# Einführung in die Algebra
# Wintersemester 2017/18

Luise Puhlmann

24. Oktober 2017

## Inhaltsverzeichnis

9. Oktober 2017

`http://www.math.uni-bonn.de/people/palmer/A1.html`

**Organisatorisches**

- Assistent: Martin Palmer
- Abgabe der Übungsblätter Donnerstag vor der Vorlesung
- Übungsgruppen Beginn nächste Woche
- Literatur siehe Homepage

# 1 Gruppen

## 1.1 Grundlegendes

**Definition 1.** Eine Gruppe ist eine Menge $G$ zusammen mit einer Abbildung

$$\begin{array}{rcl} \circ\colon G \times G & \to & G \\ (g,h) & \mapsto & g \circ h \end{array}$$

(genannt Gruppenoperation), sodass gilt:

(G1) $(a \circ b) \circ c = a \circ (b \circ c) \forall a, b, c \in G$ (Assoziativität)

(G2) $\exists e \in G$ mit $g \circ e = g = e \circ g \forall g \in G$ (Neutrales Element)

(G3) $\forall g \in G \; \exists g^{-1}$ sodass $g \circ g^{-1} = e = g^{-1} \circ g$ (Inverse Elemente)

*Bemerkung.*

- Neutrales Element $e$ ist eindeutig
- Inverse Elemente $g^{-1}$ sind eindeutig
- Es gelten die Kürzungsregeln:

$$\begin{array}{rclr} a \circ c = b \circ c & \Leftrightarrow & a = b & \forall a, b, c \in G \\ c \circ a = c \circ b & \Leftrightarrow & a = b & \forall a, b, c \in G \end{array}$$

**Definition 2.** $(G, \circ)$ heißt abelsch, falls $g \circ h = h \circ g$ für alle $g, h \in G$.

Es reicht sogar zu fordern: Existenz von Linksneutralem und Linksinversem oder Existenz von Rechtsneutralem und Rechtsinversem.

**Beispiel.**

- $(\mathbb{Z}, +)$
- $(K, +, \cdot)$ Körper $\Rightarrow (K, +)$ und $(K^* = K \setminus \{0\}, \cdot)$ sind Gruppen
- $(V, +, \cdot)$ $K$-Vektorraum, dann ist $(V, +)$ eine Gruppe
- $K$ Körper, $n \in \mathbb{N}$; $G = GL_n(K)$ ist Gruppe mit Matrixmultiplikation
- $M$ nichtleere Menge; $S_M := \{f\colon M \to M | f \text{invertierbar}\}$ mit $\circ$ = Komposition von Abbildungen ist eine Gruppe; Spezialfall: $M = \{1, \dots n\}$, $n \in \mathbb{N}$ ergibt die symmetrische Gruppe $S_n$ der Ordnung $n!$.
- Sei $(G, \circ)$ eine Gruppe und $a \in G$ fest gewählt. Dann ist $(G, \circ_a)$ eine Gruppe, wobei $g \circ_a h = g \circ a \circ h$.

**Definition 3.** $(G, \circ)$ Gruppe. Dann ist die Anzahl $|G|$ der Elemente von $G$ die Ordnung von $G$.

**Definition 4.** Sei $(G, \circ)$ Gruppe. Eine Teilmenge $H \subseteq G$ heißt Untergruppe (kurz UG), falls $H \neq \emptyset$ und $h_1, h_2 \in H \Rightarrow h_1 \circ h_2^{-1} \in H$. Wir schreiben dann: $H < (G, \circ)$ oder $H < G$.

