in \mathrm{Hom}(G, H)$, dann ist

$$\begin{aligned}(f+g)(xy) &= f(xy) + g(xy)\\ &= f(x) + f(y) + g(x) + g(y)\\ &= f(x) + g(x) + f(y) + g(y) \text{ (weil } H \text{ abelsch ist)}\\ &= (f+g)(x) + (f+g)(y),\end{aligned}$$

für alle $x, y \in G$. Man beachte, dass hier wiriklich benutzt wurde, dass H abelsch ist.

Das *neutrale Element* ist gegeben durch die triviale Abbildung $0_{\mathrm{Hom}(G,H)} :\ g \mapsto 0_H$.

Das *Inverse* zu $f \in \mathrm{Hom}(G, H)$ ist gegeben durch

$$-f : G \to H, \quad x \mapsto -f(x).$$

(Beides sollte man kurz nachrechnen).

Wie wir oben gesehen haben, ist $f + g$ im Allgemeinen kein Homomorphismus mehr, falls H nicht abelsch ist.

Aufgabe H2.2 Verschiedenes zu Gruppen

(a) Gilt $ab = ac$, so liefert Multiplikation mit a^{-1} von links:

$$a^{-1}(ab) = a^{-1}(ac),$$

wobei $a^{-1}(ab) = (a^{-1}a)b = 1b = b$ und analog $a^{-1}(ac) = c$. Also ist $b = c$.

(b) Sei $x^n = 1$, mit $n \in \mathbb{N}$. Ist $n > 1$, so gilt nach Aufgabe G2.5:

$$1 = x^n = xx^{n-1} = x^{n-1}x\,.$$

Also gilt $x^{n-1} = x^{-1}$, d.h. $x^m = x^{-1}$ mit $m := n-1 \in \mathbb{N}$.

Ist $n = 1$, so ist $x = 1$ und somit $x^{-1} = 1 = x = x^1 = x^m$ mit $m = 1$.

(c) Da G endlich ist, können die Elemente $x, x^2, x^3, \dots$ nicht alle verschieden sein. Es gibt daher natürliche Zahlen k, m mit $k < m$ und $x^k = x^m$. Dann ist

$$1 = x^m(x^k)^{-1} = x^m x^{-k} = x^{m-k}$$

(siehe Aufgabe G2.5), also $x^n = 1$ mit $n := m-k \in \mathbb{N}$.

(d) Ist G eine abelsche Gruppe und sind $x, y \in G$, so gilt

$$(xy)^n = x^n y^n \qquad \text{für alle } n \in \mathbb{N} \tag{1}$$

(der Induktionsbeweis sollte keine Schwierigkeiten bereiten).

Abgeschlossenheit von $\operatorname{tor}(G)$ *unter Multiplikation*: Sind nun $x, y \in \operatorname{tor}(G)$, so finden wir $k, m \in \mathbb{N}$ mit $x^k = 1$ und $y^m = 1$. Beachte, dass

$$x^{km} = (x^k)^m$$

aufgrund des Assoziativgesetzes für mehrfache Produkte (Aufgabe G1.3), denn beide Seiten sind Produkte der km Elemente $x, \dots, x$. Somit

$$x^{km} = (x^k)^m = 1^m = 1 \quad \text{und analog} \quad y^{km} = 1\,.$$

Nach (1) gilt daher $(xy)^{km} = x^{mk}y^{mk} = 1$. Also $(xy)^n = 1$ mit $n := km$ und somit $xy \in \operatorname{tor}(G)$.

Es ist $1 \in \operatorname{tor}(G)$: Denn $1^1 = 1$.

Abgeschlossenheit von $\operatorname{tor}(G)$ *unter der Inversion:* Ist $x \in \operatorname{tor}(G)$, so gibt es ein $n \in \mathbb{N}$ mit $x^n = 1$. Somit $1 = 1^{-1} = (x^n)^{-1} = x^{-n} = (x^{-1})^n$ mit Aufgabe G2.5, so dass $x^{-1} \in \operatorname{tor}(G)$.

