Algebra 1 WS23/24

Yousef Khell

October 28, 2023

1 Gruppen und Monoide

Notation.

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

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

- M einer Menge.
- e einem Element aus M,
- $\circ : M \times M \to M$ 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 $a_1, ..., a_n \in M$, und setzt man in

$$a_1 \circ \cdots \circ a_n$$

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:

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

$\square$

Satz 6 (ohne Beweis)**.** *Sei $(G, e, \circ)$ ein Tripel mit G eine Menge, $e \in G$, $\circ : G \times G \to G$ 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) $a^0 = e, a^1 = a, a^{n+1} = a^n a, n \in N$

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

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

(c) Die Rechtstranslation (um g) $r_g : G \to G, x \mapsto xg$ und die Linkstranslationen (um g) $\ell_g : G \to G, x \mapsto gx$ 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, $\mathrm{Abb}(X, X)$ bzw. $\mathrm{Bij}(X, X)$ die Menge aller Abbildungen bzw. Bijektionen von X in sich, so gilt:

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

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

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

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

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

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

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

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

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 $N \leqslant M, H \leqslant G$.

Übung 11. (i) $N \leqslant M \implies (N, e, \cdot|_{N\times N} \colon N \times N \to N)$ ist Monoid

(ii) $H \leqslant G \implies (H, e, \cdot|_{H\times H} \colon H \times H \to H)$ ist Monoid

Beispiel. Sei K ein Körper, dann ist

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

(ii) $SO(V) \leqslant O(V) \leqslant \mathrm{Aut}_{\mathbb{R}}(V)$

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

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

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

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

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

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

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

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

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

(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 $\langle S\rangle \leqslant G$, die S umfasst.*

Beweis. Definiere

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

□

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

$$s_1 \cdot \cdots \cdot s_n, s_i \in S, n \in N$$

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

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

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)

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

□

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

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

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

(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:

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

□

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

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

Dann gelten:

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

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

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

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

(c) Für $s \in \mathbb{Z}$ gilt

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

Beweis.

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

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

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

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

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

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

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

$$\iff g = e \underset{e,...,g^{n-1}\text{paarw. versch.}}{\overset{1.\ n=n'}{\iff}} r = 0$$

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

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

$$(g^s)^m = e \iff g^{sm} \underset{2.}{=} e \iff n \mid sm$$

$$\underset{\operatorname{ggT}(n,s)|n,s}{\iff} \frac{n}{\operatorname{ggT}(n,s)} \mid \frac{s}{\operatorname{ggT}(n,s)} m \iff \frac{n}{\operatorname{ggT}(n,s)} \mid m$$

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

$$\overset{2.}{\iff} \operatorname{ord}(g^s) = \frac{n}{\operatorname{ggT}(n,s)} \quad \square.$$

□

Beispiel.

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

Korollar 20. *Sei G eine Gruppe, dann*

(a) Für $g \in G$ gilt:

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

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

Beweis.

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

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

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

H 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: $m = tq + r : q, r \in \mathbb{Z}, 0 \leqslant r \leqslant t-1$

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

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

$\square$

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 $H \leqslant G$ 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 $h \in H$

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

   - 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

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

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

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

$\implies \#G = \sum_{g \in \mathcal{R}} \#[g]_\sim = \sum_{g \in \mathcal{R}} \#gH = \sum_{g \in \mathcal{R}} \#H \overset{3)}{=} \#\mathcal{R}\#H$
$\implies \#H$ teilt $\#G$. □

Notation. Seien G eine Gruppe, $H \leqslant G$ 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 $H' \leqslant H \leqslant G$ Untergruppen, dann ist $H' \leqslant G$ und

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

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

(a) $\forall g \in G : \mathrm{ord}(g) \mid \mathrm{ord}(G) = \#G$

(b) Ist $\mathrm{ord}(G)$ *eine Primzahl, so ist G zyklisch*

Beweis.

(a) $\langle g \rangle \leqslant G$ ist eine Untergruppe $\underset{\text{Lagrange}}{\implies} \mathrm{ord}(g) = \#\langle g \rangle \mid \#G = \mathrm{ord}(G)$

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

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

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 $\min \varnothing = \infty$).

