

Algebra 1 WS23/24

Yousef Khell

October 28, 2023

1 Gruppen und Monoide

Notation.

- $\mathbb{N} = \{1, 2, \dots\}$
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
- $\#X$ = die Kardinalität/Mächtigkeit einer Menge X

Definition 1 (Monoid). Ein Tripel (M, e, \circ) mit

- M einer Menge.
- e einem Element aus M ,
- $\circ : M \times M \rightarrow M$ einer zweistelligen Verknüpfung

heißt **Monoid** falls gilt

(M1) Assoziativität:

$$\forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$$

(M2) Neutrales Element:

$$\forall a \in M : a \circ e = a = e \circ a$$

Wir nennen ein $a \in M$ **invertierbar**, falls

$$\exists b, b' \in M : b \circ a = e = a \circ b'$$

(b bzw. b' heißen dann Links- bzw. Rechtsinverse)

Bemerkung. $b = b'$, denn

$$b' = e \circ b' = (b \circ a) \circ b' = b \circ (a \circ b') = b \circ e = b$$

Definition 2 (Gruppe). Eine **Gruppe** ist ein Monoid, in dem alle Elemente invertierbar sind.

Bemerkung 3 (zur Assoziativität). Seien $a_1, \dots, a_n \in M$, und setzt man in

$$a_1 \circ \dots \circ a_n$$

Klammern, sodass \circ jeweils 2 Elemente verknüpft, so ist wegen (M1) das Ergebnis unabhängig von der Wahl der Klammerung, and also lässt man i.a. die Klammern weg. (Die Reihenfolge ist aber schon wichtig!)

Definition 4 (Abelsche Gruppe/Monoid). Ein Monoid bzw. eine Gruppe M heißt **abelsch** (oder kommutativ) : $\iff \forall a, b \in M :$

$$a \circ b = b \circ a$$

Proposition 5 (Eindeutigkeit des neutralen Elements bzw. der neutralen Elementen). *Sei M ein Monoid, dann*

(a) *Erfüllt $e' \in M$ die Bedingung $e' \circ a = a \forall a \in M$, so gilt $e' = e$.*

(b) *Ist $a \in M$ invertierbar, so ist sein Inverses eindeutig.*

Beweis.

(a) Nach Konstruktion $e = e' \circ e = e'$.

(b) Gelte $a \circ b' = e$ und b sei ein Inverses von a , dann:

$$b' = e \circ b' = (b \circ a) \circ b' = b \circ (a \circ b') = b \circ e = b.$$

□

Satz 6 (ohne Beweis). *Sei (G, e, \circ) ein Tripel mit G eine Menge, $e \in G$, $\circ : G \times G \rightarrow G$ eine assoziative Verknüpfung sodass:*

- *e ist Linkseins, d.h.*

$$\forall g \in G : e \circ g = g$$

- *jedes g hat ein Linksinverses*

$$\forall g \in G \exists h \in G : h \circ g = e$$

So ist (G, e, \circ) eine Gruppe.

Hinweis (Nutzen von Satz 6). Es müssen weniger Axiome geprüft werden.

Notation.

(i) $ab := a \circ b$

(ii) $a^0 = e, a^1 = a, a^{n+1} = a^n a, n \in \mathbb{N}$

(iii) $a^n = (a^{-n})^{-1}, n < 0$

(iv) Ist \circ kommutativ, so schreibt man oft $+$

Übung (Rechenregeln).

(i) $a^n a^m = a^{n+m}, (a^n)^m = a^{nm}, \forall m, n \in \mathbb{N}_0$

(ii) Ist a invertierbar, so gelten die Regeln $\forall n, m \in \mathbb{Z}$

Proposition 7 (Übung). *Sei G eine Gruppe, seien $g, h \in G$, dann:*

(a) *Die Gleichung $xg = h$ besitzt genau eine Lösung (in G), nämlich $x = hg^{-1}$.*

(b) *Es gilt $(gh)^{-1} = h^{-1}g^{-1}$*

(c) *Die Rechtstranslation (um g) $r_g : G \rightarrow G, x \mapsto xg$ und die Linkstranslationen (um g) $\ell_g : G \rightarrow G, x \mapsto gx$ sind bijektiv.*

Beispiel. 1) $(\mathbb{N}_0, 0, +)$, $(\mathbb{N}_0, 1, \cdot)$ sind kommutative Monoide.

2) Jede Gruppe ist ein Monoid.

3) Ist X eine Menge, $\text{Abb}(X, X)$ bzw. $\text{Bij}(X, X)$ die Menge aller Abbildungen bzw. Bijektionen von X in sich, so gilt:

(a) $(\text{Abb}(X, X), \text{id}_X, \circ)$ ist ein Monoid.

(b) $(\text{Bij}(X, X), \text{id}_X, \circ)$ ist eine Gruppe.

Schreibe $S_n := \text{Bij}(\{1, \dots, n\}, \{1, \dots, n\})$ für die Gruppe der Permutationen von $\{1, \dots, n\}$.

4) Ist $(V, \langle \cdot, \cdot \rangle)$ ein Euklidischer Raum, so sind

(i) $O(V) := \{\varphi \in \text{End}_{\mathbb{R}}(V) \mid \varphi \text{ orthogonal}\}$ und $SO(V) := \{\varphi \in O(V) \mid \det(\varphi) = 1\}$ Gruppen.

(ii) Ist $V = \mathbb{R}^2$ und $P_n := \{\cos \frac{2\pi j}{n}, \sin \frac{2\pi j}{n} \mid j = 0, \dots, n-1\}$, dann ist

(a) $C_n := \{\varphi \in SO(V) \mid \varphi(P_n) = P\}$ die Gruppe der Drehungen um 0 von Winkel $\frac{2\pi j}{n}$, ($j = 0, \dots, n-1$) und

(b) $D_n := \{\varphi \in O(V) \mid \varphi(P_n) = P\}$ die [[Diedergruppe]] der Ordnung $2n$

(Übung) $\#C_n = n, \#D_n = 2n$.

