Gruppen

26. Oktober 2017

Aufgrund der desolaten Darbietung habe ich den Beweis für die Modulo-Rechnung hier noch einmal nachgeliefert. Zusätzlich stelle ich noch einige Beispiele mit Beweisen vor, welche wir folglich nicht geschafft hatten. Auch hier können sich Fehler eingeschlichen haben, also sollte man aufmerksam lesen. Zur Erinnerung wird hier noch einmal die Definition einer Gruppe vorgestellt.

1 Beispiele und Aufgaben

Definition 1.1 (Gruppe)**.** Sei G eine nichtleere Menge und $\cdot : G \times G \to G$ mit den folgenden Eigenschaften gegeben:

1. $\forall a, b, c \in G : \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
2. $\exists e \in G : \ a \cdot e = e \cdot a = a \ \forall a \in G$,
3. $\forall a \in G \ \exists a^{-1} \in G : \ a \cdot a^{-1} = a^{-1} \cdot a = e$.

Dann nennt man $(G, \cdot)$ eine Gruppe

Definition 1.2. Sei $(G, \cdot)$ eine Gruppe mit neutralem Element $e \in G$. Dann heißt eine nichtleere Teilmenge $U \subseteq G$ Untergruppe von G, falls

1. $a \cdot b \in U \ \forall a, b \in U$,
2. $a^{-1} \in U \ \forall a \in U$.

Bemerkung 1.3. Eine Gruppe heißt abelsch, falls sie kommutativ ist. Gewöhnlicher Weise schreibt man für die zweistellige Operation im abelschen Fall ein $+$ und kennzeichnet die Inversen durch $-$. Im nicht-kommutativen Fall greift man eher auf die multiplikative Schreibweise zurück. Bei der multiplikativen Schreibweise lässt man auch gern das Multiplikationssymbol wie gewohnt weg, d.h.

$$gh := g \cdot h \ \forall g, h \in G.$$

Beispiel 1.4. Sei $n \in \mathbb{N}$ gegeben und $G := \{0, \ldots, n-1\}$. Dann definiere für alle $a, b \in G$

$$a +_G b := \begin{cases} a+b, & \text{falls } a+b < n, \\ a+b-n, & \text{sonst.} \end{cases}$$

Zu zeigen ist nun, dass $(G, +_G)G$ eine Gruppe ist. Es müssen also alle drei Eigenschaften aus obiger Definition gezeigt werden:

Beweis. 1. Die Assoziativität ist hier das Aufwendigste und erfordert eine übersichtliche Fallunterscheidung, damit man die Identitäten vernünftig erkennen kann. Dabei sind im Tutorium Fehler entstanden. Es gilt für alle $a, b, c \in G$

$$\begin{aligned}
(a +_G b) +_G c &= \begin{cases} (a+b) +_G c, & \text{falls } a+b < n, \\ (a+b-n) +_G c, & \text{sonst} \end{cases} \\
&= \begin{cases} a+b+c, & \text{falls } a+b+c < n, \\ a+b+c-n, & \text{falls } a+b < n, a+b+c \geq n, \\ a+b+c-n, & \text{falls } a+b \geq n, a+b-n+c < n \\ a+b+c-2n, & \text{falls } a+b \geq n, a+b-n+c \geq n \end{cases} \\
&= \begin{cases} a+b+c, & \text{falls } a+b+c < n, \\ a+b+c-n, & \text{falls } a+b < n, a+b+c \geq n, \\ a+b+c-n, & \text{falls } a+b \geq n, a+b+c < 2n \\ a+b+c-2n, & \text{falls } a+b+c \geq 2n \end{cases} \\
&= \begin{cases} a+b+c, & \text{falls } a+b+c < n, \\ a+b+c-n, & \text{falls } n \leq a+b+c < 2n, \\ a+b+c-2n, & \text{falls } a+b-n+c \geq 2n \end{cases} \\
&= \begin{cases} a+b+c, & \text{falls } a+b+c < n, \\ a+b+c-n, & \text{falls } b+c < n, a+b+c \geq n, \\ a+b+c-n, & \text{falls } b+c \geq n, a+b+c < 2n \\ a+b+c-2n, & \text{falls } a+b+c \geq 2n \end{cases} \\
&= \begin{cases} a+b+c, & \text{falls } a+b+c < n, \\ a+b+c-n, & \text{falls } b+c < n, a+b+c \geq n, \\ a+b+c-n, & \text{falls } b+c \geq n, a+b+c-n < n \\ a+b+c-2n, & \text{falls } b+c \geq n, a+b+c-n \geq n \end{cases} \\
&= \begin{cases} a +_G (b+c), & \text{falls } b+c < n, \\ a +_G (b+c-n), & \text{sonst} \end{cases} \\
&= a +_G (b +_G c)
\end{aligned}$$

2. Das neutrale Element ist offensichtlich die $0 \in G$: für alle $a \in G$ gilt $0 \leq a < n$ und somit
$$a +_G 0 = 0 +_G a = 0 + a = a.$$

3. Sei $a \in G$, dann ist $n - a \in G$ und es gilt
$$a +_G (n - a) = (n - a) +_G a = n - a + a - n = 0.$$
Somit ist $n - a$ das inverse Element von a.