(e)* Gegeben eine irrationale Zahl α betrachten wir in der nicht-abelschen Gruppe $\mathrm{GL}(\mathbb{R}^2)$ die Spiegelung φ an der x-Achse g und die Spiegelung ψ an der Ursprungsgeraden

$$h := \mathbb{R}\begin{pmatrix}\cos(2\pi\alpha)\\ \sin(2\pi\alpha)\end{pmatrix}$$

welche mit der x-Achse den Winkel $2\pi\alpha$ einschließt. Dann gilt $\varphi^2 = \psi^2 = \mathrm{id}_{\mathbb{R}^2}$ und somit $\varphi, \psi \in \operatorname{tor}(\mathrm{GL}(\mathbb{R}^2))$. Wie aus der linearen Algebra bekannt ist (oder nachgerechnet werden kann durch Rechnen mit Matrizen !), ist

$$\psi \circ \varphi$$

eine Drehung um den Ursprung, um den Winkel $2(2\pi\alpha) = 4\pi\alpha$.

Aufgabe H2.3 Gruppenautomorphismen

Sei G eine Gruppe und $\mathrm{Aut}(G)$ bezeichne die Menge der Automorphismen von G.

(a) Natürlich ist $\mathrm{Aut}(G) \subset S_G$. Wir wollen Aufgabe G2.3 anwenden. Es ist offensichtlich $\mathrm{id}_G \in \mathrm{Aut}(G)$, also bleibt zu zeigen, dass mit $f, g \in \mathrm{Aut}(G)$ auch $h := f \circ g^{-1}$ ein Automorphismus von G ist. Hier bezeichnet $g^{-1} : G \to G$ den (nach Definition existierenden) Gruppenhomomorphismus, so dass

$$g \circ g^{-1} = g^{-1} \circ g = \mathrm{id}_G$$

gilt. Damit sieht man sofort, dass $g^{-1} \in \mathrm{Aut}(G)$ und ebenso $f^{-1} \in \mathrm{Aut}(G)$. Nun benutzen wir noch, dass die Verknüpfungen von Homomorphismen ein Homomorhpismus ist (ggf. nachrechnen) und, dass

$$(f^{-1} \circ g) \circ (g^{-1} \circ f) = (f \circ g^{-1}) \circ (g \circ f^{-1}) = \mathrm{id}_G,$$

und somit $f \circ g^{-1}$ in der Tat ein Automorphismus von G ist. Mit Aufgabe G2.3 (a) folgt dann, dass $\mathrm{Aut}(G)$ eine Untergruppe von S_G ist.

(b) *φ_a ist Homomorphismus:* $\varphi_a(gh) = a(gh)a^{-1} = a(g(a^{-1}a)h)a^{-1} = (aga^{-1})(aha^{-1}) = \varphi_a(g)\varphi_a(h)$.

Damit ist auch $\varphi_{a^{-1}}$ ein Homomorphismus und

$$(\varphi_a \circ \varphi_{a^{-1}})(g) = a(a^{-1}ga)a^{-1} = a,$$

sowie

$$(\varphi_{a^{-1}} \circ \varphi_a)(g) = a^{-1}(aga^{-1})a = a,$$

d.h. φ_a ist Automorphismus von G.

(c) Es ist für alle $g, h, x \in G$:

$$\begin{aligned}(\psi(gh))(x) &= \varphi_{gh}(x)\\ &= (gh)x(gh)^{-1}\\ &= (gh)x(h^{-1}g^{-1})\\ &= g(hxh^{-1})g^{-1}\\ &= \varphi_g(\varphi_h(x))\\ &= (\varphi_g \circ \varphi_h)(x)\\ &= (\psi(g) \circ \psi(h))(x).\end{aligned}$$

Also haben wir gezeigt, dass $\psi(gh) = \psi(g) \circ \psi(h)$ gilt. Somit ist erwiesen, dass $\psi : G \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus ist.

Aufgabe H2.4 Gruppenisomorphismen

(a) Man wendet die Funktionalgleichung der Exponentialfunktion $\exp(x + y) = \exp(x)\exp(y)$ an.

(b) Angenommen, $\varphi : \mathbb{Q} \to \mathbb{Q}_{>0}$ sei so ein Gruppenisomorphismus zwischen der Gruppe $\mathbb{Q}$ mit der Addition und der Gruppe $\mathbb{Q}_{>0}$ mit der Multiplikation. Dann existiert z.B. ein $x \in \mathbb{Q}$ mit $\varphi(x) = 2$. Außerdem ist natürlich $y := \frac{1}{2}x \in \mathbb{Q}$ und $x = y + y$. Daraus folgt dann aber

$$2 = \varphi(x) = \varphi(y + y) = \varphi(y)\varphi(y) = \varphi(y)^2.$$

Damit müsste $\pm\sqrt{2} = \varphi(y)$ gelten, aber $\sqrt{2} \notin \mathbb{Q}$.

(Wir haben sogar gezeigt, dass φ nicht surjektiv sein kann.)