Gruppen beschreiben oft Symmetrien eines geometrischen Objekts.

5) Ist M ein Monoid, so ist $M^\times := \{a \in M \mid a \text{ invertierbar}\}$ eine Gruppe, also (M^\times, e, \circ) .

Definition 8 (Ring). Ein [[Ring]] ist ein [[Tupel]] $(R, 0, 1, +, \cdot)$, sodass

(R1) $(R, 0, +)$ eine [[abelsche Gruppe]],

(R2) $(R, 1, \cdot)$ ein Monoid,

(R3) Es gelten die Distributivgesetze

Definition 9 (Ordnung einer Gruppe). Ist M ein Monoid oder eine Gruppe, so heißt

$$\text{ord}(M) := \#M$$

die Ordnung von M .

Definition 10 (Untermonoid/Untergruppe). Seien M ein Monoid, G eine Gruppe, dann

(a) $N \subseteq M$ heißt Untermonoid (UM) wenn:

- $e \in N$
- $\forall n, n' \in N : n \circ n' \in N$

(b) $H \subseteq G$ heißt Untergruppe (UG) wenn:

- $e \in H$
- $\forall h, h' \in H : h \circ h' \in H$

So schreiben wir $N \leq M, H \leq G$.

Übung 11. (i) $N \leq M \implies (N, e, \cdot |_{N \times N}: N \times N \rightarrow N)$ ist Monoid

(ii) $H \leq G \implies (H, e, \cdot |_{H \times H}: H \times H \rightarrow H)$ ist Monoid

Beispiel. Sei K ein Körper, dann ist

(i) $SL_n(K) \leq GL_n(K)$

(ii) $SO(V) \leq O(V) \leq \text{Aut}_{\mathbb{R}}(V)$

Proposition 12 (Übung). Sind $(H_i)_{i \in I}$ Untergruppen von G , so ist

$$\bigcap_{i \in I} H_i \leq G.$$

Beispiel. Sei G eine Gruppe, $g \in G, S \leq G$, dann:

(i) $C_G(g)$ **Zentralisator** von $g \in G$, also

$$C_G(g) = \{h \in G \mid hg = gh\} \leq G$$

(ii) $C_G(S)$ **Zentralisator** von S , also

$$C_G(S) = \{h \in G \mid hs = sh \forall s \in S\} = \bigcap_{s \in S} C_G(s) \leq G$$

(iii) $Z(G)$ **Zentrum** von G , also

$$Z(G) = C_G(G) \underset{\text{komm.}}{\leq} G$$

(iv) (Übung) $Z(GL_n(K)) = K^\times \mathbf{1}_n$

Lemma 13. Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge, dann \exists kleinste Untergruppe $\langle S \rangle \leq G$, die S umfasst.

Beweis. Definiere

$$\langle S \rangle := \bigcap \{H \leq G \mid S \subseteq H\}.$$

□

Übung 14. Sei M ein Monoid, $S \subseteq M$ eine Teilmenge, ein Wort aus S ist ein Ausdruck

$$s_1 \cdot \dots \cdot s_n, s_i \in S, n \in \mathbb{N}$$

Dann gilt: $\{\text{Worte in } S \cup \{e\}\} = \langle S \rangle \leq M$ ist das kleinste Untermonoid von M , das S umfasst. Und ist G eine Gruppe, so gilt $\{\text{Worte in } S \cup S^{-1} \cup \{e\}\} = \langle S \rangle \leq G$ ist die kleinste Untergruppe von G , die S umfasst.

Definition 15 (Erzeugendensystem). Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. S heißt Erzeugendensystem von $G \iff \langle S \rangle = G$.

Beispiel (Übung). Seien $E_{ij} \in M_{n \times n}(K)$ die Elementarmatrizen mit 1 an der Stelle (i, j) und 0 sonst. Dann ist

$$\{1_n + aE_{ij} \mid a \in K, i, j \in \{1, \dots, n\}, i \neq j\}$$

ein Erzeugendensystem von $SL_n(K)$ (Gauß-Algorithmus)

Lemma 16. Sei G eine Gruppe, $g \in G$, dann gilt

$$\langle g \rangle = \langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Beweis. (Nach Übung 14)

$$\begin{aligned} \langle \{g\} \rangle &= \{\text{Worte in } \{g, g^{-1}, e\}\} \\ &= \{g^{i_1}, \dots, g^{i_n} \mid n \in \mathbb{N}, i_1, \dots, i_n \in \{0, \pm 1\}\} \\ &= \{g^{i_1 + \dots + i_n} \mid n \in \mathbb{N}, i_1, \dots, i_n \in \{0, \pm 1\}\} \\ &= \{g^n \mid n \in \mathbb{Z}\} \end{aligned}$$

□

Bemerkung. $\langle g \rangle$ ist abelsch.

Definition 17 (Ordnung eines Gruppenelements, Zyklische Gruppe).

Sei G eine Gruppe, $g \in G$

(a) Die Ordnung von g ist

$$\text{ord}(g) = \#\langle g \rangle = \#\{g^n \mid n \in \mathbb{Z}\} \in \mathbb{N} \cup \{\infty\}$$

(b) g hat endliche Ordnung $\iff \text{ord}(g) \in \mathbb{N}$

(c) G ist zyklisch $\iff \exists g \in G : G = \langle g \rangle$

Proposition 18. Zyklische Gruppen sind abelsch.

