Übung zur Vorlesung
Einführung in die Algebra

Prof. Dr. J. H. Bruinier
Stephan Ehlen

TECHNISCHE UNIVERSITÄT DARMSTADT

Sommersemester 2009
Lösungshinweise zu Übungsblatt 1

Testaufgabe 1.1 Wahr oder falsch?

Eine Gruppe ist ...

- NICHT definiert als eine unter Multiplikation und Inversion abgeschlossene Menge.
- i.A. KEINE Menge von Symmetrien. (Das kommt zwar vor, ist aber nicht im Allgemeinen so.)
- in der Tat ein Spezialfall eines Monoids.
- ein Spezialfall einer Halbgruppe. Ganz streng genommen wurde zwar die Gruppe als ein Tripel $(G,\circ,1)$ und die Halbgruppe als ein Paar $(S,\circ)$ eingeführt, aber wenn $(G,\circ,1)$ eine Gruppe ist, so ist in der Tat $(G,\circ)$ eine Halbgruppe.

Aufgabe G1.1 Äquivalenzrelationen

(a) a) Für $x \in X$ ist $x \in [x]$, also $X = \bigcup_{x \in X/\sim} [x]$.

b) *Verschiedene Äquivalenzklassen sind disjunkt.* Seien $x, y \in X$ mit $S := [x] \cap [y] = \emptyset$. Dann existiert ein $z \in S$ und es gilt $x \sim z$ und $z \sim y$ (Symmetrie) und somit (Transitivität) $x \sim y$. Ist nun $u \in [x]$, dann folgt $u \sim y$ (Transitivität) und somit $[x] \subseteq [y]$. Ebenso folgt für $v \in [y]$, dass $v \sim x$ und somit $[y] \subseteq [x]$, also $[x] = [y]$.

(b) *Reflexivität*: Sei $z \in \mathbb{C}$. Da $z = 1z$ mit $|1| = 1$, gilt $z \sim z$.

Transitivität: Sind $z_1, z_2, z_3 \in \mathbb{C}$ mit $z_1 \sim z_2$ und $z_2 \sim z_3$, so existieren komplexe Zahlen u und v vom Betrag 1 derart, dass

$$z_2 = uz_1 \qquad \text{und} \qquad z_3 = vz_2 \,.$$

Dann ist also $z_3 = vz_2 = v(uz_1) = (vu)z_1 = wz_1$, wobei $w := vu$ eine komplexe Zahl vom Betrag 1 ist. Somit $z_1 \sim z_3$.

Symmetrie: Ist $z_1 \sim z_2$, so existiert eine komplexe Zahl w vom Betrag 1, mit $z_2 = wz_1$. Dann hat auch w^{-1} den Betrag 1, und wegen

$$z_1 = (w^{-1}w)z_1 = w^{-1}(wz_1) = w^{-1}z_2$$

gilt $z_2 \sim z_1$.

Gestalt der Äquivalenzklassen: Die Äquivalenzklasse $[z]$ von $z \in \mathbb{C}$ besteht aus allen Vielfachen wz von z, wobei w den Einheitskreis $\mathbb{S}^1 := \{w \in \mathbb{C} \colon |w| = 1\}$ durchläuft. Es ist daher

$$[0] = \{0\} \,,$$

und für $z \neq 0$ ist $[z]$ der Kreis vom Radius $|z|$ um 0 in $\mathbb{C}$.

Aufgabe G1.2 Assoziativgesetz für mehrfache Produkte I

Induktionsanfang $k=1$: Für jedes $n \in \mathbb{N}$ und Elemente $x_1, \ldots, x_{n+1} \in S$ haben wir

$$x_1 \circ \cdots \circ x_{n+1} = (x_1 \circ \cdots \circ x_n) \circ x_{n+1}$$

per Definition der linken Seite. Also gilt die zu zeigende Behauptung im Falle $k=1$.

Induktionsschritt. Die Behauptung gelte für k (Induktionsvoraussetzung). Für jedes $n \in \mathbb{N}$ und Elemente $x_1, \ldots, x_{n+(k+1)} \in S$ gilt dann

$$\begin{aligned} x_1 \circ \cdots \circ x_{n+(k+1)} &= (x_1 \circ \cdots \circ x_{n+k}) \circ x_{n+k+1} \\ &= \big((x_1 \circ \cdots \circ x_n) \circ (x_{n+1} \circ \cdots \circ x_{n+k})\big) \circ x_{n+k+1} \\ &= (x_1 \circ \cdots \circ x_n) \circ \big((x_{n+1} \circ \cdots \circ x_{n+k}) \circ x_{n+k+1}\big) \\ &= (x_1 \circ \cdots \circ x_n) \circ (x_{n+1} \circ \cdots \circ x_{n+k+1}), \end{aligned}$$

wobei die erste und letzte Zeile auf der rekursiven Definition mehrfacher Produkte basiert, beim Übergang zur zweiten Zeile die Induktionsvoraussetzung benutzt wurde und beim Übergang zur dritten Zeile das Assoziativgesetz.