*Bemerkung.* $H < (G, \circ)$ gilt genau dann, wenn gilt:

(UG0) $e \in H$

(UG1) $h_1, h_2 \in H \Rightarrow h_1 \circ h_2 \in H$

(UG2) $h \in H \Rightarrow h^{-1} \in H$

Klar: Untergruppen sind Gruppen

**Beispiel** (selber nachprüfen!!!)**.**

- $2\mathbb{Z} < (\mathbb{Z}, +)$
- $n \in \mathbb{N}$; $O(n) = \{A \in GL_n(\mathbb{R}) | AA^T = \mathbb{1}_n\} < GL_n(\mathbb{R})$ die orthogonale Gruppe
- $n \in \mathbb{N}$; $U(n) = \{A \in GL_n(\mathbb{C}) | A\overline{A}^T = \mathbb{1}_n\} < GL_n(\mathbb{C})$ die unitäre Gruppe

- $SL_n(K) = \{A \in GL_n(K) | \det(A) = 1\} < GL_n(K)$
- $SO(n) = O(n) \cap SL_n(\mathbb{R}) < O(n)$
- Spezielle Unitäre Gruppe
- $H(3, \mathbb{R}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\}$: Obere Dreiecksmatrizen, nur 1en auf der Diagonalen (Heisenberggruppe)

**Definition 5.** Sei $(G, \circ)$ eine Gruppe. Sei $\emptyset \neq N \subseteq G$. Dann ist $\langle N \rangle$ die kleinste (bzgl. Inklusion) UG von $G$, die $N$ enthält (also: $H < G$ mit $N \subseteq H \Rightarrow \langle N \rangle \subseteq H$). Wir nennen $\langle N \rangle$ die von $N$ erzeugte UG von $(G, \circ)$.

*Bemerkung.* $\langle N \rangle$ ist wohldefiniert, denn seien $H_1, H_2 < G$ mit $N \subseteq H_1, N \subseteq H_2$, dann $N \subseteq H_1 \cap H_2$ und $H_1 \cap H_2 < G$. Also existiert kleinste Untergruppe, die $N$ enthält; $\langle N \rangle$ ist wohldefiniert.

**Definition 6.** $G$ Gruppe, $N \subseteq G$

1. $N$ erzeugt die Gruppe $G$, falls $\langle N \rangle = G$. In diesem Fall heißt $N$ Erzeugendensystem der Gruppe $G$
2. $(G, \circ)$ heißt endlich erzeugt als Gruppe, falls $\exists N \subseteq G$ mit $|N|$ endlich und $G = \langle N \rangle$.

*Bemerkung.* $(G, \circ)$ Gruppe. $N \subseteq G$, dann gilt: $N$ erzeugt $G$ (also $G = \langle N \rangle$) genau dann, wenn $\forall g \in G : \exists n_1, \ldots, n_r \in G$ (mit $r \in \mathbb{N}_0$), sodass $g = n_1 \circ \cdots \circ n_r$ (mit $g = e$, falls $r = 0$) und $n_i \in N$ oder $n_i^{-1} \in N$ für alle $1 \leq i \leq r$ (*).

*Beweis.* „$\Leftarrow$“: Sei $g \in G$ und $g = n_1 \circ \cdots \circ n_r$ wie in (*). Daraus folgt $g \in \langle N \rangle$, da $n_1, \ldots, n_r \in \langle N \rangle$ und dann auch $g$, weil $\langle N \rangle$ Gruppe. Dadurch ist $G \subseteq \langle N \rangle$, also $G = \langle N \rangle$.
„$\Rightarrow$“: Sei $G = \langle N \rangle$. Behauptung: $H := \{g \in G | g \text{ von der Form (*)}\} < G$. (dkddiermsü)

Da $\langle N \rangle \subseteq H$ nach Definition von $\langle N \rangle$ und Gruppe, muss also $\langle N \rangle = H$ wegen Minimalität, da $N \subseteq H$. Nach Voraussetzung folgt $G = H$. Also hat jedes $g \in G$ die Form (*). □

**Beispiel.**

- $\{\text{Transpositionen}\} \subseteq S_n$, d.h. $(i, j)$ mit $1 \leq i < j \leq n$ erzeugen die Gruppe $S_n$

- $\{\text{Einfache Transpositionen}\} \subseteq S_n$, d.h. $(i,j)$ mit $1 \leq i < j = i+1 \leq n$ erzeugt $S_n$

**Definition 7.** $G$ Gruppe heißt zyklisch, falls $\exists g \in G$, sodass $\langle\{g\}\rangle = G$ (d.h. falls $G$ von einem Element erzeugt wird).