Beispiel (Übung)**.**

(i) $\exp(C_n) = n$

(ii) $\exp D_n = \mathrm{kgV}(2, n)$

(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) $\exp(G) \mid \mathrm{card}(G)$

(b) $\exp(G) = \mathrm{kgV}(\{\mathrm{ord}(g) \mid g \in G\})$

Beweis.

(a) Folgt aus (b) und $\mathrm{ord}(g) \mid \mathrm{ord}(G) \forall g \in G$ nach Korollar 24.

(b) $\mathrm{ord}(g) \mid \exp(G), \forall g \in G$, denn nach Definition gilt:

$$g^{\exp(G)} = e \underset{19}{\Longrightarrow} \mathrm{ord}(g) \mid \exp(G)$$

folglich: $N := \mathrm{kgV}(\{\mathrm{ord}(g) \mid g \in G\})$ teilt $\exp G$.
Behauptung: $\exp G \leqslant N$, (dann fertig)
Wir zeigen: $g^N = e \implies \exp G \leqslant N$. Dies folgt aus $g^{\mathrm{ord}(g)} = e$ und $\mathrm{ord}(g) \mid N = \mathrm{kgV}(...)$. □

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

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

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

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

(c) Ist G abelsch, so $\exists g \in G : \exp(G) = \mathrm{ord}(g)$

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

Beweis.

- “ $\Longrightarrow$ ”: Sei $g \in G$ Erzeuger $\underset{19}{\Longrightarrow}$ $\mathrm{ord}(G) = \mathrm{ord}(g)$

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

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

□

2 Gruppenhomomorphismen

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

Definition 29 (Monoid-/Gruppenhomomorphismus).

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

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

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

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

Bemerkung 30.

(a) Ist $\varphi : M \to M'$ 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 $\implies \varphi(m^{-1}) = \varphi(m)^{-1}$. $\square$

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

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

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

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

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

ein Gruppenhomomorphismus.

(c) Die Vorzeichenfunktion (Aus der linearen Algebra)

$$\mathrm{sgn} : S_n \to \{\pm 1\}, \sigma \mapsto \mathrm{sgn}(\sigma)$$

ist ein Gruppenhomomorphismus.

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

(a) Der Kern von φ ist $\mathrm{Kern}(\varphi) := \{g \in G \mid \varphi(g) = e'\}$

(b) Das Bild von φ ist $\mathrm{Bild}(\varphi) := \{\varphi(g) \in G' \mid g \in G\}$

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

(a) Für $H \leqslant G$ eine Untergruppe ist $\varphi(G) \leqslant G'$ eine Untergruppe.

(b) Für $H' \leqslant G'$ eine Untergruppe ist $\varphi^{-1}(H') \leqslant G$ eine Untergruppe.
Insbesondere sind $\mathrm{Bild}(\varphi) \leqslant G', \mathrm{Kern}(\varphi) \leqslant G$ Untergruppen.

(c) φ ist injektiv (ein Gruppenmonomorphismus) $\iff \mathrm{Kern}(\varphi) = \{e\}$.

(d) φ ist surjektiv (ein Gruppenepimorphismus) $\iff \mathrm{Bild}(\varphi) = G'$

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

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

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

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

Bemerkung 36 (Übung)**.** (a) $\mathrm{id}_G : G \to G \in \mathrm{Aut}(G)$

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

(c) Ist $\varphi : G \to G'$ 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. $(\mathrm{Aut}(G), \mathrm{id}_G, \circ)$ *und* $(\mathrm{Aut}(M), \mathrm{id}_M, \circ)$ *sind Gruppen.*

Beweis. (Übung) Zeige:

$$\mathrm{Aut}(G) \leqslant \mathrm{Bij}(G), \mathrm{Aut}(M) \leqslant \mathrm{Bij}(M)$$

sind Untergruppen. □

Beispiel 38 (Übung)**.**

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

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

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

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

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

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

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

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

   (iii) $c_\cdot : G \to \mathrm{Aut}(G), g \mapsto c_g$ ist ein Gruppenhomomorphismus.

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

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

Lemma 39. *Seien $\varphi, \varphi' : G \to G'$ 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)

- " $\Longleftarrow$ ": Klar.
- " $\Longrightarrow$ ":
    1) Zeige $H := \{g \in G \mid \varphi(g) = \varphi'(g)\} i \leqslant G$ ist eine Untergruppe.
    2) Da $S \subseteq$ nach Definition von H und Voraussetzung von " $\Longrightarrow$ ", folgt $G = \langle S \rangle \subseteq H \leqslant G$

□

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 assoziaativ $\Longrightarrow$

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

(ii) $g(hX) = (gh)X$ und $(Xg)h = X(gh)$.

