Prof. Dr. M. Zähle
Lösung von: Dr. T. Bohl Abgegeben: 04.11.–08.11.13

Wintersemester 2013/14
Lineare Algebra und Geometrie 1
Lösung zum 3. Übungsblatt

Zielgruppe: Mo 8:15h Übungsgruppe

Aufgabe 1. Es sei G eine Gruppe mit der **binären** (=zweistelligen) Verknüpfung $\circ$. Zeigen Sie, dass für alle $a, b \in G$ genau ein $x \in G$ existiert, so dass $a \circ x = b$, und genau ein $y \in G$ existiert, so dass $y \circ a = b$. Geben Sie x und y explizit an.

Lösung: bereits in Übung vorgerechnet.

Aufgabe 2. Beweisen Sie die folgenden Aussagen:

(1) Gilt $(ab)^2 = a^2b^2$ für alle Elemente a, b einer Gruppe G, dann ist G kommutativ.
(2) Wenn jedes Element einer Gruppe G zu sich selbst invers ist, so ist G kommutativ.
(3) Jede Gruppe mit drei Elementen ist kommutativ.

Lösung: Sei G eine Gruppe (mit Eins e) und $u, v \in G$ beliebig. Möge $G2$ das Gruppenaxiom vom Existenz einer (beidseitigen) Eins e und $G3$ die Existenz eines (beidseitigen) Inversen bezeichnen.

(1) Sei $(ab)^2 = a^2b^2 \forall a, b \in G$ (*1).
Zu zeigen: $uv = vu$.
Beweis:

$$uv \overset{G2}{=} e\,(uv) \overset{G2}{=} (e\,(uv))\,e \overset{G3 \text{ mit } e=vv^{-1}=u^{-1}u}{=} \left(\left(u^{-1}u\right)(uv)\right)\left(vv^{-1}\right) \overset{\text{assoz}}{=} u^{-1}\left(((uu)\,(vv))\,v^{-1}\right)$$

$$\overset{*1 \text{ für } u,v}{=} u^{-1}\left(((uv)\,(uv))\,v^{-1}\right) \overset{\text{assoz}}{=} \left(\left(u^{-1}u\right)(vu)\right)\left(vv^{-1}\right) \overset{G3}{=} (e\,(vu))\,e \overset{G2}{=} vu$$

(2) Sei $a^{-1} = a \forall a \in G$ (*2).
Zu zeigen: $uv = vu$.
Beweis: $uv \overset{*2 \text{ für } u,v}{=} \left(u^{-1}\right)\left(v^{-1}\right) \overset{\text{Vorlesung 2.1.2.(2)}}{=} (vu)^{-1} \overset{*2 \text{ für } (uv) \in G}{=} vu$.

(3) Sei G dreielementig. OBdA bezeichne seine Elemente: $G = \{u, v, e\}$ mit $e \neq u \neq v \neq e$.
Zu zeigen: G ist kommutativ.
Genügt zu zeigen: $uv = vu$, denn die übrigen Produkte sind durch $G2$ abgedeckt (ue, eu, ve, ev) oder symmetrisch (uu, vv, ee).
Genügt zu zeigen: $uv = e$ und $e = vu$.
Beweis: Fallunterscheidung nach uv. Falls $uv = u$ gilt, dann besagt der Eindeutigkeitsteil von Aufgabe 1, dass $v = e$ (denn $ue = u$). Das widerspricht der OBdA-Annahme, d.h. unserer Konvention, wie wir die Gruppenelemente bezeichnen. Falls $uv = v$ gilt, führen $ev = v$ und Aufgabe 1 zum gleichen Widerspruch. Der Fall $uv = e$ bleibt als einziger übrig. Genauso zeigt man $vu = e$.

- 2.1.2.(2) aus der der Vorlesung: Seien $a, b \in G$ beliebige Elemente einer Gruppe G mit Eins e. Zeigen: $(ab)^{-1} = b^{-1}a^{-1}$. Denn: $e \overset{G2}{=} b^{-1}b \overset{G3}{=} \left(b^{-1}e\right)b \overset{G2}{=} \left(b^{-1}\left(a^{-1}a\right)\right)b \overset{\text{assoz}}{=} \left(b^{-1}a^{-1}\right)(ab)$. Weil das Inverse $(ab)^{-1}$ von ab nach $G3$ eindeutig ist, muss $b^{-1}a^{-1}$ mit ihm übereinstimmen.

Aufgabe 3.

(1) Zeigen Sie, dass die Permutationsgruppe S_n aus $n!$ Elementen besteht.
(2) Zeigen Sie, dass S_n für $n \geq 3$ nicht kommutativ ist.

Zur Erinnerung, $S_n = \{\pi : \text{Die Funktion } \pi : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ ist bijektiv.}\}$. Insbesondere ist S_n keine Teilmenge von S_{n+1}. Die Schreibweise $(a\, b)$ (für $a, b \in \{1, \ldots n\}$) bezeichnet diejenige Transposition $(a\, b) \in S_n$, die a und b vertauscht. Dabei ist $(a\, a)$ die Identität, die gar nichts vertauscht.