Beachte: $\langle\{g\}\rangle = \{e, g, g^{-1}, g^2, g^{-2}, \dots\} = \{g^i | i \in \mathbb{Z}\}$

**Beispiel.** $(\mathbb{Z}, +)$ ist zyklisch mit $\mathbb{Z} = \langle\{1\}\rangle = \langle\{-1\}\rangle$

**Definition 8.** $(G, \circ)$ und $(G', \circ')$ seien Gruppen. Ein Gruppenhomomorphismus (kurz: Gruppenhomo) von $G$ nach $G'$ ist eine Abbildung $f\colon G \to G'$ mit $f(g \circ h) = f(g) \circ' f(h) \ \forall g, h \in G$.

Er ist ein Gruppenisomorphismus (kurz: Gruppeniso), falls zusätzlich $f$ invertierbar ist. Wir schreiben $(G, \circ) \simeq (G', \circ')$, falls ein Gruppeniso von $G$ nach $G'$ existiert und nennen die Gruppen isomorph.

**Eigenschaften von Gruppenhomomorphismen** $f\colon G \to G'$ von $G$ nach $G'$ sei ein Gruppenhomo. Dann:

(E1) $f$ Gruppeniso $\Leftrightarrow$ $f^{-1}$ Gruppeniso: Nach Definition existiert $f^{-1}$. Zu zeigen: $f^{-1}(g' \circ' h') = f^{-1}(g') \circ f^{-1}(h')$ für alle $g', h' \in G$. Sei $g', h' \in G' \Rightarrow \exists g, h \in G \ f(g) = g', f(h) = h'$. Also: $f^{-1}(g' \circ' h') = f^{-1}(f(g) \circ' f(h)) = f^{-1}(f(g \circ h)) = g \circ h = f^{-1}(g') \circ f^{-1}(h')$

(E2) $f$ bildet Neutrales auf Neutrales ab

12. Oktober 2017

(E3) $f$ bildet Inverse auf Inverse ab

(E4) Sei $(G'', \circ'')$ eine weitere Gruppe; $f'\colon G' \to G''$ Gruppenhomo von $(G', \circ')$ nach $(G'', \circ'')$, dann ist $f' \circ f$ Gruppenhomo. Denn:

$$(f' \circ f)(g \circ h) = f'(f(g \circ h)) = f'(f(g) \circ' f(h)) = (f' \circ f)(g) \circ'' (f' \circ f)(h)$$

**Beispiel** (Gruppenhomos)**.**

1. $(G, \circ)$ mit $\mathrm{id}\colon G \to G, \ g \mapsto g$ Gruppenhomo von $(G, \circ)$ nach $(G, \circ)$

   **Achtung** $\mathrm{id}\colon G \to G, \ g \mapsto g$ ist kein Gruppenhomo von $(G, \circ)$ nach $(G, \circ_a)$, falls $a \neq e$

2. $\det\colon GL_n(K) \to K^*$ für einen Körper $K$ ist ein Gruppenhomo

3. $f\colon \mathbb{R}^* \to \mathbb{R}_{\geq 0},\ x \mapsto |x|$ Gruppenhomo von $(\mathbb{R}^*, \cdot)$ nach $(\mathbb{R}_{\geq 0}, \cdot)$

4. $x \mapsto \exp(x)$ Gruppenhomo von $(\mathbb{Z}, +)$ nach $(\mathbb{R}^*, \cdot)$

5. Betrachte $G = \left\{ \left( \begin{array}{cc} 1 & a \\ 0 & 1 \end{array} \right) \middle| a \in \mathbb{Z} \right\} < GL_n(\mathbb{R}, \cdot)$ und $f\colon \mathbb{Z} \to G,\ a \mapsto \left( \begin{array}{cc} 1 & a \\ 0 & 1 \end{array} \right)$ Gruppenhomo von $(\mathbb{Z}, +)$ nach $(G, \text{Matrixmultiplikation})$.