Aufgabe G1.3 Assoziativgesetz für mehrfache Produkte II

Wir beweisen die Aussage durch Induktion über n.

Induktionsanfang. Der Fall $n=1$ ist klar nach Definition.

Induktionsschritt. Wir nehmen an, die Aussage gelte bis zu einem gewissen $n \in \mathbb{N}$ (Induktionsvoraussetzung). Sei nun $p \in S$ ein Produkt von $n+1$ Elementen $x_1, \ldots, x_{n+1} \in S$. Dann existieren (per Definition eines Produkts) ein $k \in \{1, \ldots, n\}$, ein Produkt p_1 der k Elemente $x_1, \ldots, x_k$ und ein Produkt p_2 der $n+1-k$ Elemente $x_{k+1}, \ldots, x_{n+1}$ derart, dass

$$p = p_1 \circ p_2 \,.$$

Da $k \leq n$ und $n+1-k \leq n$, gilt per Induktionsvoraussetzung

$$p_1 = x_1 \circ \cdots \circ x_k \qquad \text{und} \qquad p_2 = x_{k+1} \circ \cdots \circ x_{n+1} \,.$$

Nach Aufgabe G2 ist also

$$p = p_1 \circ p_2 = (x_1 \circ \cdots \circ x_k) \circ (x_{k+1} \circ \cdots \circ x_{n+1}) = x_1 \circ \cdots \circ x_{n+1} \,,$$

was zu zeigen war.

Aufgabe G1.4 Untergruppe oder nicht?

H_1 ist Untergruppe der $\mathrm{GL}_2(\mathbb{R})$: Es ist $E_2 = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ mit $b=0$, also $E_2 \in H_1$.

Sind $b_1, b_2 \in \mathbb{R}$, so gilt

$$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix} \in H_1 \,.$$

H_1 ist also unter der Gruppenmultiplikation von $\mathrm{GL}_2(\mathbb{R})$ abgeschlossen. Da

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in H_1$$

für alle $b \in \mathbb{R}$, ist H_1 auch unter der Inversion der Gruppe $\mathrm{GL}_2(\mathbb{R})$ abgeschlossen und somit eine Untergruppe.

H_2 ist eine Untergruppe der $\mathrm{GL}_2(\mathbb{R})$: Offensichtlich ist $E_2 \in H_2$; die Abgeschlossenheit unter der Multiplikation und Inversion der Gruppe $\mathrm{GL}_2(\mathbb{R})$ folgt aus den Formeln

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 \\ 0 & 1 \end{pmatrix} \in H_2$$

und

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \frac{1}{a} \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^{-1} & -a^{-1} b \\ 0 & 1 \end{pmatrix} \in H_2 \,.$$

H_3 ist keine Untergruppe, da $A := \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in H_3$ aber $A^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \notin H_3$.

Aufgabe H1.1 Faktorisieren von Abbildungen

(a) Gegeben $x \in X$ gilt $q(x) = q(x)$ und somit $x \sim_q x$. Gilt $x \sim_q y$ und $y \sim_q z$ für $x, y, z \in X$, so ist $q(x) = q(y)$ und $q(y) = q(z)$, daher $q(x) = q(z)$ und somit $x \sim_q z$. Weiter ist dann $q(y) = q(x)$ und somit $y \sim_q x$. Also ist $\sim_q$ eine Äquivalenzrelation.

(b) Falls $\overline{f} : Y \to Z$ existiert mit $\overline{f} \circ q = f$, so gilt $\overline{f}(q(x)) = f(x)$ für alle $x \in X$. Sind also $x_1, x_2 \in X$ mit $q(x_1) = q(x_2)$ (d.h. $x_1 \sim_q x_2$), so gilt

$$f(x_1) = \overline{f}(q(x_1)) = \overline{f}(q(x_2)) = f(x_2)$$

und daher $x_1 \sim_f x_2$. Wir haben gezeigt, dass $(x_1, x_2) \in \sim_q \Rightarrow (x_1, x_2) \in \sim_f$; also gilt $\sim_q \subseteq \sim_f$. Die angegebene Bedingung ist somit *notwendig* für die Existenz von $\overline{f}$.