Lösung: Salopper Beweis von (i): Für jedes $n \in \mathbb{N}^*$ entspricht S_n der Menge R_n der Zahlenketten $(\pi(1), \pi(2), \ldots, \pi(n))$, die jede der Zahlen $\{1, \ldots, n\}$ genau einmal enthalten (denn man kann jeder solchen Folge eine Permutation $S_n \ni \pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$ zuordnen und umgekehrt). Es genügt also induktiv zu zeigen, dass es genau $n!$ solcher Zahlenketten in R_n gibt, d.h. $|R_n| = n!$.
Induktionsanfang $n = 1$: $R_1 = \{(1)\}$, daher $|R_1| = 1$.
Induktionsschritt von n nach $n+1$: Nach IV möge $|R_n| = n!$. Zu zeigen ist $|R_{n+1}| = (n+1)!$. Es gibt $n+1$ mögliche Positionen, an denen in $\tilde{\pi} \in R_{n+1}$ die Zahl $n+1$ vorkommen kann. Durch Streichen der $n+1$ in $\tilde{\pi}$ erhält man stets eine Zahlenfolge in R_n. Umgekehrt entsteht jedes Element von R_n genau so, und $\tilde{\pi}$ ist durch die Angabe der gestrichenen Position eindeutig rekostruierbar. Also enthält R_{n+1} $n+1$-mal so viele Elemente wie R_n. Nach IV ist daher $|R_{n+1}| = |R_n|(n+1) = n!(n+1) = (n+1)!$.

Beweis von (ii): $[(1\,2) \circ (2\,3)](1) = 2$ aber $[(2\,3) \circ (1\,2)](1) = 3$. Daher kommutieren $(1\,2)$ und $(2\,3)$ nicht.

Umständliche, aber "geradlinig gedachte", formalistische Lösung zu 3.1: Beweis von (i) per Induktion über n.
Induktionsanfang (Fall $n = 1$): zu zeigen: S_1 besteht aus einem Element. Beweis: S_1 enthält nur die identische Abbildung $\mathrm{id} : \{1\} \to \{1\}$, $1 \mapsto \mathrm{id}(1) = 1$.
Induktionsschritt (von n nach $n+1$): Induktionsvoraussetzung (kurz IV) ist, dass S_n $n!$ Elemente enthält.
Zu zeigen: S_{n+1} enthält $(n+1)!$ Elemente.
Setze $N_{n+1} := \{\pi \in S_{n+1} : \pi(n+1) = n+1\}$. Die Einschränkungsabbildung $P : N_{n+1} \to S_n$, $\pi \mapsto P[\pi]$ ordnet jedem $\pi \in N_{n+1}$, $\pi : \{1, \ldots, n+1\} \to \{1, \ldots, n+1\}$ die eingeschränkte Abbildung $P[\pi] : \{1, \ldots, n\} \to \{1, \ldots, n\}$ zu, so dass $P[\pi](k) := \pi(k)$ für alle $k \leq n$. Die Abbildung P ist wohldefiniert (Denn $\pi(k) \leq n$ gilt nach Definition von N_{n+1}, was garantiert, dass $P[\pi]$ seinen Wertebereich nicht verlässt. Denn $P[\pi]$ erbt Injektivität von π, was als Selbstabbildung einer endlichen Menge $\{1, \ldots, n\}$ die Bijektivität von $P[\pi]$ garantiert). Die Abbildung P ist offensichtlich bijektiv. Deshalb enthalten N_{n+1} und S_n gleich viele Elemente. Nach IV sind das $|N_{n+1}| = |S_n| = n!$.
Jedes $\pi \in S_{n+1}$ lässt sich als $\pi = \pi \circ (n+1\; \pi(n+1)) \circ (n+1\; \pi(n+1))$ schreiben. (Es ist $(n+1\; \pi(n+1)) \in S_{n+1}$.) Offensichtlich ist $\pi \circ (n+1\; \pi(n+1)) \in N_{n+1}$ und $\pi(n+1) \in \{1, \ldots, n+1\}$. Deshalb ist $Q : S_{n+1} \to N_{n+1} \times \{1, \ldots, n+1\}$, $\pi \mapsto (\pi \circ (n+1\; \pi(n+1)),\ \pi(n+1))$ wohldefiniert. Außerdem ist $R : N_{n+1} \times \{1, \ldots, n+1\} \to S_{n+1}$, $(\pi, k) \mapsto \pi \circ (n+1\; k)$ das Inverse von Q, weil offensichtlich $Q \circ R$ und $R \circ Q$ die Identitäten auf $N_{n+1} \times \{1, \ldots, n+1\}$ bzw auf S_{n+1} sind. Daher $|S_{n+1}| \overset{Q\, bijek}{=} |N_n \times \{1, \ldots, n+1\}| \overset{\text{Produktmenge}}{=} |N_n|\,|\{1, \ldots, n+1\}| \overset{\underline{IV}}{=} n!(n+1) = (n+1)!$.

Aufgabe 4. Beweisen Sie mittels vollständiger Induktion, dass sich jede Permutation als Komposition von endlich vielen Transpositionen darstellen lässt.

Lösung: Wurde in der umständlichen Version zu Aufgabe 3 mitbewiesen, denn $(n+1\; \pi(n+1))$ ist eine Transposition und P erhält die Eigenschaft, aus endlich vielen Transpositionen zusammengesetzt zu sein.