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

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

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

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

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

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

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}:

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

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

$\square$

Notation.
$H \leqslant G$ bedeuteg $H \subseteq G$ ist eine Untergruppe.
$H \trianglelefteq G$ bedeuteg $H \subseteq G$ ist ein Normailteiler.

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

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

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) \underset{h \in \mathrm{Kern}(\varphi)}{=} \varphi(g) \circ e' \circ \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1})$$

$$= \varphi(gg^{-1}) = \varphi(e) = e'.$$

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

Übung 43.

(a) Ist $N' \trianglelefteq G'$ und $\varphi : G \to G'$ Gruppenhomomorphismus, so gilt $\varphi^{-1}(N') \trianglelefteq G$.

(b) Ist $h \leqslant G$ eine Untergruppe mit $[G : H] = \# {}^{G}\!/\!_{H} = 2$, so folgt $H \trianglelefteq G$.

(c) Ist G abelsch, so ist jede Untergruppe $H \leqslant G$ ein Normalteiler.

(d) 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:

(i) $\exists H \leqslant G : H \ntrianglelefteq G$

(ii) $\varphi : G \to G'$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $\varphi(G) \ntrianglelefteq G'$

(iii) $\exists N \trianglelefteq G$ und $H \trianglelefteq N$, so dass $H \ntrianglelefteq G$.

Beweis.

(i) $G = S_3 = \mathrm{Bij}(\{1,2,3\}) \supseteq H = \{\mathrm{id}, \sigma\}$ mit $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Dann $H \leqslant G$ Klar, aber $H \ntrianglelefteq G$, denn für $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ gilt $\tau\sigma\tau^{-1}$ (Übung) $\Longrightarrow$ $\tau H \tau^{-1} \nsubseteq H$

(ii) Betrachte $\varphi : H \to G$ Inklusion mit G, H aus (i), dann gilt $H \trianglelefteq H$ aber $\varphi(H) = H$ nein Nullteiler von $G = S_3$.

(iii) Später.

$\square$

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

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

wohl-definiert.

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

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

(d) $\pi : G \to G/N, g \mapsto gN$ ist ein Gruppenhomomorphismus mit $\mathrm{Kern}(\pi) =$ *N.*

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

$$(gh)N = g(hN) \overset{N \trianglelefteq G}{=} g(Nh) = (gN)h$$
$$= (g'N)h = g'(Nh) = g'(hN) = g'(h'N) = (g'h')N \Longrightarrow (a)$$

(b) Überlege Gruppenaxiome.

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

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

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

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

(c) $gN = g'N \underset{g^{-1}\circ\_}{=} N = g^{-1}g'N \underset{e \in N}{\Longrightarrow} N \ni g^{-1}g'e$, d.h. $g^{-1}g' \in G$.

$$g^{-1}g' \in N \underset{\substack{\ell_{g^{-1}g'} : N \to N \\ \text{ist bijektiv.}}}{\Longrightarrow} N = g^{-1}N \underset{g^{-1}\circ\_}{\Longrightarrow} gN = g'N$$

(d) $\pi : G \to {}^{G}\!/_{N}, g \mapsto gN$ ist Gruppenhomomorphismus, denn

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

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

□

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 $\varphi : G \to G'$ ein Gruppenhomomorphismus mit $N = \mathrm{Kern}(\varphi)$, dann existiert genau ein Gruppenhomomorphismus $\overline{\varphi} : {}^{G}\!/_{N} \longrightarrow G'$, sodass*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\ {}^{G}\!/_{N} \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

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

Beweis.

