Vorkurs Gruppen

Jonas Müller*

11. Oktober 2018

Für den Vorkurs der Fachschaft MathPhysInfo im Wintersemester 2018/19.
Basierend auf den Vorträgen der letzten Jahre von Saskia Klaus.

Inhaltsverzeichnis

1 Elementare Eigenschaften 2

2 Untergruppen und Nebengruppen 4

3 Der Satz von Lagrange 7

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

1 Elementare Eigenschaften

Definition 1.1. 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 1.2.

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

Beispiel 1.3. Sei $M_n := \{1, \ldots, n\}$ und

$$S_n := \{\, f\colon M_n \to M_n \mid f \text{ bijektiv} \,\} \,.$$

Dann ist $(S_n, \circ, \mathrm{id})$ eine Gruppe, denn seien f, g und $h \in S_n$ und $x \in M_n$ beliebig, dann gilt

(i)

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

$$\big(f \circ (g \circ h)\big)(x) = f\big((g \circ h)(x)\big) = f\Big(g\big(h(x)\big)\Big) \,.$$

Das heißt es gilt $(f \circ g) \circ h = f \circ (g \circ h)$.

(ii)

$$(f \circ \mathrm{id})(x) = f(\mathrm{id}(x)) = f(x)\,,$$

also $f \circ \mathrm{id} = f$.

(iii) Nach der Vorlesung über Abbildungen existiert f^{-1} mit $f \circ f^{-1} = \mathrm{id}$.

(iv) Für $n \geqslant 3$ ist S_n nicht abelsch.

Lemma 1.4. *Sei G eine Gruppe, $a \in G$ und $b \in G$ ein rechtsinverses von a, d. h. $a*b = e$. Dann ist b auch ein linksinverses von a, also $b * a = e$.*

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

$$b * a \overset{1.1\,(\mathrm{ii})}{=} (b * a) * e \overset{b*c=e}{=} (b * a) * (b * c) \overset{1.1\,(\mathrm{i})}{=} b * (a * b) * c$$

$$\overset{a*b=e}{=} b * e * c \overset{1.1\,(\mathrm{ii})}{=} b * c \overset{n.V}{=} e.$$

q.e.d.

Lemma 1.5. *Sei G eine Gruppe, dann ist $e \in G$ auch linksneutral, also für $a \in G$: $e*a = a$.*

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

$$e * a \overset{\mathrm{n.V.}}{=} (a * b) * a \overset{1.1\,(\mathrm{i})}{=} a * (b * a) \overset{1.4}{=} a * e \overset{1.1\,(\mathrm{ii})}{=} a$$

q.e.d.

Lemma 1.6. *Sei G eine Gruppe. Dann ist e das einzige neutrale Element, d. h., für $\widetilde{e} \in G$ ein neutrales Element gilt bereits $e = \widetilde{e}$.*

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

Lemma 1.7 (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 und $d \in G$ mit $d * a = e$, dann gilt:

$$b \overset{1.5}{=} e * b \overset{1.1\,(\mathrm{iii})}{=} (d * a) * b \overset{1.1\,(\mathrm{i})}{=} d * (a * b)$$

$$\overset{\text{n. V.}}{=} d * (a * c) \overset{1.1\,(\mathrm{i})}{=} (d * a) * c \overset{1.1\,(\mathrm{i})/(\mathrm{iii})}{=} c$$

q.e.d.

Lemma 1.8. *Sei G eine Gruppe, $a \in G$. Dann ist das zu a inverse Element eindeutig, d. h., für $b, c \in G$ mit $a * b = e = a * c$ gilt bereits $b = c$. Dieses bezeichnen wir mit a^{-1}.*

Beweis. Denn es gilt

$$a * b = a * c$$

$$\overset{1.7}{\Longrightarrow} \qquad b = c$$

q.e.d.

2 Untergruppen und Nebengruppen

Definition 2.1. 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 2.2.

(i) $\{\pm 1\} \subseteq \mathbb{Q} \setminus \{0\}$ ist eine Untergruppe.

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

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

(iv) $\mathbb{N} \subseteq \mathbb{Z}$ ist keine Untergruppe.