Beweis. G zyklisch $\implies \exists g \in G : G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Dann:

$$g^n g^m = g^{n+m} \stackrel{+ \text{ komm. in } \mathbb{Z}}{=} g^{m+n} = g^m g^n.$$

□

Proposition 19. Sei G eine Gruppe, $g \in G, n := \text{ord}(g)$ und

$$n' = \sup\{m \in \mathbb{N} \mid e, g, g^2, \dots, g^{m-1} \text{ paarw. versch.}\}$$

Dann gelten:

(a) $n' = \infty = \sup \mathbb{N}$ oder $g^{n'} = e$ und $\langle g \rangle = \{e, g, g^2, \dots, g^{n'-1}\}$. Insbesondere ist $n' = n$

(b) Falls $n = \text{ord}(g) < \infty$, so gilt für $m, m' \in \mathbb{Z}$:

$$g^m = g^{m'} \iff m \equiv m' \pmod{n}$$

Insbesondere ist $g^m = e \iff n \mid m$

(c) Für $s \in \mathbb{Z}$ gilt

$$\text{ord}(g^s) = \frac{n}{\text{ggT}(n, s)}$$

Beweis.

(a) Gelte $n' < \infty$:

Definition von $n' \implies g^{n'} \in \{e, g, \dots, g^{n'-1}\}$ Annahme: $g^{n'} = g^i$ für ein $i \in \{1, \dots, n'-1\}$ Multipliziere mit $g^{-i} \implies g^{n'-i} = g^0 = e$ und $0 < n'-i < n'$, d.h. $g^{n'-i} \in \{e, \dots, g^{n'-1}\} \implies \{g^0, \dots, g^{n'-1}\}$ nicht paarweise verschieden (Widerspruch) Sei schließlich $m \in \mathbb{Z}$ beliebig, Division mit Rest:

$$m = qn' + r : q, r \in \mathbb{Z}, 0 \leq r \leq n' - 1$$

$$\implies g^m = g^{qn'+r} = (g^{n'})^q g^r = g^r \in \{g^0, \dots, g^{n'-1}\}$$

Also: $\langle g \rangle = \{e, \dots, g^{n'-1}\}$ sind paarweise verschieden. $\implies \text{ord}(g) = \#\langle g \rangle = n'$

(b) Seien $m, m' \in \mathbb{Z}$, schreibe $m' - m = qn' + r$, ($q, r \in \mathbb{Z}, 0 \leq r \leq n' - 1$), dann:

$$g^{m'} = g^m \iff g^{m'-m} = g^0 = e \iff g^{qn'+r} = e$$

$$\iff g = e \quad \begin{matrix} 1. \xleftrightarrow{n=n'} \\ e, \dots, g^{n-1} \text{ paarw. versch.} \end{matrix} \quad r = 0$$

$$\iff m' - m \text{ ist Vielfaches von } n = n' \iff m \equiv m' \pmod{n}$$

(c) Bestime die $m \in \mathbb{Z}$ mit $(g^s)^m = e$

$$(g^s)^m = e \iff g^{sm} = e \iff n \mid sm$$

$$\iff \frac{n}{\text{ggT}(n, s)} \mid \frac{s}{\text{ggT}(n, s)} m \iff \frac{n}{\text{ggT}(n, s)} \mid m$$

Da $\frac{n}{\text{ggT}(n, s)}, \frac{s}{\text{ggT}(n, s)}$ teilerfremd sind

$$\xleftrightarrow{2.} \text{ord}(g^s) = \frac{n}{\text{ggT}(n, s)} \quad \square.$$

□

Beispiel.

$$\text{ord}(g) = 6 \implies \text{ord}(g^2) = 3 = 6/\text{ggT}(6, 2) = 6/2$$

Korollar 20. Sei G eine Gruppe, dann

(a) Für $g \in G$ gilt:

$$\text{ord}(g) = \infty \iff g^n, n \in \mathbb{Z} \text{ sind paarw. verschieden}$$

(b) Ist G zyklisch und $H \leq G$ eine Untergruppe, so ist H zyklisch.

Beweis.

(a) \Leftarrow vgl. 19(a) \implies wissen nach 19(a), dass e, g, \dots, g^n, \dots paarw. versch. sind. Multipliziere mit g^{-m} , ($m \in \mathbb{N}$) $\implies g^{-m}, g^{-m+1}, \dots, g^0, g^1, \dots$ sind paarw. versch.

- (b) Sei $g \in G$ ein Erzeuger von $G, H \leq G$ eine UG von G und ohne Einschränkung $H \supsetneq \{e\}$

$$\implies \exists m \in \mathbb{Z} \setminus \{0\} : g^m \in H \setminus \{e\}$$

$$H \text{ ist Gruppe} \implies g^m, (g^m)^{-1} = g^{-m} \in H$$

Sei $t \in \min\{m \in \mathbb{N} \mid g^m \in H\}$. Behauptung: $\langle g^t \rangle = H$.

- “ \subseteq ”: Klar, da $g^t \in H$ also auch $\langle g^t \rangle \subseteq H$ (H ist UG die t enthält)
- “ \supseteq ”: Sei $g^m \in H$, Division mit Rest: $m = tq + r : q, r \in \mathbb{Z}, 0 \leq r \leq t-1$

$$\implies H \ni g^m = g^{tq+r} = \underbrace{(g^t)^q}_{\in H} g^r \implies g^r = (g^m)((g^t)^q)^{-1} \in H$$

Nach Def von t muss gelten: $r = 0$, da $r = 1, \dots, t-1$ verboten. Also ist $g^m = (g^t)^q \in \langle g^t \rangle$. □

Korollar 21 (Übung). Untergruppen von \mathbb{Z} sind die Mengen $\mathbb{Z}n = \{an \mid a \in \mathbb{Z}\}, (n \in \mathbb{N}_0)$

Wiederholung (Vorbereitung).

- Äquivalenzrelationen
- Äquivalenzklassen
- Repräsentantensysteme

Bemerkung.

- $X = \bigsqcup_{r \in \mathcal{R}} [r]_{\sim}$
- Falls $\#X < \infty : \# = \sum_{r \in \mathcal{R}} \#[r]_{\sim}$

Satz 22 (Satz von Lagrange). Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe, dann gilt $\#H \mid \#G$.

Beweis.