- Existenz von $\overline{\varphi}$: Definiere $\overline{\varphi}(gN) = \varphi(g), \forall g \in G$.
- $\overline{\varphi}$ wohl-definiert: Es gilt: $gN = g'N \iff N = g^{-1}g'N \underset{44c}{\iff} g^{-1}g' \in N$. Damit

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

- $\overline{\varphi}$ Gruppenhomomorphismus:

$$\overline{\varphi}(gN \circ g'N) \underset{\text{Def. von } \circ}{=} \overline{\varphi}(gg'N) \underset{\text{Def. von } \overline{\varphi}}{=} \varphi(gg') \underset{\varphi \text{ Hom.}}{=} \varphi(g)\varphi(g')$$

$$\underset{\text{Def. von } \overline{\varphi}}{=} \overline{\varphi}(gN)\overline{\varphi}(g'N).$$

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

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

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

□

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

$$\overline{\varphi} : {}^{G}\!/_{N} \longrightarrow G' \text{ mit } \overline{\varphi} \circ \pi = \varphi.$$

wobei $\pi : G \to {}^{G}\!/_{N}, g \mapsto gN$

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 $m := \mathrm{ord}(G) \in \mathbb{N} \implies G \cong \mathbb{Z}_m = {}^{\mathbb{Z}}\!/_{(m)}$.

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

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

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

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

$$\underset{\text{Satz 45}}{\Longrightarrow} \overline{\varphi} : {}^{\mathbb{Z}}\!/_{\mathbb{Z}m} \xrightarrow{\cong} G$$

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

- Fall (b): $\mathrm{ord}(G) = \infty \implies \mathrm{Kern}(\varphi) = \{0\} \implies \varphi : \mathbb{Z} \to G$ ist ein Isomorphismus.
- Fall (a): $\mathrm{ord}(G) = m \in \mathbb{N}$ dann ist $\overline{\varphi}$ 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:

$$ {}^{G}\!/_{N} \text{ abelsch} \iff [G,G] \leqslant N$$

Einschub: Faktorringe

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

(i) I ist Untergruppe von $(R, 0, +)$

(ii) $RI := \{ri \mid r \in R, i \in I\} \subseteq I$

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) $(R/_I, \overline{0}, \overline{1}, +, \cdot)$ *ist ein kommutativer Ring* ($\overline{r} := r + I$ *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!)

"·" wohl-definiert: Gelte $a + I = a' + I$ und $b + I = b' + I$.

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

(b) (Übung)

(c) Wie in 45 (d)

□

Die Isomorphiesätze

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

(a) $HN = \{hn \mid h \in H, n \in N\} \subseteq G$ *ist ein 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:

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

und $e = ee = HN$

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

Dazu:

$$\begin{matrix} h(H \cap N)h^{-1} \subseteq hHh^{-1} = H \\ h(H \cap N)h^{-1} \subseteq hNh^{-1} \underset{N \trianglelefteq G}{=} N \end{matrix} \Longrightarrow h(H \cap N)h^{-1} \subseteq H \cap N.$$

(c) Betrachte die Verkettung von Gruppenhomomorphismen

$$\varphi : H \xrightarrow[h \longmapsto h]{\text{Inklusion}} HN \xrightarrow[x \longmapsto xN]{} HN/N$$

dann ist φ ein Gruppenautomorphismus.

φ ist surjektiv: Jede Klasse in HN/N ist von der Form

$$hnN = \underbrace{hN}_{=\varphi(h)}$$

für ein $h \in H$. Nach Homomorphiesatz: nur noch zu zeigen $\mathrm{Kern}(\varphi) = H \cap N$: für $h \in H$:

$$h \in \mathrm{Kern}(\varphi) \iff \varphi(h) = eN \iff hN = eN \underset{44(c)}{\Longrightarrow} h \in N \underset{h \in H}{\Longrightarrow} h \in N \cap H$$

Umgekehrt: $h \in N \cap H \implies h \in N \implies hN = eN = N$.

$\square$

Satz 51 (**Zweiter Isomorphiesatz**). *Sei G eine Gruppe und $N \trianglelefteq G$ ein Normailteiler, und sei $\pi : G \longrightarrow G/N, g \longmapsto \overline{g} = gN$ die Faktorabbildung.*

(a) Sei $X := \{H \leqslant G \mid N \subseteq H\}$, und sei $\overline{X} := \left\{\overline{H} \leqslant G/N\right\}$, dann ist die Abbildung

$$\psi : X \longrightarrow \overline{X}, H \longmapsto \pi(H) = H/N =: \overline{H}$$

eine Bijektion mit inverser Abbildung

$$\nu : \overline{X} \longrightarrow X, \overline{H} \longmapsto \pi^{-1}(\overline{H}).$$

Dabei gilt:

$$X \ni H \trianglelefteq G \iff \overline{X} \ni \pi(H) \trianglelefteq G/N$$

(b) Ist $H \in X$ ein Normalteiler von G, so ist

$$G/H \longrightarrow \left(G/N\right)/\left(H/N\right), g \longmapsto \underbrace{\overline{g}}_{gN}\,\underbrace{\overline{H}}_{\pi(H)}$$

wohl-definiert und ein Gruppenisomorphismus.

