

Kapitel 7

Gruppen

Dieser Vortrag basiert auf den vorangegangenen Vorträgen von Jonas Müller bzw. Saskia Klaus.

§01 Einführung

§01.01 **Definition** ((*abelsche*) Gruppe). Sei G eine nicht-leere Menge, $e \in G$ ein (ausgezeichnetes) Element und

$$*: G \times G \rightarrow G$$

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

$$(i) \quad (a * b) * c = a * (b * c) \quad (\text{Assoziativität})$$

$$(ii) \quad a * e = a \quad (\text{Ex. rechtsneutrales El.})$$

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

wir nennen die Gruppe zusätzlich *abelsch*, falls gilt

$$(iv) \quad a * b = b * a \quad (\text{Kommutativität})$$

§01.02 **Beispiel.** (a) $(\mathbb{Z}, +, 0)$ ist eine abelsche Gruppe

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

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

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

§01.03 **Beispiel.** Wir betrachten die Menge der bijektiven Abbildungen $M = \{1, 2, 3\} \rightarrow M$

$$S_3 = \{e = \text{id}_3, d_1 = (1\ 2\ 3), d_2 = (1\ 3\ 2), \tau_1 = (2\ 3), \tau_2 = (1\ 3), \tau_3 = (1\ 2)\}$$

Als erstes fällt uns auf, 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:

$$\begin{aligned} ((f \circ g) \circ h)(x) &\stackrel{\text{Def}}{=} (f \circ h)(h(x)) \stackrel{\text{Def}}{=} f(g(h(x))) \\ (f \circ (g \circ h))(x) &= f((g \circ h)(x)) = f(g(h(x))) \end{aligned}$$

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 $M_n = \{1, \dots, n\}$ für $n \geq 3$ 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.

§02 Elementare Eigenschaften

§02.01 **Lemma.** 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 .

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

$$b * a \stackrel{\text{lii}}{=} (b * a) * e \stackrel{b * c = e}{=} (b * a) * (b * c) \stackrel{\text{li}}{=} b * (a * b) * c \stackrel{a * b = e}{=} b * e * c \stackrel{\text{lii}}{=} b * c \stackrel{\text{n.V.}}{=} e.$$

□

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

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

$$e * a \stackrel{\text{n.V.}}{=} (a * b) * a \stackrel{\text{li}}{=} a * (b * a) \stackrel{4}{=} a * e \stackrel{\text{lii}}{=} a$$

□

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

§02.06 **Beweis.** Es gilt $e = e * \tilde{e} = \tilde{e}$

□

§02.07 **Lemma.** 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 $b = c$

§02.08 **Beweis.** Es ergibt sich

$$b \stackrel{5}{=} e * b \stackrel{\text{n.V.}}{=} (c * a) * b \stackrel{\text{li}}{=} c * (a * b) \stackrel{\text{n.V.}}{=} c * e \stackrel{\text{lii}}{=} c$$

□

§02.09 **Bemerkung.** Wir haben bis jetzt gesehen, dass ein rechtsneutrales Element auch ein linksneutrales Element ist und es nur ein Element mit 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 $(a^{-1})^{-1} = a$.

□

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

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

$$b \stackrel{5}{=} e * b \stackrel{\text{liii}}{=} (a^{-1} * a) * b \stackrel{\text{lii}}{=} a^{-1} * (a * b) \stackrel{\text{n.V.}}{=} a^{-1} * (a * c) \stackrel{\text{li}}{=} (a^{-1} * a) * c \stackrel{\text{li/iii}}{=} c$$

□

§03 Untergruppen und Nebengruppen

§03.01 **Definition.** 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) $a^{-1} \in H$

□

§03.02 **Beispiel.** (a) $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ist eine Untergruppe

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

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

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

§03.03 **Lemma.** 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.

§03.04 **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

1. Assoziativ: Seien $a, b, c \in H$, dann gilt $a, b, c \in G$, also gilt

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

2. Rechtsneutrale Element: Es ist $e \in H$ und für $a \in H : a * e = a$

3. Inverses Element: folgt aus 10ii

4. Kommutativität: falls G abelsch ist, gilt für $a, b \in H : a * b = b * a$ in G , also auch in H

□

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

§03.06 **Beweis.**

(i) gilt, da H wohldefiniert

(ii) folgt aus 1(iii)

□

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

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

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*.

§03.08 **Beweis.** Übungsaufgabe □

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

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

□

§03.10 **Beispiel.** 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. □

§03.11 **Lemma.** Die Relation aus ?? ist eine Äquivalenzrelation.

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

1. Reflexiv: $a^{-1}a = e \in H$, also $a \sim_H a$
2. 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 ??ii, also $b \sim_H a$

3. 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 $a \sim_H c$

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

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

§03.14 **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 $b \in [a]$.

