Vorkurs Gruppen

Jonas Müller*

12. Oktober 2017

Für den Vorkurs der Fachschaft MathPhysInfo im Wintersemster 2017/18. Basierend auf den Vorträgen der letzten Jahre von Saskia Klaus.

Inhaltsverzeichnis

*jj@mathphys.stura.uni-heidelberg.de

1 Einführung

Definition 1. Sei G eine nicht-leere Menge, $e \in G$ ein (ausgezeichnetes) Element und

$$*\colon G \times G \to G$$

eine Abbildung. Wir nennen das Tripel $(G, *, e)$ eine Gruppe, falls für beliebige $a, b, c \in G$ gilt

(i) $(a * b) * c = a * (b * c)$ (Assoziativität)

(ii) $a * e = a$ (Ex. rechtsneutrales El.)

(iii) Es gibt $d \in G$ mit $a * d = e$ (Ex. rechtsinverses El.)

wir nennen die Gruppe zusätzlich abelsch, falls gilt

(iv) $a * b = b * a$ (Kommutativität)

Beispiel 2. (i) $(\mathbb{Z}, +, 0)$ ist eine abelsche Gruppe

(ii) $(\mathbb{Q}\backslash\{0\}, \cdot, 1)$ ist eine abelsche Gruppe

(iii) $(\{-1, 1\}, \cdot, 1)$ ist eine abelsche Gruppe

(iv) $(\mathbb{N}, \cdot, 1)$ ist keine Gruppe

Beispiel 3. Wir betrachten die Menge der bijektiven Abbildungen $M = \{1, 2, 3\} \to M$

$$S_3 = \{e = \mathrm{id},\ d_1 = (1\,2\,3),\ d_2 = (1\,3\,2),\ \tau_1 = (2\,3),\ \tau_2 = (1\,3),\ \tau_3 = (1\,2)\}$$

Als erstes fällt uns auch, dass für $f, g \in S_3$: $f \circ g \in S_3$. Z. B.: $d_1 \circ \tau_1 = (1\,2) = \tau_3 \in S_3$ oder $\tau_1 \circ d_1 = (1\,3) \in S_3$. Insbesondere gilt hier also nicht die Kommutativität.

Außerdem gilt für $f, g, h \in S_3$: $(f \circ g) \circ h = f \circ (g \circ f)$, denn es gilt für $x \in M$ beliebig:

$$((f \circ g) \circ h)(x) \overset{\text{def}}{=} (f \circ h)(h(x)) \overset{\text{def}}{=} f(g(h(x)))$$
$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

Also gilt die behauptete Gleichheit. Da $e \in S_3$ jedes Element wieder auf sich selber abbildet, gilt für $f \in S_3$: $f \circ e = f$.

Außerdem können jede dieser Abbildungen wieder umkehren:

$$e \circ e = e,\ d_1 \circ d_2 = e,\ d_2 \circ d_1 = e\ \tau_1 \circ \tau_1 = e,\ \tau_2 \circ \tau_2 = e\ \tau_3 \circ \tau_3 = e$$

Insgesamt handelt es sich bei S_3 also um eine Gruppe.

Wenn wir nun die bijektiven Abbildungen S_n von $M_n = \{1, \ldots, n\}$ für $n \geqslant 3$ betrachten, fällt uns auf, dass diese auch nicht-abelsche Gruppen sind. Deshalb betrachten wir jetzt Gruppen, als Verallgemeinerung dieses Konzeptes, um Aussagen über all diese Mengen zu treffen.

2 Elementare Eigenschaften

Lemma 4. *Sei G eine Gruppe, $a, b \in G$, s. d., $a * b = e$. Dann gilt auch $b * a = e$, b ist also auch ein linksinverses El. von a.*

Beweis. Sei $c \in G$ rechtsinvers von b, also $b * c = e$. Dann gilt:

$$b*a \overset{1ii}{=} (b*a)*e \overset{b*c=e}{=} (b*a)*(b*c) \overset{1i}{=} b*(a*b)*c \overset{a*b=e}{=} b*e*c \overset{1ii}{=} b*c \overset{n.V}{=} e.$$

q.e.d.

Lemma 5. *Sei G eine Gruppe, dann ist $e \in G$ auch linksneutral, also für $a \in G$: $e * a = a$.*

Beweis. Sei $a \in G$ bel. und $b \in G$, s. d., $a * b = e$. Dann gilt:

$$e * a \overset{\text{n. V.}}{=} (a * b) * a \overset{1i}{=} a * (b * a) \overset{4}{=} a * e \overset{1ii}{=} a$$

q.e.d.

Lemma 6. *Sei G eine Gruppe. Dann ist e das einzige neutrale Element, d. h., für $\tilde{e} \in G$ ein neutrales Element gilt bereits $e = \tilde{e}$.*

Beweis. Es gilt $e = e * \tilde{e} = \tilde{e}$ *q.e.d.*

Lemma 7. *Sei G eine Gruppe, $a \in G$. Dann gilt es nur ein zu a inverses Element. D. h., für $b, c \in G$ mit $a * b = e = a * c$ gilt bereits $b = c$*

Beweis. Es ergibt sich

$$b \overset{5}{=} e * b \overset{\text{n. V.}}{=} (c * a) * b \overset{1i}{=} c * (a * b) \overset{\text{n. V.}}{=} c * e \overset{1ii}{=} c$$

q.e.d.