Beweis. (a) Nach Proposition 33 sind ψ und ν wohl-definiert.

- $\nu \circ \psi = \mathrm{id}_X$: Sei $H \leqslant G$ mit $N \subseteq H$, zu zeigen ist $\pi^{-1}(\pi(H)) = H$. Es gilt:

$$g \in \pi^{-1}(\pi(H)) \iff \pi(g) \in \pi(H) \iff gN \in \bigcup_{h \in H} hN$$

$$\iff \exists h \in H : gN = hN \underset{44(c)}{\Longrightarrow} h^{-1}g \in N \subseteq H \implies g \in hH = H.$$

(“ $\Longleftarrow$ ” klar: $g \in H \implies g \in \pi^{-1}(\pi(H))$).

- $\psi \circ \nu = \mathrm{id}_{\overline{X}}$: Für $\overline{H} \in \overline{X}$ (d.h. $\overline{H} \leqslant {}^{G}\!\diagup_{N}$) ist zu zeigen $\pi(\pi^{-1}(\overline{H})) = \overline{H}$. Dies gilt, denn π ist surjektiv.
- Schließlich: Sei $H \in X$, zu zeigen ist $H \trianglelefteq G \iff \pi(H) \trianglelefteq {}^{G}\!\diagup_{N}$

$$H \trianglelefteq G \iff \forall g \in G : gHg^{-1} \subseteq H$$

$$\underset{\pi:G\to\overline{G}\text{ surj.}}{\Longrightarrow} \forall \overline{g} \in {}^{G}\!\diagup_{N} : \overline{g}\pi(H)\overline{g} \subseteq \pi(H) \implies \pi(H) \trianglelefteq \overline{G}$$

Umgekehrt: Falls $\pi(H) \trianglelefteq\trianglelefteq \overline{G}$ und $g \in G$:

$$\pi(gHg^{-1}) = \overline{g}\pi(H)\overline{g}^{-1} \leqslant \pi(H)$$

$$\implies gHg^{-1} \subseteq \pi^{-1}(\pi(gHg^{-1})) \subseteq \pi^{-1}(\pi(H)) \underset{\nu\circ\psi=\mathrm{id}_X}{=} H$$

(b) Sei $H \trianglelefteq G$ ein Normalteiler mit $N \subseteq H$, so dass nach (a)

$$\overline{H} = \underbrace{{}^{H}\!\diagup_{N}}_{\pi(H)} \trianglelefteq \underbrace{{}^{G}\!\diagup_{N}}_{\pi(G)}$$

ein Normalteiler ist. Betrachte den verketteten Gruppenautomorphismus

$$\varphi : G \xrightarrow[g\longmapsto gN]{\pi} {}^{G}\!\diagup_{N} \xrightarrow[\overline{g}\longmapsto \overline{g}\overline{H}]{\pi'} {}^{\left({}^{G}\!\diagup_{N}\right)}\!\diagup_{\left({}^{H}\!\diagup_{N}\right)}$$

π, π' sind surjektive Gruppenhomomorphismen nach Satz 44(d) $\implies$ die Verkettung φ ist ein surjektiver Gruppenhomomorphismus.

Nach Homomorphiesatz für Gruppen bleibt zu zeigen: $\mathrm{Kern}(\varphi) = H$:

$$g \in \mathrm{Kern}(\varphi) \underset{\pi'(\pi(g))=e}{\iff} \pi(g) \in \mathrm{Kern}(\pi') \iff gN \in {}^{H}\!\diagup_{N}$$

$$\iff gN \subseteq H \underset{N\leqslant H}{\iff} g \in H.$$

□

(Semi-)direkte Produkte

Lemma 52 (Übung)**.** *Seien $(G_1, e_1, \circ_1)$ und $(G_2, e_2, \circ_2)$ Gruppen, dann ist $G = (G_1 \times G_2, (e_1, e_2), \circ)$ eine Gruppe mit*

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 \circ h_1, g_2 \circ h_2)$$

Analog für $k \geqslant 2$ Faktoren. Dabei sind $G_1 \times \{e_2\} \trianglelefteq G$ und $\{e_1\} \times G_2 \trianglelefteq G$ Nullteiler von G.