   Sogar Gruppeniso mit Inversem: $\left( \begin{array}{cc} 1 & a \\ 0 & 1 \end{array} \right) \mapsto a$

6. **Trivialer Gruppenhomo:** Schicke alles auf das neutrale Element

7. Gegeben $(G, \circ)$ Gruppe, $a \in G$. Dann ist $f\colon G \to G,\ g \mapsto g \circ a^{-1}$ ein Gruppenhomo von $(G, \circ)$ nach $(G, \circ_a)$

**Lemma 1.** *Sei $n \in \mathbb{Z}$.*

1. *Dann $\exists!$ Gruppenhomo can: $\mathbb{Z} \to Z/n\mathbb{Z}$ von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}/n\mathbb{Z}, +)$ mit $can(1) = \overline{1}$*

2. *Falls $n \neq 0$, existiert kein nichttrivialer Gruppenhomo $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$*

*Beweis.*

1. **Eindeutigkeit:** Sei $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ Gruppenhomo. Dann $f(0) = \overline{0}$ nach (E2) und falls $f(1) = \overline{1}$, dann gilt $f(n) = f(1 + \ldots 1) = n \cdot f(1)$ für alle $n \in \mathbb{N}$ und damit auch $f(-n) = -nf(1)$ nach (E5) $\Rightarrow f$ eindeutig.

   **Gruppenhomo:** Es gilt dann $\text{can}(x) = \overline{x}$ für alle $x \in \mathbb{Z}$ und da $\text{can}(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \text{can}(x) + \text{can}(y)$ ist das auch ein Gruppenhomomorphismus

2. Sei $n \neq 0$. Sei $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ Gruppenhomo. Sei $f(\overline{1}) = x$. Dann: (ObdA $n \in \mathbb{N}$) $0 = f(0) = f(\overline{n}) = f(\overline{1} + \ldots \overline{1}) = nf(\overline{1}) = nx \Rightarrow x = 0 \Rightarrow f$ trivialer Gruppenhomomorphismus

$\square$

**Lemma 2.** *Sei $(G, \circ)$ eine Gruppe.*

1. *Sei Aut(G) $= \{f\colon G \to G | f$ Gruppeniso von $(G, \circ)$ nach $(G, \circ)\}$. Dann ist Aut(G) Gruppe, die Automorphismengruppen von G*

2. *Betrachte die Abbildung Konj: $G \to$ Aut(G), $g \mapsto$ Konj(g), wobei Konj(g)(h) $= g \circ\ h \circ g^{-1}$ für alle $h \in G$. Dann ist Konj ein Gruppenhomo von G nach Aut(G). (Im Allgemeinen nicht injektiv.)*

*Beweis.* einfach nachrechnen □

*Bemerkung.*

1. Falls $(G, \circ)$ abelsch, dann ist jede Konjugation die Identität

2. $\mathrm{Konj}(g) = \mathrm{id}_G \Leftrightarrow g \in Z(G) := \{x \in G | x \circ y = y \circ x \ \ \forall y \in G\}$

**Konvention:** Von jetzt an schreiben wir meist $gh$ statt $g \circ h$ und $G$ statt $(G, \circ)$.

**Satz 3.** Sei $f\colon G \to G'$ Gruppenhomo. Dann gilt:

$$\begin{array}{llll} \mathrm{Ker}(f) & := \{g \in G | f(g) = e\} & < G & \text{Kern von } f \\ \mathrm{im}(f) & := \{g' \in G' | \exists g \in G \ f(g) = g'\} & < G' & \text{Bild von } f \end{array}$$

*Beweis.* einfach nachrechnen □

**Beispiel.**

1. $\mathrm{Ker}(\mathrm{can}\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z} < \mathbb{Z}$

2. $\mathrm{Ker}(\mathrm{Konj}\colon G \to \mathrm{Aut}(G)) = Z(G) < G$

3. $\mathrm{Ker}(\det\colon GL_n(K) \to K^*) = SL_n(K)$

**Übung:** $f$ Gruppenhomo; $f$ ist injektiv genau dann, wenn $\mathrm{Ker}(f) = \{e\}$

**Satz 4** (Satz von Cayley)**.** Sei $G$ eine Gruppe. Dann ist

$$\begin{array}{rcl} \Phi\colon G & \to & S_G \\ g & \mapsto & \Phi(g) \end{array}$$

mit $\Phi(g)(h) = gh$ für alle $h \in G$ ein injektiver Gruppenhomomorphismus. (Damit kann man $G$ als Untergruppe einer Permutationsgruppe „realisieren“.)