Bemerkung 8. Wir haben bis jetzt gesehen, dass ein rechtsneutrales Element auch ein linksneutrales Element ist und es nur ein Element mir dieser Eigenschaft gibt. Dieses Element nennen wir das neutrale Element.

Außerdem ist ein rechtsinverses Element auch ein linksinverses Element und zu jedem $a \in G$ gibt es genau ein $b \in G$ mit dieser Eigenschaft. Wir nennen dieses Element das inverse Element von a und wir schreiben $a^{-1} := b$. Insbesondere gilt $(a^{-1})^{-1} = a$.

Lemma 9 (Kürzungsregel). *Sei G eine Gruppe. $a, b, c \in G$ mit $a * b = a * c$. Dann gilt $b = c$*

Beweis. Seien $a, b, c \in G$ wie oben, dann gilt:

$$b \overset{5}{=} e * b \overset{1iii}{=} (a^{-1} * a) * b \overset{1ii}{=} a^{-1} * (a * b) \overset{\text{n.V.}}{=} a^{-1} * (a * c) \overset{1i}{=} (a^{-1} * a) * c \overset{1i/iii}{=} c$$

q.e.d.

3 Untergruppen und Nebengruppen

Definition 10. Sei G eine Gruppe und $H \subseteq G$ nicht-leer. Wir nennen H eine Untergruppe von G, falls für alle $a, b \in H$ gilt

(i) $a * b \in H$

(ii) $a^{-1} \in H$

Beispiel 11. (i) $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ist eine Untergruppe

(ii) $\{\pm 1\} \subseteq \mathbb{Q}$ ist eine Untergruppe

(iii) Für G eine Gruppe, ist $\{e\} \subseteq G$ eine Untergruppe

(iv) $A_3 = \{e, d_1, d_2\} \subseteq S_3$ ist eine Untergruppe (sogar abelsch)

Lemma 12. *Seien G Gruppe, $H \subseteq G$ Untergruppe. Dann gilt $e \in H$ und $(H, *_{|H}, e)$ mit der auf H eingeschränkten Verknüpfung selbst eine Gruppe. Gilt zusätzlich G abelsch, dann ist H abelsch.*

Beweis. H ist nicht-leer, also gibt es $a \in H$. Damit ist $a^{-1} \in H$ nach 10ii. Dann gilt $e = a * a^{-1} \in H$ nach 10i.

(0) Wohldefiniertheit: es muss gelten $\forall a, b \in H : a * b \in H$, dies gilt nach 10i

(i) Assoziativ: Seien $a, b, c \in H$, dann gilt $a, b, c \in G$, also gilt

$$(a * b) * c = a * (b * c)$$

(ii) Rechtsneutrale Element: Es ist $e \in H$ und für $a \in H$: $a * e = a$

(iii) Inverses Element: folgt aus 10ii

(iv) Kommutativität: falls G abelsch ist, gilt für $a, b \in H$: $a * b = b * a$ in G, also auch in H

q.e.d.

Lemma 13. *Sei G Gruppe, $H \subseteq G$, $e \in H$, $(H, *, e)$ Gruppe. Dann gilt $H \subseteq G$ Untergruppe.*

Beweis. 10i) gilt, da H wohldefiniert

10ii) folgt aus 1iii

q.e.d.

Bemerkung 14. G eine Gruppe, $a \in G$. Für $n \in \mathbb{Z}$ definieren wir:

$$a^n := \begin{cases} \overbrace{a * a * \cdots * a}^{n\text{-mal}} & n > 0 \\ e & n = 0 \\ \underbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}_{-n\text{-mal}} & n < 0, \end{cases}$$

es gilt

$$\langle a \rangle := \{a^n | n \in \mathbb{Z}\} \subseteq G$$

ist eine Untergruppe. Wir nennen diese, die von a erzeugte Untergruppe.

Beweis. Übungsaufgabe *q.e.d.*

Definition 15. G Gruppe, $H \subseteq G$ Untergruppe. Wir definieren eine Relation auf G via

$$a \sim_H b :\Longleftrightarrow a^{-1}b \in H$$

Beispiel 16. Wir betrachten $G = \mathbb{Z}$ und $H = 2\mathbb{Z}$. Für $a, b \in \mathbb{Z}$ erhalten wir also

$$a \sim b \Longleftrightarrow b - a \in 2\mathbb{Z}$$

Also muss die Differenz von a und b gerade sein. Das ist genau dann der Fall, wenn a und b beide gerade sind oder beide ungerade sind.