- 1) Definiere \sim auf G durch $g \sim g' : \iff \exists h \in H : g' = gh \sim$ ist eine Äquivalenzrelation:

- reflexiv: $g \sim g$ denn $g = ge, e \in H$
- symmetrisch: gelte $g' = gh$ für ein $h \in H$

$$\xRightarrow{_{-h^{-1}}} g' h^{-1} = g \xRightarrow{H \text{ Gruppe}} h^{-1} \in H \implies g' \sim g$$

- transitiv: gelte $g \sim g', g' \sim g''$, d.h. $\exists h \in H : g' = gh, \exists h' \in H : g'' = g'h$

$$\implies g'' = g'h' = (gh)h' = g(hh') \implies g \sim g''$$

- 2) Äquivalenzklassen: Für $g \in G$ ist

$$[g]_{\sim} = \{g' \in G \mid \exists h \in H : g' = gh\} = \{gh \mid h \in H\} =: gH$$

- 3) Beachte G endlich $\implies H \subseteq G$ endlich (und ebenso jede Teilmenge von G)
 Behauptung: $\#gH = \#H \forall g \in G$ Grund: Die Abbildungen

$$\ell_g : H \rightarrow gH, h \mapsto gh, \ell_{g^{-1}} : gH \rightarrow H, x \mapsto g^{-1}x$$

sind zueinander invers (Übung) und also bijektiv. $\implies \#H = \#gH$.

- 4) Sei $\mathcal{R} \subseteq G$ ein Repräsentantensystem zu \sim

$$\begin{aligned} \implies \#G &= \sum_{g \in \mathcal{R}} \#[g]_{\sim} = \sum_{g \in \mathcal{R}} \#gH = \sum_{g \in \mathcal{R}} \#H \stackrel{3)}{=} \#\mathcal{R} \#H \\ \implies \#H &\text{ teilt } \#G. \end{aligned} \quad \square$$

Notation. Seien G eine Gruppe, $H \leq G$ eine Untergruppe und \sim wie im Beweis vom Satz 22.

- Schreibe G/H für die Menge aller Äquivalenzklassen also für $\{gH \mid g \in G\}$
- Schreibe $[G : H] := \#G/H = \#\mathcal{R}$ (Index von H in G)

Lagrange sagt: $\#G = \#G/H \cdot \#H = [G : H] \cdot \#H$

Übung 23. Seien $H' \leq H \leq G$ Untergruppen, dann ist $H' \leq G$ und

$$[G : H'] = [G : H] \cdot [H : H']$$

Korollar 24. Sei G eine endliche Gruppe, dann gelten:

- (a) $\forall g \in G : \text{ord}(g) \mid \text{ord}(G) = \#G$
 (b) Ist $\text{ord}(G)$ eine Primzahl, so ist G zyklisch

Beweis.

- (a) $\langle g \rangle \leq G$ ist eine Untergruppe $\xRightarrow{\text{Lagrange}} \text{ord}(g) = \#\langle g \rangle \mid \#G = \text{ord}(G)$

- (b) Sei $p = \text{ord}(G) \in \mathbb{P}$ eine Primzahl, sei $g \in G \setminus \{e\}$ ($\#G \geq 2$) Nach 1. gilt
 $\underbrace{\text{ord}(g)}_{\neq 1 \text{ da } g \neq e} \mid \text{ord}(G) = p$

Folglich: $p = \text{ord}(g) = \text{ord}(G)$, d.h. $\langle g \rangle \leq G$ ist Inklusion gleichmächtiger endlicher Mengen, also $\langle g \rangle = G$. \square

Definition 25 (Gruppenexponent). Sei G eine Gruppe, der Exponent von G ist $\exp(G) = \min\{n \in \mathbb{N} \mid \forall g \in G : g^n = e\}$ (wobei $\min \emptyset = \infty$).

Beispiel (Übung).

- (i) $\exp(C_n) = n$
- (ii) $\exp D_n = \text{kgV}(2, n)$
- (iii) $\exp(S_3) = 6$
- (iv) $\exp(S_4) = 12$
- (v) $\exp(G) = 2 \implies G$ abelsch

- (vi) \mathbb{F}_p Körper mit p Elementen und $0 \neq V$ ein \mathbb{F}_p -[[Vektorraum]], so gilt $\exp(V, 0, +) = p$

Satz 26. Sei G eine endliche Gruppe, es gelten

- (a) $\exp(G) \mid \text{card}(G)$
 (b) $\exp(G) = \text{kgV}(\{\text{ord}(g) \mid g \in G\})$

Beweis.

- (a) Folgt aus (b) und $\text{ord}(g) \mid \text{ord}(G) \forall g \in G$ nach Korollar 24.
 (b) $\text{ord}(g) \mid \exp(G), \forall g \in G$, denn nach Definition gilt:

$$g^{\exp(G)} = e \xrightarrow[19]{\implies} \text{ord}(g) \mid \exp(G)$$

folglich: $N := \text{kgV}(\{\text{ord}(g) \mid g \in G\})$ teilt $\exp G$.

Behauptung: $\exp G \leq N$, (dann fertig)

Wir zeigen: $g^N = e \implies \exp G \leq N$. Dies folgt aus $g^{\text{ord}(g)} = e$ und $\text{ord}(g) \mid N = \text{kgV}(\dots)$. \square

Übung 27. Sei G eine endliche Gruppe, dann gelten:

- (a) Sind $g, h \in G : gh = hg$ und gilt $\text{ggT}(\text{ord}(g), \text{ord}(h)) = 1$, so gilt

$$\text{ord}(gh) = \text{ord}(g)\text{ord}(h)$$

- (b) Gelte $p^f \mid \exp G$ für p eine Primzahl und $f \in \mathbb{N}$, dann $\exists g \in G : \text{ord}(g) = p^f$
 (c) Ist G abelsch, so $\exists g \in G : \exp(G) = \text{ord}(g)$

Satz 28. Sei G eine endliche abelsche Gruppe, dann ist G genau dann zyklisch, wenn $\text{ord}(G) = \exp(G)$

Beweis.