Falls $\overline{f}$ mit $\overline{f} \circ q = f$ existiert, so ist $\overline{f}$ eindeutig festgelegt. Gegeben $y \in Y$ existiert wegen der Surjektivität von q nämlich ein $x \in X$ mit $q(x) = y$. Dann ist

$$\overline{f}(y) = \overline{f}(q(x)) = f(x) \tag{1}$$

durch f festgelegt.

Gelte nun $\sim_q \subseteq \sim_f$. Gegeben $y \in Y$, existiert (wie zuvor) ein $x \in X$ mit $q(x) = y$. Motiviert durch (1) definieren wir:

$$\overline{f}(y) := f(x). \tag{2}$$

Hier hängt $\overline{f}(y)$ nicht von der Wahl von x ab, denn sind $x_1, x_2 \in X$ mit $q(x_1) = q(x_2) = y$, so gilt $x_1 \sim_q x_2$, also $x_1 \sim_f x_2$, also $f(x_1) = f(x_2)$. Somit ist eine Funktion

$$\overline{f} : Y \to Z$$

durch (2) wohldefiniert, und per Definition erfüllt diese $\overline{f}(q(x)) = f(x)$ für alle $x \in X$, also $\overline{f} \circ q = f$.

Aufgabe H1.2 Untergruppen

(a)

- Abgeschlossenheit: Sind $g, h \in H$, so ist auch $gh \in H_j$ für alle j, da alle H_j Untergruppen sind.
- Das neutrale Element ist in allen Untergruppen H_j enthalten, also auch in ihrem Schnitt H.
- Inverse: Ist $h \in H$, so ist $h^{-1} \in H_j$ für alle j, da alle H_j Untergruppen sind.

Für (b) und (c): Siehe Skript von Herrn Prof. Neeb.

Aufgabe H1.3 Vereinigungen von Untergruppen

Sei G eine Gruppe. Beweisen oder widerlegen Sie: Sind $H_1, H_2 \subset G$ zwei Untergruppen von G, so ist die Vereinigung $H_1 \cup H_2$ eine Untergruppe von G.

Aufgabe H1.4 Beispiele von Untergruppen

(a) Da $\{x \in X : \mathrm{id}_X(x) \neq x\} = \emptyset$ eine endliche Menge ist, gilt $\mathrm{id}_X \in S_{X,\mathrm{fin}}$. Gegeben $\phi, \psi \in S_{X,\mathrm{fin}}$ sind

$$A := \{x \in X : \phi(x) \neq x\} \quad \text{und} \quad B := \{x \in X : \psi(x) \neq x\}$$

endliche Mengen und somit auch $A \cup B$. Für $x \in X \setminus (A \cup B)$ haben wir $\psi(x) = x$ (da $x \notin B$) und somit $\phi(\psi(x)) = \phi(x) = x$ (da $x \notin A$). Somit ist

$$\{x \in X : (\phi \circ \psi)(x) \neq x\} \subseteq A \cup B$$

eine endliche Menge, daher $\phi \circ \psi \in S_{X,\mathrm{fin}}$.
Schließlich gilt wegen $\phi(x) = x$ für $x \in X \setminus A$ auch $x = \phi^{-1}(x)$, somit

$$\{x \in X : \phi^{-1}(x) \neq x\} \subseteq A.$$

Also $\phi^{-1} \in S_{X,\mathrm{fin}}$.

(b) Offensichtlich ist $\mathrm{id}_V \in \mathrm{Aff}(V)$. Sind $\phi : x \mapsto \phi_L(x) + v$ und $\psi : x \mapsto \psi_L(x) + w$ invertierbare affine Abbildungen, so zeigt

$$(\phi \circ \psi)(x) = \phi_L(\psi_L(x) + w) + v = \underbrace{\phi_L(\psi_L(x))}_{\text{lin. in } x} + \underbrace{\phi_L(w) + v}_{\in V},$$

dass $\phi \circ \psi$ affin ist, also in $\mathrm{Aff}(V)$.

ϕ wie zuvor können wir auch schreiben als $\phi = \tau_v \circ \phi_L$, wobei

$$\tau_v : V \to V, \quad x \mapsto x + v$$

offensichtlich eine Bijektion ist, mit Umkehrabbildung τ_{-v}. Somit $\phi^{-1} = \phi_L^{-1} \circ \tau_v^{-1} = \phi_L^{-1} \circ \tau_{-v}$ mit

$$\phi_L^{-1}(\tau_{-v}(x)) = \phi_L^{-1}(x - v) = \phi_L^{-1}(x) + \phi_L^{-1}(-v).$$

Aufgrund dieser Formel ist ϕ^{-1} affin.