*Beweis.*

Wohldefiniert: $\Phi(g)$ ist invertierbar mit Inversem $h \mapsto g^{-1}h$.

Zu zeigen: $\Phi(g_1 g_2) = \Phi(g_1) \circ \Phi(g_2)$, also $\Phi(g_1 g_2)(h) = \Phi(g_1)(\Phi(g_2)(h))$ für alle $h \in G$. Es gilt aber $\Phi(g_1 g_2)(h) = g_1 g_2 h$ und $\Phi(g_1)(\Phi(g_2)(h)) = \Phi(g_1)(g_2 h) = g_1 g_2 h$ ✓

Injektiv: es reicht zu zeigen, dass der Kern trivial ist. Sei $g \in \mathrm{Ker}\Phi \Leftrightarrow \Phi(g) = e = \mathrm{id}_G \Leftrightarrow \Phi(g)(h) = h \ \ \forall h \in G \Leftrightarrow gh = h \forall h \in G \Leftrightarrow g = e$ ✓ □

## 1.2 Satz von Lagrange und Normalteiler

**Definition 1.** $G$ Gruppe, $H < G$, $a \in G$. Dann ist:

$$aH = \{ah|h \in H\} \subseteq G \text{ Linksnebenklasse von } H \text{ zu } a$$

$$Ha = \{ha|h \in H\} \subseteq G \text{ Rechtsnebenklasse von } H \text{ zu } a$$

Meist arbeiten wir mit Linksnebenklassen und nennen sie einfach Nebenklassen.

Aus der Linearen Algebra wissen wir folgendes:

1. Zwei Nebenklassen sind gleich oder disjunkt d.h. $aH \cap bH \neq \emptyset \Leftrightarrow aH = bH \Leftrightarrow b^{-1}a \in H$

2. Die Abbildung $aH \to H$, $ah \mapsto h$ ist bijektiv $\Rightarrow$ alle Nebenklassen haben dieselbe Kardinalität

3. $$G = \bigcup_{g \in G} gH = \dot{\bigcup_{b \in R}} bH$$

   , wobei $R \subseteq G$, sodass die $bH$ mit $b \in R$ genau ein Repräsentantensystem für die verschiedenen Nebenklassen bilden.

4. $g \in aH \Leftrightarrow g^{-1} \in Ha^{-1}$ (dadurch ergibt sich eine Bijektion zwischen Links- und Rechtsnebenklassen)

**Definition 2.** Bezeichne mit $G/H$ die Menge der Nebenklassen von $G$ bezüglich $H$ und mit $H \backslash G$ die Menge der Rechtsnebenklassen. Dann gilt $|G/H| = |H \backslash G|$ (nach (4)). Wir nennen diese Zahl den Index, auch $(G : H)$, von $H$ in $G$

**Satz 1** (Satz von Lagrange)**.** $G$ Gruppe, $H < G$, $|G| < \infty$. Dann gilt

$$|G| = |H| \cdot (G : H) .$$

Insbesondere: $|G| = p$ Primzahl $\Rightarrow H = \{e\}$ oder $H = G$.

*Beweis.* Formel folgt direkt aus (3), (2) und Definition von Index. Falls nun $|G| = p \Rightarrow |H| = 1$ oder $|H| = p \Rightarrow H = \{e\}$ oder $H = G$. $\square$

Noch mehr Wissen aus der Linearen Algebra: Falls $G$ abelsch ist, dann ist $G/H$ wieder eine Gruppe mit Gruppenoperation

$$\begin{aligned} \circ\colon G/H \times G/H &\to G/H \\ (aH, bH) &\mapsto abH \end{aligned}$$

Im Allgemeinen (falls $G$ nicht abelsch ist) ist $\circ$ nicht wohldefiniert (siehe Übungsblatt 2).

**Definition 3.** $G$ Gruppe, $H < G$ heißt Normalteiler falls gilt: $\forall g \in G, h \in H: \quad g \circ h \circ g^{-1} \in H$. Wir schreiben dann: $H \lhd G$.