§03.15 **Schreibweise.** Wir schreiben

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

§03.16 **Beispiel.** $\mathbb{Z}/2\mathbb{Z} = \{\{\dots, -4, -2, 0, 2, 4, \dots\}, \{\dots, -5, -3, -1, 1, 3, 5, \dots\}\}$

§04 Der Satz von Lagrange

§04.01 **Definition.** 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

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

□

§04.02 **Bemerkung.** Sei G eine Gruppe, $a \in G$. Dann gilt

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

§04.03 **Beweis.** Übungsaufgabe

□

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

1. Je zwei Äquivalenzklassen sind gleichmächtig
2. Je zwei Äquivalenzklassen sind disjunkt oder gleich
3. G ist die disjunkte Vereinigung der Äquivalenzklassen

§04.05 **Beweis.** 1. Es genügt für $a \in G$ bel zu zeigen, dass $\#[a] = \#[e]$. Dafür betrachten wir $f: H \rightarrow aH, h \mapsto ah$. f ist injektiv, denn seien $h_1, h_2 \in H$ mit $f(h_1) = f(h_2)$ dann gilt

$$ah_1 = f(h_1) = f(h_2) = ah_2 \stackrel{9}{\implies} h_1 = h_2$$

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

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

$$b = f(h)$$

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

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

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

2. folgt da \sim -Äquivalenzrelation

3. folgt da \sim -Äquivalenzrelation

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

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

§04.07 **Beweis.** Wir schreiben zunächst

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

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

$$G = \dot{\bigcup}_{i=1, \dots, n} [a_i] \quad \text{Lemma 23iii}$$

und damit folgt

$$\#G = \# \left(\dot{\bigcup}_{i=1, \dots, n} [a_i] \right) = \sum_{i=1}^n \#[a_i] \stackrel{23}{=} \sum_{i=1}^n \#[e] = n \cdot \#[e] = (G : H) \cdot \#H$$

□

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

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

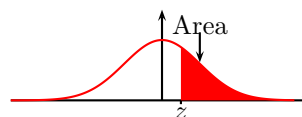
§05 Übungsaufgaben

§06 Lösungen zu den Übungsaufgaben

Anhang

A.1 Normalverteilung

Figure 1: Normal Curve Areas. Standard normal probability in right-hand tail. For negative values of z , areas are found by symmetry.



z	Second decimal place of z									
	0	.01	.02	.03	.04	.05	.06	.07	.08	.09
0.0	.5000	.4960	.4920	.4880	.4840	.4801	.4761	.4721	.4681	.4641
0.1	.4602	.4562	.4522	.4483	.4443	.4404	.4364	.4325	.4286	.4247
0.2	.4207	.4168	.4129	.4090	.4052	.4013	.3974	.3936	.3897	.3859
0.3	.3821	.3783	.3745	.3707	.3669	.3632	.3594	.3557	.3520	.3483
0.4	.3446	.3409	.3372	.3336	.3300	.3264	.3228	.3192	.3156	.3121
0.5	.3085	.3050	.3015	.2981	.2946	.2912	.2877	.2843	.2810	.2776
0.6	.2743	.2709	.2676	.2643	.2611	.2578	.2546	.2514	.2483	.2451
0.7	.2420	.2389	.2358	.2327	.2296	.2266	.2236	.2206	.2177	.2148
0.8	.2119	.2090	.2061	.2033	.2005	.1977	.1949	.1922	.1894	.1867
0.9	.1841	.1814	.1788	.1762	.1736	.1711	.1685	.1660	.1635	.1611
1.0	.1587	.1562	.1539	.1515	.1492	.1469	.1446	.1423	.1401	.1379
1.1	.1357	.1335	.1314	.1292	.1271	.1251	.1230	.1210	.1190	.1170
1.2	.1151	.1131	.1112	.1093	.1075	.1056	.1038	.1020	.1003	.0985
1.3	.0968	.0951	.0934	.0918	.0901	.0885	.0869	.0853	.0838	.0823
1.4	.0808	.0793	.0778	.0764	.0749	.0735	.0721	.0708	.0694	.0681
1.5	.0668	.0655	.0643	.0630	.0618	.0606	.0594	.0582	.0571	.0559
1.6	.0548	.0537	.0526	.0516	.0505	.0495	.0485	.0475	.0465	.0455
1.7	.0446	.0436	.0427	.0418	.0409	.0401	.0392	.0384	.0375	.0367
1.8	.0359	.0351	.0344	.0336	.0329	.0322	.0314	.0307	.0301	.0294
1.9	.0287	.0281	.0274	.0268	.0262	.0256	.0250	.0244	.0239	.0233
2.0	.0228	.0222	.0217	.0212	.0207	.0202	.0197	.0192	.0188	.0183
2.1	.0179	.0174	.0170	.0166	.0162	.0158	.0154	.0150	.0146	.0143
2.2	.0139	.0136	.0132	.0129	.0125	.0122	.0119	.0116	.0113	.0110
2.3	.0107	.0104	.0102	.0099	.0096	.0094	.0091	.0089	.0087	.0084
2.4	.0082	.0080	.0078	.0075	.0073	.0071	.0069	.0068	.0066	.0064
2.5	.0062	.0060	.0059	.0057	.0055	.0054	.0052	.0051	.0049	.0048
2.6	.0047	.0045	.0044	.0043	.0041	.0040	.0039	.0038	.0037	.0036
2.7	.0035	.0034	.0033	.0032	.0031	.0030	.0029	.0028	.0027	.0026
2.8	.0026	.0025	.0024	.0023	.0023	.0022	.0021	.0021	.0020	.0019
2.9	.0019	.0018	.0018	.0017	.0016	.0016	.0015	.0015	.0014	.0014
3.0	.00135									
3.5	.000 233									
4.0	.000 031 7									
4.5	.000 003 40									
5.0	.000 000 287									