- “ \implies ”: Sei $g \in G$ Erzeuger $\xrightarrow[19]{\implies} \text{ord}(G) = \text{ord}(g)$

$$\text{ord}(g) \mid \exp G, \exp G \mid \text{ord}(G) \implies \exp G = \text{ord}(G)$$

- “ \impliedby ”: Wähle nach 27.3 ein $g \in G$ mit $\text{ord}(g) = \exp(G)$, nach Voraussetzung ist $\exp(G) = \text{ord}(g) \implies \text{ord}(g) = \text{ord}(G) \implies \langle g \rangle \subseteq G$ ist Gleichheit, d.h. $\langle g \rangle = G$. \square

2 Gruppenhomomorphismen

Seien im Weiteren M, M' Monoide und G, G' Gruppen.

Definition 29 (Monoid-/Gruppenhomomorphismus).

- (a) Eine Abbildung $\varphi : M \rightarrow M'$ heißt **Monoidhomomorphismus**, falls

- (i) $\varphi(e) = e'$ und

$$(ii) \quad \forall m, \tilde{m} \in M : \varphi(m \circ \tilde{m}) = \varphi(m) \circ' \varphi(\tilde{m})$$

(b) Sind M, M' Gruppen, so heißt ein Gruppenhomomorphismus \iff (ii) gilt.

Bemerkung 30.

- (a) Ist $\varphi : M \rightarrow M'$ ein Gruppenhomomorphismus, so gilt $\varphi(e) = e'$ und $\varphi(m^{-1}) = \varphi(m)^{-1}, \forall m \in M$.
- (b) (Übung) Die Verkettung von Monoid- bzw. Gruppenhomomorphismen ist wieder ein solcher.

Beweis. Zu (a):

$$e' \circ' \varphi(e) = \varphi(e) = \varphi(e \circ e) = \varphi(e) \circ' \varphi(e)$$

Kürzen $\implies e' = \varphi(e)$. Und

$$\varphi(m^{-1}) \circ' \varphi(m) = \varphi(m^{-1} \circ m) = \varphi(e) = e'$$

Eindeutigkeit des Inverses $\implies \varphi(m^{-1}) = \varphi(m)^{-1}$. □

Beispiel 31. (a) Für $g \in G$ ist die Abbildung

$$\varphi : \mathbb{Z} \rightarrow G, n \mapsto g^n$$

ein Gruppenhomomorphismus mit $\text{Bild}(\varphi) = \langle g \rangle$.

- (b) Sei K ein Körper, V, W K -Vektorräume, $\varphi : V \rightarrow W$ ein Vektorraumhomomorphismus, dann ist

$$\varphi : (V, 0_V, +_V) \rightarrow (W, 0_W, +_W)$$

ein Gruppenhomomorphismus.

- (c) Die Vorzeichenfunktion (Aus der linearen Algebra)

$$\text{sgn} : S_n \rightarrow \{\pm 1\}, \sigma \mapsto \text{sgn}(\sigma)$$

ist ein Gruppenhomomorphismus.

Definition 32 (Kern/Bild). Sei $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus.

- (a) Der Kern von φ ist $\text{Kern}(\varphi) := \{g \in G \mid \varphi(g) = e'\}$
- (b) Das Bild von φ ist $\text{Bild}(\varphi) := \{\varphi(g) \in G' \mid g \in G\}$

Proposition 33 (Übung). Sei $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus, dann

- (a) Für $H \leq G$ eine Untergruppe ist $\varphi(H) \leq G'$ eine Untergruppe.
- (b) Für $H' \leq G'$ eine Untergruppe ist $\varphi^{-1}(H') \leq G$ eine Untergruppe.
Insbesondere sind $\text{Bild}(\varphi) \leq G', \text{Kern}(\varphi) \leq G$ Untergruppen.
- (c) φ ist injektiv (ein Gruppenmonomorphismus) $\iff \text{Kern}(\varphi) = \{e\}$.
- (d) φ ist surjektiv (ein Gruppenepimorphismus) $\iff \text{Bild}(\varphi) = G'$

Bemerkung. (a), (b) und (d) gelten auch für Monoide.

Definition 34 (Gruppenisomorphismus). Ein Gruppenhomomorphismus φ ist ein Gruppenisomorphismus, wenn φ bijektiv ist. ($\iff \text{Kern}(\varphi) = \{e\}$ und $\text{Bild}(\varphi) = G'$).

Bemerkung (Übung). Definiere ein Monoidhomomorphismus analog zu Definition 24.

Notation. Wir schreiben $G \cong G'$ (G ist isomorph zu G') wenn \exists Gruppenisomorphismus $\varphi : G \rightarrow G'$.

Definition 35 (Gruppenautomorphismus). (a) Ein Gruppenisomorphismus $\varphi : G \rightarrow G$ heißt Gruppenautomorphismus.

(b) $\text{Aut}(G) := \{\varphi : G \rightarrow G \mid \varphi \text{ ist ein Gruppenautomorphismus}\}.$

Bemerkung 36 (Übung). (a) $\text{id}_G : G \rightarrow G \in \text{Aut}(G)$

(b) Verkettung von Gruppenisomorphismen (oder Automorphismen) ist wieder ein solcher.

(c) Ist $\varphi : G \rightarrow G'$ ein Gruppenisomorphismus, so gelten

(i) $\#G = \#G'.$

(ii) G abelsch $\iff G'$ abelsch.

(iii) $S \subseteq G$ ein Erzeugendensystem $\iff \varphi(S) \subseteq G'$ ein Erzeugendensystem.

Proposition 37. $(\text{Aut}(G), \text{id}_G, \circ)$ und $(\text{Aut}(M), \text{id}_M, \circ)$ sind Gruppen.

Beweis. (Übung) Zeige:

$$\text{Aut}(G) \leq \text{Bij}(G), \text{Aut}(M) \leq \text{Bij}(M)$$

sind Untergruppen. □

Beispiel 38 (Übung).