*Bemerkung.* Falls $G$ abelsch, dann ist jede Untergruppe Normalteiler.

**Lemma 2.** *Sei $f\colon G \to G'$ Gruppenhomomorphismus. Dann: $Ker(f) \lhd G$.*

*Beweis.* Sei $g \in G$ und $h \in \mathrm{Ker} f$. $\Rightarrow f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e \Rightarrow ghg^{-1} \in \mathrm{Ker} f \Rightarrow \mathrm{Ker} f \lhd G$. □

16. Oktober 2017

**Satz 3.** Sei $G$ Gruppe, $N \lhd G$. Dann gilt:

1. $G/N$ bilden Gruppe mit $\circ\colon G/N \times G/N \to G/N, \quad (aN, bN) \mapsto abN$.
2. Die Abbildung

$$\begin{aligned} \mathrm{can}\colon G &\to G/N \\ g &\mapsto gN \end{aligned}$$

ist ein surjektiver Gruppenhomo.

*Beweis.*

1. Es gilt $(aN \circ bN) \circ cN = abN \circ cN = abcN = aN \circ (bN \circ cN) \Rightarrow$ (G1) Offensichtlich $eN = N$ ist neutrales Element. (G2). $a^{-1}N$ ist offensichtlich Inverses zu $aN$ (G3).

   noch zu zeigen: Das ist wohldefiniert. Sei also $a_1N = a_2N$ und $b_1N = b_2N$. Daraus sollte $a_1b_1N = a_2b_2N$ folgen.

   Tatsächlich gilt $a_1^{-1}a_2 \in N$ und $b_1^{-1}b_2 \in N$. Dann $(a_1b_1)^{-1}(a_2b_2) = b_1^{-1}a_1^{-1}a_2b_2$, wobei $a_1^{-1}a_2 \in N$ und $b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}b_2(b_2a_1^{-1}a_2b_2) \in N \Rightarrow (a_1b_1)^{-1}a_2b_2 \in N \Rightarrow a_1b_1N = a_2b_2N$.

2. surjektiv klar nach (3); um zu zeigen, dass das ein Gruppenhomomorphismus ist, muss man das einfach nachrechnen

$\square$

*Bemerkung.* Somit gilt: Normalteiler sind genau die Kerne von Gruppenhomomorphismen.

**Satz 4** (Homomorphiesatz)**.** Sei $f\colon G \to H$ Gruppenhomo. Sei $N \lhd G$. Dann: $N \subseteq \mathrm{Ker}(f) \Leftrightarrow \exists!$ Gruppenhomo $\overline{f}\colon G/N \to H$, sodass $\overline{f} \circ \mathrm{can} = f$. Also

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "\mathrm{can}"'] & H \\ & G/N \arrow[u, "\exists! \overline{f} \text{ Gruppenhomo}"'] \end{tikzcd}$$

*Beweis.* „$\Leftarrow$“: $\mathrm{Ker}(\mathrm{can}) = \{g \in G | gN = N\} = \{g \in G | g \in N\} = N \Rightarrow f(N) = \overline{f}(\mathrm{can}(N)) = \overline{f}(e) = e \Rightarrow N \subseteq \mathrm{Ker}(f)$.
„$\Rightarrow$“: **Eindeutigkeit:** Es mus für $\overline{f}$ gelten: $\overline{f}(aN) = \overline{f}(\mathrm{can}(a)) = f(a) \ \ \forall aN \in G/N \Rightarrow \overline{f}$ eindeutig bestimmt durch $f$.