Lemma 17. *Die Relation aus 15 ist eine Äquivalenzrelation.*

Beweis. Seien $a, b, c \in G$ beliebig

(i) Reflexiv: $a^{-1}a = e \in H$, also $a \sim_H a$

(ii) Symmetrie: Gelte $a \sim_H b$, also $a^{-1}b \in H$
Es gilt $(b^{-1}a) = (a^{-1}b)^{-1}$, denn:

$$(a^{-1}b)(b^{-1}a) = a^{-1} * (bb^{-1}) * a = a^{-1}a = e$$

Also $b^{-1}a = (a^{-1}b)^{-1} \in H$, folgt aus 10ii, also $b \sim_H a$

(iii) Transitiv: Gelte $a \sim_H b$ und $b \sim_H c$. Dann gilt

$$a^{-1}c = a^{-1}(bb^{-1})c = \underbrace{(a^{-1}b)}_{\in H}\underbrace{(b^{-1}c)}_{\in H} \in H$$

also $a \sim_H c$

q.e.d.

Lemma 18. *G Gruppe $H \subseteq G$ UG, $a \in G$. Dann ist die Äquivalenzklasse von a bzgl $\sim_H$ gegeben durch*

$$[a] = aH := \{ah \mid h \in H\}$$

Beweis. „$\subseteq$“ Sei $b \in [a]$, also $a \sim b$, also $a^{-1} * b = h \in H$. Damit erhalten wir

$$b = (aa^{-1})b = a(\underbrace{a^{-1}b}_{=h}) = ah$$

Also $b \in aH$.

„$\supseteq$“ Sei $b \in aH$, also $b = ah$ für $h \in H$. Wir erhalten

$$a^{-1}b = a^{-1}ah = h \in H$$

Also $a \sim b$ und $b \in [a]$.

q.e.d.

Notation 19. Wir schreiben

$$G/H := G/\sim_H = \{[a] \mid a \in G\}$$

Beispiel 20. $\mathbb{Z}/2\mathbb{Z} = \{\{\ldots, -4, -2, 0, 2, 4, \ldots\}, \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}\}$

4 Der Satz von Lagrange

Definition 21. Sei G eine Gruppe. Wir nennen G endlich, falls die Menge G nur endlich viele Elemente besitzt. Sei $H \subseteq G$ eine Untergruppe. Ist G/H eine endliche Menge, so nennen wir

$$(G : H) := \#(G/H)$$

den Index von H in G.

Sei $a \in G$. Wir definieren die Ordnung von a durch

$$\operatorname{ord}(a) := \min\{n \in \mathbb{N} \mid a^n = e\} \qquad \text{wobei } \min \emptyset := \infty$$

Bemerkung 22. Sei G eine Gruppe, $a \in G$. Dann gilt

$$\operatorname{ord}(a) = \#\langle a \rangle$$

Beweis. Übungsaufgabe *q.e.d.*

Lemma 23. *Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe. Dann gilt*

(i) Je zwei Äquivalenzklassen sind gleichmächtig

(ii) Je zwei Äquivalenzklassen sind disjunkt oder gleich

(iii) G ist die disjunkte Vereinigung der Äquivalenzklassen

Beweis. (i) Es genügt für $a \in G$ bel zu zeigen, dass $\#[a] = \#[e]$. Dafür betrachten wir $f\colon H \to aH, h \mapsto ah$. f ist injektiv, denn seien $h_1, h_2 \in H$ mit $f(h_1) = f(h_2)$ dann gilt

$$ah_1 = f(h_1) = f(h_2) = ah_2 \overset{9}{\Longrightarrow} h_1 = h_2$$

Da f injektiv ist, gilt nun $\#[a] \geqslant \#[e]$.

Außerdem ist f surjektiv, denn sei $b = ah \in aH$. Dann gilt

$$b = f(h)$$

Damit ist $\#[a] \leqslant \#[e]$.

Also muss bereits $\#[a] = \#[e]$ gelten. Damit folgt nun für $a, b \in G$ beliebig

$$\#[a] = \#[e] = \#[b]$$

(ii) folgt da $\sim$-Äquivalenzrelation

(iii) folgt da $\sim$-Äquivalenzrelation

q.e.d.

Satz 24 (Lagrange). *Sei G eine endliche Gruppe, $H \subseteq G$ eine Untergruppe. Dann gilt:*

$$\#G = \#H \cdot (G : H)$$

Beweis. Wir schreiben zunächst

$$G/H = \{[a_1], \ldots, [a_n]\}$$

mit disjunkten $[a_1], \ldots, [a_n]$ (Lemma 23ii) und $n = \#G/H = (G : H)$ (Definition 21). Wir haben

$$G = \dot{\bigcup_{i=1,\ldots,n}} [a_i] \qquad \text{Lemma 23iii}$$

und damit folgt

$$\#G = \#\left(\dot{\bigcup_{i=1,\ldots,n}} [a_i]\right) = \sum_{i=1}^{n} \#[a_i] \overset{23}{=} \sum_{i=1}^{n} \#[e] = n \cdot \#[e] = (G : H) \cdot \#H$$

q.e.d.

Korollar 25. *Sei G eine endliche Gruppe, $a \in G$. Dann gilt* $\mathrm{ord}(a) | ord(G)$ *bzw.*

$$a^{\#G} = e$$