(a) $\text{Aut}((\mathbb{Z}, 0, +)) = \{\text{id}_{\mathbb{Z}}, -\text{id}_{\mathbb{Z}}\} \cong C_2$

(b) Für $\mathbb{Z}_n := \mathbb{Z}/(n)$ der Ring der Restklassen modulo n gilt

$$(\mathbb{Z}_n, \bar{0}, +) \cong C_n \text{ und } \text{Aut}(\mathbb{Z}_n, \bar{0}, +) \cong \mathbb{Z}_n^\times$$

z.B. Erzeuger von \mathbb{Z}_n sind Reste \bar{a} , sodass $\text{ggT}(a, n) = 1$

(c) Sei G beliebig, zu $g \in G$ definiere den **Konjugationsautomorphismus** (**Konjugation** mit g)

$$c_g : G \rightarrow G, h \mapsto g \circ h \circ g^{-1}$$

(i) $c_g \circ c_{g'} = c_{g \circ g'}, \forall g, g' \in G$

(ii) $c_e = \text{id}_G$ und $c_g \in \text{Aut}(G), \forall g \in G$

(iii) $c : G \rightarrow \text{Aut}(G), g \mapsto c_g$ ist ein Gruppenhomomorphismus.

(iv) $\text{Kern}(c.) = Z(G)$ (Zentrum von G).

Bemerkung. $\text{Bild}(c.) =: \text{Inn}(G)$ die Gruppe der **inneren Automorphismen** von G

Lemma 39. Seien $\varphi, \varphi' : G \rightarrow G'$ Gruppenhomomorphismen. Sei $S \subseteq G$ ein Erzeugendensystem. Dann gilt

$$\varphi(s) = \varphi'(s) \forall s \in S \iff \varphi = \varphi' \quad (*)$$

Analoge Aussage gilt für Monoide

Beweisskizze. (Übung)

- “ \Leftarrow ”: Klar.
- “ \Rightarrow ”:
 1) Zeige $H := \{g \in G \mid \varphi(g) = \varphi'(g)\} \leq G$ ist eine Untergruppe.
 2) Da $S \subseteq H$ nach Definition von H und Voraussetzung von “ \Rightarrow ”, folgt
 $G = \langle S \rangle \subseteq H \leq G$

□

Normalteiler (Normal Subgroup)

Notation. Für $X \subseteq G$ und $g \in G$ setze

$$\ell_g(X) = \{gx \mid x \in X\} = gX \text{ und } r_g(X) = \{xg \mid x \in X\} = Xg$$

Gruppenverknüpfung assoziativ \implies

$$(i) \quad c_g(X) = \{g x g^{-1} \mid x \in X\} = (gX)g^{-1} = g(Xg^{-1}).$$

$$(ii) \quad g(hX) = (gh)X \text{ und } (Xg)h = X(gh).$$

Bemerkung. Ist $H \leq G$ eine Untergruppe, dann heißt gH **Linksnebenklasse** und Hg **Rechtsnebenklasse**.

Definition 40 (Normalteiler). Eine Untergruppe $N \leq G$ heißt Normalteiler (N.T.) $\iff \forall g \in G : Ng = gN$. (Diese Definition ist auch für Monoide sinnvoll)

Lemma 41. Für eine Untergruppe $N \leq G$ sind äquivalent:

$$(i) \quad \forall g \in G : gN = Ng$$

$$(ii) \quad \forall g \in G : gNg^{-1} = N$$

$$(iii) \quad \forall g \in G : gNg^{-1} \subseteq N$$

Beweis. • “(ii) \implies (iii)”: Klar.

- “(iii) \implies (i)”: Rechtsmultiplikation mit g liefert aus (iii):

$$(gNg^{-1})g = gN(g^{-1}g) = gNe = gN \subseteq Ng$$

Für die andere Inklusion betrachte (iii) für g^{-1} :

$$g^{-1}Ng \subseteq N \xRightarrow{\text{Linksmult. mit } g} Ng \subseteq gN$$

- “(i) \implies (ii)”: Wende auf (i) Rechtsmultiplikation mit g^{-1} an. ($r_{g^{-1}} : G \rightarrow G$ ist eine bijektive Abbildung.)

□

Notation.

$H \leq G$ bedeutet $H \subseteq G$ ist eine Untergruppe.

$H \trianglelefteq G$ bedeutet $H \subseteq G$ ist ein Normalteiler.

Satz 42. Ist $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus, so ist $\text{Kern}(\varphi) \trianglelefteq G$ ein Normalteiler.

Beweis. Sei $g \in G$ beliebig, zu zeigen ist $g \circ \text{Kern}(\varphi) \circ g^{-1} \subseteq \text{Kern}(\varphi)$

Sei $h \in \text{Kern}(\varphi)$, zu zeigen ist $ghg^{-1} \in \text{Kern}(\varphi)$. Damit:

$$\begin{aligned} \varphi(ghg^{-1}) &= \varphi(g)\varphi(h)\varphi(g^{-1}) \underset{h \in \text{Kern}(\varphi)}{=} \varphi(g) \circ e' \circ \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) \\ &= \varphi(gg^{-1}) = \varphi(e) = e'. \end{aligned}$$

$$\implies \text{Kern}(\varphi) \trianglelefteq G.$$

□

Übung 43.

- Ist $N' \trianglelefteq G'$ und $\varphi : G \rightarrow G'$ Gruppenhomomorphismus, so gilt $\varphi^{-1}(N') \trianglelefteq G$.
- Ist $h \leq G$ eine Untergruppe mit $[G : H] = \#G/H = 2$, so folgt $H \trianglelefteq G$.
- Ist G abelsch, so ist jede Untergruppe $H \leq G$ ein Normalteiler.
- Der **Kommutator** zu $g, h \in G$ ist $ghg^{-1}h^{-1}$, die **Kommutatoruntergruppe** von G ist

$$[G, G] := \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle$$

Es gilt $[G, G] \trianglelefteq G$.