Definition 53 (**Direktes Produkt**)**.** Die Gruppe G aus Lemma 52 heißt das direkte Produkt von G_1 und G_2, Notation $G_1 \times G_2$.

Beispiel.

$$(\mathbb{R}^n, \underline{0}, +) = (\mathbb{R}, 0, +) \times \cdots \times (\mathbb{R}, 0, +) = \bigtimes_{i=1}^{n} (\mathbb{R}, 0, +)$$

Proposition 54. *Sei G eine Gruppe, seien $N_1, N_2 \trianglelefteq G$ Nullteiler mit $N_1 \cap N_2 = \{e\}$, dann gelten:*

(a) $\forall n_1 \in N_1, n_2 \in N_2 : n_1 n_2 = n_2 n_1$

(b) $N_1 N_2 \trianglelefteq G$ *ist ein Normalteiler in* G

(c) $\psi : N_1 \times N_2 \to N_1 N_2, (n_1, n_2) \mapsto n_1 n_2$ *ist ein Gruppenisomorphismus. (Insbesondere gilt* $\#N_1 N_2 = \#N_1 \# N_2$*)*

Zusatz: Gilt $G = N_1 N_2$*, so folgt* $G \cong N_1 \times N_2$ *via* ψ*.*

Beweis. (a) Seien $n_1 \in N_1, n_2 \in N_2$, setze $x = n_1 n_2 n_1^{-1} n_2^{-1}$. Nun:

$$x = (n_1 n_2 n_1^{-1}) n_2^{-1} \in (n_1 N_2 n_1^{-1}) N_2 \subseteq N_2 N_2 = N_2$$

analog

$$x = n_1 (n_2 n_1^{-1} n_2^{-1}) \in N_1 (n_2 N_1 n_2^{-1}) \overset{N_2 \trianglelefteq G}{\subseteq} N_1 N_1 = N_1$$

damit ist $x \in N_1 \cap N_2 = \{e\} \implies x = e \implies n_1 n_2 = n_2 n_1$.

(b) Für $g \in G$:

$$g N_1 N_2 g^{-1} = g N_1 g^{-1} g N_2 g^{-1} \subseteq N_1 N_2$$

(c) ψ ist wohl-definiert: klar. ψ ein Gruppenhomomorphismus folgt aus (a)

$$\begin{aligned} \psi((n_1, n_2) \circ (n_1', n_2')) &= \psi((n_1 \circ n_1', n_2 \circ n_2')) = n_1 n_1' n_2 n_2' \\ &\underset{(a)}{=} n_1 n_2 n_1' n_2' = \psi(n_1, n_2) \circ \psi(n_1', n_2') \end{aligned}$$

$\{(e, e)\} = \mathrm{Kern}(\psi)$:

$$\begin{aligned} \psi(n_1, n_2) = e \iff n_1 n_2 = e &\iff n_1 = n_2^{-1} \in N_1 \cap N_2 = \{e\} \\ &\iff n_1 = n_2 = e \end{aligned}$$

$\mathrm{Bild}(\psi) = N_1 N_2$.

□

Korollar 55 (Übung)**.** *Sei G eine endliche Gruppe. Seien $N_1, ..., N_k \trianglelefteq G$ Normalteiler von G und gelte:*

(i) $\forall i \neq j : \mathrm{ggT}(\#N_i, \#N_j) = 1$

(ii) $\prod_{j=1}^{k} \#N_j = \#G$

Dann ist

$$\psi : \bigtimes_{j=1}^{k} N_j \longrightarrow G, (n_1, ..., n_k) \longmapsto n_1 \cdot ... \cdot n_k = \prod_{j=1}^{k} n_j$$

ein Gruppenisomorphismus.

Übung. Spezialfall: $n = \prod_{i=1}^{k} p_i^{f_i}$ für $p_1, ..., p_k$ paarweise verschiedene Primzahlen, dann gilt:

$$\bigtimes_{i}^{k} \mathbb{Z} / (p_i^{f_i}) \cong \mathbb{Z} / (n)$$

ist Folge von Korollar 55.