□

Bemerkung 1.5. Die obige Gruppe ist offensichtlicher Weise kommutativ, d.h. für alle $a, b \in G$ gilt $a +_G b = b +_G a$. Demnach ist $(G, +_G)$ sogar eine abelsche Gruppe.

Bemerkung 1.6. Die entscheidende Identität in obiger Rechnung ist
$$a +_G b +_G c = \begin{cases} a + b + c, & \text{falls } a + b + c < n, \\ a + b + c - n, & \text{falls } n \leq a + b + c < 2n, \\ a + b + c - 2n, & \text{falls } a + b - n + c \geq 2n. \end{cases}$$
Jene entspricht exakt dem gewohnten Rechnen mit Restklassen, welches sich allgemein auf Gruppen fortsetzen lässt (siehe hierfür Normalteiler).

Jetzt folgen ein paar Beispielaufgaben, welche man lösen kann, um besser mit dem Konzept der Gruppen vertraut zu werden. Die Lösungen befinden sich am Ende.

Aufgabe 1.7. *Sei $(G, \cdot)$ eine Gruppe mit neutralem Element $e \in G$. Außerdem gelte*
$$g \cdot g = e \ \forall g \in G.$$
Dann ist G kommutativ.

Aufgabe 1.8. *Sei $(G, \cdot)$ eine Gruppe und $U \subseteq G$. Dann sind folgende Aussagen äquivalent:*

1. *U ist eine Untergruppe von G,*
2. *$g^{-1}h \in U \ \forall g, h \in U$.*

Aufgabe 1.9. *Definiere für $a, b \in \mathbb{R}$ die Abbildung $f_{a,b} : \mathbb{R} \to \mathbb{R}$ durch*
$$f_{a,b}(x) := ax + b, \ x \in \mathbb{R}.$$
Die Menge der affin-linearen Transformationen auf $\mathbb{R}$
$$G := \{f_{a,b}, a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}\}.$$
bilden eine Gruppe bezüglich der Komposition von Abbildungen.

Aufgabe 1.10. *Sei*
$$a * b := (a + b)^2, \ a, b \in \mathbb{R}.$$
Zeige, dass $(\mathbb{R}, *)$ keine Gruppe ist.

Aufgabe 1.11. *Sei $(G, \cdot)$ eine endliche Gruppe, d.h. $\#G < \infty$, dann gilt*

$$\forall g, h \in G \; \exists n \in \mathbb{N} : g^n = h^n.$$

Aufgabe 1.12. *Die n-te Symmetrische Gruppe sei definiert durch*

$$S_n := \{f : \{1, \ldots, n\} \to \{1, \ldots, n\} : f \text{ bijektiv}\}.$$

Zeige, dass S_n eine Gruppe bezüglich der Komposition von Abbildungen ist und dass $\#S_n = n!$.

2 Lösungen

Beweis von Aufgabe 1.7. Seien $g, h \in G$, dann gilt

$$gh = gh(hghg) = g(hh)ghg = gghg = hg.$$

□

Beweis von Aufgabe 1.8. 1. $\implies$ 2.:
Seien $g, h \in U$. Dann gilt aufgrund der Untergruppeneigenschaften auch $g^{-1} \in U$ und folglich

$$g^{-1}h \in U.$$

2. $\implies$ 1.:
Als erstes zeigen wir

$$g^{-1} \in U \; \forall g \in U.$$

Sei $g \in U$ (nach Voraussetzung ist U nicht leer), dann gilt

$$e = g^{-1}g \in U$$

und demnach

$$g^{-1} = g^{-1}e \in U.$$

Folglich ist U unter Inversenbildung abgeschlossen. Nun ist nur noch zu zeigen, dass U auch multiplikativ abgeschlossen ist: seien wieder $g, h \in U$. Dann gilt nach obiger Diskussion auch $g^{-1} \in U$ und somit

$$gh = (g^{-1})^{-1}h \in U.$$

□

Beweis von Aufgabe 1.9. Aus einer der Übungsaufgaben folgt, dass

$$\{f : \mathbb{R} \to \mathbb{R} : f \text{ bijektiv}\}$$

eine Gruppe bezüglich der Komposition bildet. Es ist somit nur noch zu zeigen, dass G eine Untergruppe ist. Die Menge G ist offenbar nicht leer und jedes $f_{a,b} \in G$ mit $a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}$ besitzt eine Umkehrabbildung

$$f_{a,b}^{-1}(x) = \frac{x-b}{a} = \frac{x}{a} - \frac{b}{a} = f_{\frac{1}{a},-\frac{b}{a}}(x),$$

wobei $f_{\frac{1}{a},-\frac{b}{a}} \in G$. Also ist nur noch die multiplikative Abgeschlossenheit zu zeigen: seien $f_{a_1,b_1}, f_{a_2,b_2} \in G$ mit $a_1, a_2 \in \mathbb{R} \setminus \{0\}, b_1, b_2 \in \mathbb{R}$.. Dann gilt