Beispiel. Es gibt Beispiele für folgende Aussagen:

- $\exists H \leq G : H \not\trianglelefteq G$
- $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $\varphi(G) \not\trianglelefteq G'$
- $\exists N \trianglelefteq G$ und $H \trianglelefteq N$, so dass $H \not\trianglelefteq G$.

Beweis.

- (i) $G = S_3 = \text{Bij}(\{1, 2, 3\}) \supseteq H = \{\text{id}, \sigma\}$ mit $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Dann
 $H \leq G$ Klar, aber $H \not\trianglelefteq G$, denn für $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ gilt $\tau\sigma\tau^{-1}$ (Übung)
 $\implies \tau H \tau^{-1} \not\subseteq H$
- (ii) Betrachte $\varphi : H \rightarrow G$ Inklusion mit G, H aus (i), dann gilt $H \trianglelefteq H$ aber
 $\varphi(H) = H$ kein Nullteiler von $G = S_3$.
- (iii) Später. □

Satz 44. Sei $N \trianglelefteq G$ ein Nullteiler, dann gelten:

- (a) Aus $gN = g'N$ und $hN = h'N$ für $g, g', h, h' \in G$ folgt $ghN = g'h'N$ und insbesondere ist die Verknüpfung

$$\circ : \underbrace{G/N}_{\{gN \mid g \in G\}} \times G/N \longrightarrow G/N, (gN, hN) \mapsto gN \circ hN = ghN$$

wohl-definiert.

- (b) $G/N, \underbrace{N}_{=eN}, \circ$ ist eine Gruppe.

- (c) $gN = g'N \iff g^{-1}g' \in N$.

- (d) $\pi : G \rightarrow G/N, g \mapsto gN$ ist ein Gruppenhomomorphismus mit $\text{Kern}(\pi) = N$.

Beweis. (a) Es gelten (Formeln von Definition 40)

$$\begin{aligned} (gh)N &= g(hN) \stackrel{N \trianglelefteq G}{=} g(Nh) = (gN)h \\ &= (g'N)h = g'(Nh) = g'(hN) = g'(h'N) = (g'h')N \implies (a) \end{aligned}$$

- (b) Überlege Gruppenaxiome.

- Assoziativität (Übung)
- Linkseins ist $N = eN$, denn

$$N \circ (gN) = eN \circ gN \stackrel{\text{wohl-def.}}{=} (e \circ g)N = gN$$

- Linksinverses zu gN ist $g^{-1}N$, denn

$$(g^{-1}N) \circ gN \stackrel{\text{nach Def.}}{=} (g^{-1}g)N \stackrel{\text{Gruppe}}{=} eN = N$$

- (c) $gN = g'N \stackrel{g^{-1} \circ_-}{=} N = g^{-1}g'N \stackrel{e \in N}{\implies} N \ni g^{-1}g'e$, d.h. $g^{-1}g' \in G$.

$$g^{-1}g' \in N \stackrel{\ell_{g^{-1}g'} : N \rightarrow N \text{ ist bijektiv.}}{\implies} N = g^{-1}N \stackrel{g^{-1} \circ_-}{\implies} gN = g'N$$

(d) $\pi : G \rightarrow G/N, g \mapsto gN$ ist Gruppenhomomorphismus, denn

$$\pi(gg') = gg'N \stackrel{\text{Def. von } \circ}{=} gN \circ g'N = \pi(g) \circ \pi(g')$$

$$g \in \text{Kern}(\pi) \iff gN = eN \stackrel{(c)}{\iff} e^{-1}g = g \in N$$

□

Bemerkung (Bezeichnung). G/N (bzw. $(G/N, eN, \circ)$) heißt **Faktorgruppe** von G modulo N .

Bemerkung (Übung). G abelsch $\implies G/N$ abelsch.

Satz 45 (Homomorphiesatz für Gruppen). Sei $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus mit $N = \text{Kern}(\varphi)$, dann existiert genau ein Gruppenhomomorphismus $\bar{\varphi} : G/N \rightarrow G'$, sodass

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ G/N & & \end{array}$$

kommutiert, d.h. $\bar{\varphi} \circ \pi = \varphi$. (wobei $\pi : G \rightarrow G/N, g \mapsto gN$ aus Satz 44). Die Abbildung $\bar{\varphi}$ ist injektiv und $\bar{\varphi}$ bijektiv $\iff \varphi$ surjektiv.

Beweis. • Existenz von $\bar{\varphi}$: Definiere $\bar{\varphi}(gN) = \varphi(g), \forall g \in G$.

- $\bar{\varphi}$ wohl-definiert: Es gilt: $gN = g'N \iff N = g^{-1}g'N \stackrel{44c}{\iff} g^{-1}g' \in N$.
Damit

$$\implies \varphi(g') = \varphi(gg^{-1}g') = \varphi(g)\varphi(\underbrace{g^{-1} \circ g'}_{\in N = \text{Kern}(\varphi)}) = \varphi(g)e = \varphi(g).$$

- $\bar{\varphi}$ Gruppenhomomorphismus:

$$\begin{aligned} \bar{\varphi}(gN \circ g'N) &\stackrel{\text{Def. von } \circ}{=} \bar{\varphi}(gg'N) \stackrel{\text{Def. von } \bar{\varphi}}{=} \varphi(gg') \stackrel{\varphi \text{ Hom.}}{=} \varphi(g)\varphi(g') \\ &\stackrel{\text{Def. von } \bar{\varphi}}{=} \bar{\varphi}(gN)\bar{\varphi}(g'N). \end{aligned}$$

- $\bar{\varphi} \circ \pi = \varphi$: (Aus der Definition von $\bar{\varphi}$):

$$\underbrace{\bar{\varphi}(gN)}_{\bar{\varphi}(\pi(g))} = \varphi(g)$$

- $\bar{\varphi}$ injektiv: $\bar{\varphi}(gN) = e \iff \varphi(g) = e \iff g \in N = \text{Kern}(\varphi) \stackrel{44c}{\iff} gN = eN = N$.
- $\bar{\varphi}$ eindeutig: Folgt aus der Surjektivität von π .
- Zusatz φ surjektiv $\iff \bar{\varphi}$ Isomorphismus (Übung): Verwende $\text{Bild}(\varphi) = \text{Bild}(\bar{\varphi})$ und $\bar{\varphi}$ injektiv.