Lemma 2.3. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt $e \in H$ und $(H, *|_{H \times H}, e)$ ist 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 Definition 2.1. Dann gilt $e = a * a^{-1} \in H$ nach Definition 2.1. Die Abbildung $*|_{H \times H} \to H$ ist aufgrund von Definition 2.1 (i) wohldefiniert. Und es gilt außerdem

(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 Definition 2.1

(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 2.4. *Sei G Gruppe, $H \subseteq G$, $e \in H$, $(H, *|_{H \times H}, e)$ Gruppe. Dann gilt $H \subseteq G$ Untergruppe.*

Beweis.

2.1 (i) gilt, da $(H, *|_{H \times H}, e)$ wohldefiniert

2.1 (ii) folgt aus Definition 1.1 *q.e.d.*

Bemerkung 2.5. 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

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

ist eine Untergruppe. Wir nennen diese, die VON a ERZEUGTE UNTERGRUPPE.

Beweis. Übungsaufgabe *q.e.d.*

Definition 2.6. G Gruppe, $H \subseteq G$ Untergruppe. Wir definieren eine Relation auf G via

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

Beispiel 2.7. Wir betrachten $G = \mathbb{Z}$ und $H = 2\mathbb{Z}$. Für $a, b \in \mathbb{Z}$ erhalten wir also

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

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 2.8. *Die Relation aus 2.6 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 $(a^{-1} * b)^{-1} = (b^{-1} * a)$, denn:

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

Also $b^{-1} * a = (a^{-1} * b)^{-1} \in H$, folgt aus 2.1 (ii), also $b \sim_H a$

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

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

also $a \sim_H c$

q.e.d.

Lemma 2.9. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe, $a \in G$. Dann ist die Äquivalenzklasse von a bezüglich $\sim_H$ gegeben durch*

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

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

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

Also $b \in aH$.

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

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

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

q.e.d.

Notation 2.10. Wir schreiben

$$G/_H := G/_{\sim_H} = \{\, [a] \mid a \in G \,\}$$

Beispiel 2.11. $\mathbb{Z}/_{2\mathbb{Z}} = \Big\{ \{\ldots, -4, -2, 0, 2, 4, \ldots\},\ \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\} \Big\}$

3 Der Satz von Lagrange

Definition 3.1. 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 3.2. Sei G eine Gruppe, $a \in G$. Dann gilt

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

Beweis. Übungsaufgabe *q.e.d.*

Lemma 3.3. *Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe. Dann gilt*

(i) Je zwei Äquivalenzklassen sind disjunkt oder gleich

(ii) G ist die disjunkte Vereinigung der Äquivalenzklassen

(iii) Je zwei Äquivalenzklassen sind gleichmächtig

Beweis.

(i) folgt da $\sim$-Äquivalenzrelation

(ii) folgt da $\sim$-Äquivalenzrelation

(iii) Es genügt für $a \in G$ beliebig zu zeigen, dass $\#[a] = \#[e]$. Dafür betrachten wir $f\colon H \to aH$, $b \mapsto ab$. Sei $g\colon aH \to H$, $b \mapsto a^{-1}b$. Dann gilt für $ah \in aH$ beliebig

$$(f \circ g)(ah) = f(a^{-1}ah) = f(h) = ah$$

und für $h \in H$ beliebig

$$(g \circ f)(h) = g(ah) = a^{-1}ah = h\,.$$

Das heißt f ist bijektiv und somit gilt $\#H = \#f(H) = \#aH$. *q.e.d.*

Satz 3.4 (Lagrange). *Sei G eine endliche Gruppe, $H \subseteq G$ eine Untergruppe. Dann gilt:*

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

Beweis. Sei $n = \#\, {}^{G}/_{H}$ (Definition 3.1) und $a_1, \ldots, a_n \in G$, so dass

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

Nach Lemma 3.3 sind $[a_1], \ldots, [a_n]$ also disjunkt und es gilt

$$G = \dot{\bigcup_{i=1,\ldots,n}} [a_i]$$

und damit folgt

$$\#G = \#\left(\dot{\bigcup_{i=1,\ldots,n}} [a_i]\right) = \sum_{i=1}^{n} \#[a_i]$$

$$\overset{3.3}{=} \sum_{i=1}^{n} \#[e] = n \cdot \#[e] = (G : H) \cdot \#H$$

q.e.d.

Korollar 3.5. *Sei G eine endliche Gruppe, $a \in G$. Dann gilt* $\mathrm{ord}(a) \mid ord(G)$ *bzw.*

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