$$f_{a_1,b_1} \circ f_{a_2,b_2}(x) = f_{a_1,b_2}\left(a_2 x + b_2\right) = a_1 a_2 x + a_1 b_2 + b_1 = f_{a_1 a_2, a_1 b_2 + b_1}(x)$$

mit $a_1 a_2 \neq 0$. Demnach ist auch $f_{a_1,b_1} \circ f_{a_2,b_2} \in G$. □

Beweis von Aufgabe 1.10. Es gilt

$$(1 * 2) * 3 = \left((1+2)^2 + 3\right)^2 = (9+3)^2 = 144,$$

aber

$$1 * (2 * 3) = \left(1 + (2+3)^2\right)^2 = (1+25)^2 = 676.$$

Demnach ist keine Assoziativität gegeben. Man kann jedoch leicht zeigen, dass ein neutrales Element existiert und jedes Element ein Inverses besitzt. Jene Operation ist sogar kommutativ. □

Beweis von Aufgabe 1.11. Sei $e \in G$ das neutrale Element der Gruppe $(G, \cdot)$. Aufgrund der Endlichkeit der Gruppe G gilt folgende Aussage

$$\forall g \in G\ \exists m, n \in \mathbb{N} : m < n, g^m = g^n.$$

Durch Umstellen obiger Gleichung erhält man

$$\forall g \in G \exists n \in \mathbb{N} : g^n = e.$$

Seien nun $g, h \in G$ beliebig, dann existieren nach eben bewiesener Aussage $m, n \in \mathbb{N}$ mit $g^m = e$ und $h^n = e$. Hieraus folgt

$$g^{mn} = (g^m)^n = e^n = e = e^m = (h^n)^m = h^{mn}.$$

□

Beweis von Aufgabe 1.12. Die Gruppeneigenschaften von S_n wurden bereits in den Übungsaufgaben nachgewiesen. Es bleibt nur noch $\#S_n = n!$ zu zeigen. Dies kann durch Induktion nachgewiesen werden:
Induktionsanfang: es gilt

$$S_1 = \{f : \{1\} \to \{1\} : f \text{ bijektiv}\} = \{\mathrm{Id} : \{1\} \to \{1\}, \mathrm{Id}(1) = 1\},$$

also $\#S_1 = 1 = 1!$.
Induktionsschritt: sei $n \in \mathbb{N}$ gegeben mit $\#S_n = n!$. Zu zeigen ist nun $\#S_{n+1} = (n+1)!$. Definiere hierfür

$$S_{n+1}^i := \{f \in S_{n+1} : f(i) = n+1\},\ i \in \{1, \dots, n+1\}.$$

Es gilt offenbar

$$\bigcup_{i=1}^{n+1} S_{n+1}^i = S_{n+1}$$

und

$$S_{n+1}^i \cap S_{n+1}^j = \emptyset\ \forall i, j \in \{1, \dots, n+1\}, i \neq j.$$

Falls wir nun zeigen könnten, dass für jedes $i \in \{1, \dots, n+1\}$ die Menge S_{n+1}^i bijektiv auf S_n abgebildet werden kann, wären wir fertig, denn dann würde folgendes gelten:

$$\#S_{n+1} = \#\left(\bigcup_{i=1}^{n+1} S_{n+1}^i\right) = \sum_{i=1}^{n+1} \#S_{n+1}^i = \sum_{i=1}^{n+1} \#S_n = \sum_{i=1}^{n+1} n! = (n+1)n! = (n+1)!.$$

Sei nun $i \in \{1, \dots, n+1\}$ gegeben. Definiere nun $s_i \in S_{n+1}$ durch

$$s_i(j) = \begin{cases} i, & \text{falls } j = n+1, \\ n+1 & \text{falls } j = i, \\ j & \text{sonst.} \end{cases}$$

Dann betrachte folgende Abbildung $s_i : S_{n+1}^i \to S_{n+1}^{n+1}$ mit

$$t_i(f) := f \circ s_i.$$

Zu zeigen ist nun, dass t_i in der Tat eine bijektive Abbildung ist: seien $f_1, f_2 \in S_{n+1}^i$ mit $t_i(f_1) = t_i(f_2)$ gegeben, dann gilt

$$f_1 = f_2 \circ s_i \circ s_i^{-1} = f_2.$$

Demnach ist t_i injektiv. Sei nun $f \in S_{n+1}^{n+1}$, dann ist $f \circ s_i^{-1} \in S_{n+1}^i$ und folglich

$$t_i\left(f \circ s_i^{-1}\right) = f \circ s_i^{-1} \circ s_i = f.$$

Also ist t_i auch surjektiv, die Bijektivität ist somit gezeigt. Zusammengefasst ergibt dies nun

$$\#S_{n+1}^i = \#S_{n+1}^{n+1}\ \forall i \in \{1, \dots, n+1\}.$$

Nun kann jedoch S_{n+1}^{n+1} in offensichtlicher Weise auf S_n bijektiv abgebildet werden:

$$S_{n+1}^{n+1} \ni f \mapsto f_{|\{1,\dots,n\}} \in S_n,$$

womit alles gezeigt ist. □