□

Satz 45' (Homomorphiesatz'). (Übung) Ist $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus und $N \trianglelefteq G$, so dass $N \subseteq \text{Kern}(\varphi)$, dann existiert genau ein Gruppenhomomorphismus

$$\bar{\varphi} : G/N \longrightarrow G' \text{ mit } \bar{\varphi} \circ \pi = \varphi.$$

wobei $\pi : G \rightarrow G/N, g \mapsto gN$

Notation. Für $n \in \mathbb{N}$ sei $\mathbb{Z}_n = \mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ der Restklassenring. ($n\mathbb{Z} \subseteq \mathbb{Z}$ eine Untergruppe)

Korollar 46. Sei G eine zyklische Gruppe,

(a) Falls $m := \text{ord}(G) \in \mathbb{N} \implies G \cong \mathbb{Z}_m = \mathbb{Z}/(m)$.

(b) Falls $\text{ord}(G) = \infty \implies G \cong \mathbb{Z}$.

Beweis. Sei $g \in G$ ein Erzeuger und betrachte

$$\varphi : \mathbb{Z} \rightarrow G, n \mapsto g^n$$

φ ist surjektiv, da $\text{Bild}(\varphi) = \langle g^n \mid n \in \mathbb{Z} \rangle = G$.

$$\xRightarrow[\text{Satz 45}]{} \bar{\varphi} : \mathbb{Z}/\mathbb{Z}m \xrightarrow{\cong} G$$

für $m \in \mathbb{N}_0$, so dass $\text{Kern}(\varphi) = \mathbb{Z}m$.

- Fall (b): $\text{ord}(G) = \infty \implies \text{Kern}(\varphi) = \{0\} \implies \varphi : \mathbb{Z} \rightarrow G$ ist ein Isomorphismus.
- Fall (a): $\text{ord}(G) = m \in \mathbb{N}$ dann ist $\bar{\varphi}$ der gewünschte Isomorphismus.

□

Korollar 47. Für zyklische Gruppen G, H gilt $G = H \iff \#G = \#H$

Übung. (a) $G/[G, G]$ ist eine abelsche Gruppe.

(b) Für $N \trianglelefteq G$ gilt:

$$G/N \text{ abelsch} \iff [G, G] \leq N$$

Einschub: Faktorringe

Definition 48 (Ideal). Sei R ein kommutativer Ring. $I \subseteq R$ heißt Ideal wenn

- I ist Untergruppe von $(R, 0, +)$
- $RI := \{ri \mid r \in R, i \in I\} \subseteq I$

Beispiel. 1) $\mathbb{Z}n \subseteq \mathbb{Z}$ ist ein Ideal $\forall n \in \mathbb{Z}$.

2) $Ra \subseteq R$ für $a \in R$ ist ein Ideal von R .

Satz 49. Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal, und $R/I = \{r+I \mid r \in R\}$ die Nebenklassenmenge von R modulo I (für die Gruppe $(R, 0, +)$). Dann:

(a) Die Verknüpfungen

$$+ : R/I \times R/I \longrightarrow R/I, (r+I, s+I) \longmapsto (r+s)+I$$

$$\cdot : R/I \times R/I \longrightarrow R/I, (r+I, s+I) \longmapsto rs+I$$

sind wohl-definiert auf R/I

(b) $(R/I, \bar{0}, \bar{1}, +, \cdot)$ ist ein kommutativer Ring ($\bar{r} := r+I$ Notation für die Klasse von r) der Restklassenring von R modulo I .

(c) $\pi : R \longrightarrow R/I, r \longmapsto r+I$ ist ein surjektiver Ringhomomorphismus.

Beweis. (a) “+” wohl-definiert folgt aus Satz 44. ($I \subseteq (R, 0, +)$ Ideal!)

“ \cdot ” wohl-definiert: Gelte $a+I = a'+I$ und $b+I = b'+I$.

$$\implies a'b'+I = ab+aj+bi+ij+I = ab+I$$

(b) (Übung)

(c) Wie in 45 (d)

□

Die Isomorphiesätze

Satz 50 (Erster Isomorphiesatz). Sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $H \leq G$ eine Untergruppe, dann gelten:

(a) $HN = \{hn \mid h \in H, n \in N\} \subseteq G$ ist eine Untergruppe.

(b) $H \cap N \subseteq H$ ist ein Normalteiler (und (Übung) $N \trianglelefteq HN$)

(c) Die folgende Abbildung ist wohl-definiert und ein Gruppenisomorphismus

$$H/H \cap N \longrightarrow HN/N, h(H \cap N) \longmapsto hN$$

Beweis. (a) Seien $hn, h'n' \in HN$, dann:

$$(h'n')(hn)^{-1} = h' \underbrace{n'n^{-1}h^{-1}}_{\substack{\in Nh^{-1} \\ N \trianglelefteq G} = h^{-1}N} = h'h^{-1}\tilde{n} \stackrel{H \text{ U.G.}}{=} (h'h^{-1})\tilde{n} \in HN$$

und $e = ee = HN$

(b) Zu zeigen: für $h \in H$ gilt $h(H \cap N)h^{-1} \subseteq H \cap N$

Dazu:

$$\begin{aligned} h(H \cap N)h^{-1} &\subseteq hHh^{-1} = H \\ h(H \cap N)h^{-1} &\subseteq hNh^{-1} \stackrel{N \trianglelefteq G}{=} N \implies h(H \cap N)h^{-1} \subseteq H \cap N. \end{aligned}$$

□