**Existenz:** Setzen $\overline{f}(aN) := f(a) \ \forall aN \in G/N$. Das ist wohldefiniert (klar). Zu zeigen: Das ist ein Gruppenhomo. (nachrechnen) $\square$

**Korollar 5.** *$f\colon G \to H$ Gruppenhomo. Dann gilt $G/\ker f \cong \mathrm{Im}\, f$.*

*Beweis.* $\mathrm{Ker}f \lhd G$ nach Lemma 2.2. $\Rightarrow G/\mathrm{Ker}f$ ist eine Gruppe nach Satz 2.3. $\mathrm{im}f$ ist eine Gruppe nach 1.3. Setze $N := \mathrm{Ker}f$. Klar: $N \subseteq \mathrm{Ker}f$. Also existiert nach Satz 2.4 ein $\overline{f}$, sodass

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "\mathrm{can}"'] & H \\ & G/\mathrm{Ker}f \arrow[u, "\exists! \overline{f} \text{ Gruppenhomo}"'] \end{tikzcd}.$$

Also haben wir $\overline{f}\colon G/\mathrm{Ker}f \to \mathrm{im}f$ ein Gruppenhomomorphismus. Er ist surjektiv, weil can surjektiv ist.
Behauptung: $\overline{f}$ ist injektiv.

Es gilt $\overline{f}(aN) = f(a) = e \Leftrightarrow a \in \mathrm{Ker}f = N$. Also $\mathrm{Ker}\overline{f} = \{N\} = \{$neutrales Element in $G/\mathrm{Ker}f\}$. Also ist $\overline{f}$ injektiv. $\Rightarrow \overline{f}$ ist Gruppenisomorphismus. $\square$

**Satz 6** (1. Isomorphiesatz)**.** Sei $G$ eine Gruppe, $H < G$, $N \lhd G$.

1. $HN := \{hn | h \in H, n \in N\} < G$
2. $N \lhd HN$, $(H \cap N) \lhd H$
3. Es gilt $H/(H \cap N) \cong HN/N$ mit dem Gruppenisomorphismus $h(H \cap N) \mapsto hN$.

*Beweis.*

1. $HN \neq \emptyset$, da $e = ee \in HN$. Seien $h_1 n_1, h_2 n_2 \in HN$ $(h_i \in H, n_i \in N)$. Dann ist $h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2 {-} 1 = h_1 h_2^{-1} h_2 n_1 n_2^{-1} h_2 {-} 1$, wobei $n_1 n_2^{-1} \in N$, $h_2 n_1 n_2^{-1} h_2^{-1} \in N$, da $N \lhd G$ und $h_1 h_2^{-1} \in H$, also ist der gesamte Ausdruck Element von $HN$.

2. Zunächst zeigen wir, dass $N \lhd HN$: $N \subseteq HN$ (Klar, denn $n = en$). $\Rightarrow N < HN$, weil $N < G$; genauso $N \lhd HN$, weil $N \lhd G$.

   Noch zu zeigen: $(H \cap N) \lhd H$. Klar: $(H \cap N) \subseteq H$, $(H \cap N) < H$, weil $(H \cap N) < G$. Sei $x \in H \cap N$, $h \in H$. Dann $hxh^{-1} \in H$, weil $H < G$; und $\in N$, weil $N \lhd G$. Also $hxh^{-1} \in (H \cap N) \Rightarrow H \cap N \lhd H$

3. Betrachte

   $$\begin{aligned} f \colon H &\to HN \xrightarrow{\text{can}} HN/N \\ h &\mapsto he \end{aligned}$$

   Nachprüfen: $f$ ist ein Gruppenhomo. Für $x \in H$ gilt $x \in \text{Ker}(f) \Leftrightarrow xeN = N \Leftrightarrow x = xe \in \text{Ker}(\text{can}) = N \Leftrightarrow x \in (H \cap N)$. Also existiert nach dem Homomorphiesatz ein Gruppenhomo $\overline{f}$:

   $$\overline{f} \colon H/(H \cap N) \to (HN)/N$$

   ist nach Konstruktion injektiv.

   Surjektiv: Sei $hnN \in (HN)/N$ mit $h \in H, n \in N$. Dann gilt aber: $hnN = hN$ und dann $f(h) = hN$ und damit $\overline{f} \circ \text{can}(h) = \overline{f}(\text{can}(h)) = hN \Rightarrow hN \in \text{im} f \Rightarrow \overline{f}$ surjektiv. $\Rightarrow \overline{f}$ Gruppenisomorphismus.

□

# Alle Lehramtsstudierenden bitte nach der Vorlesung sich melden!

Anmerkung zu Beweis des Homomorphiesatzes: Wo wird in „⇒“verwendet, dass $N \subseteq \text{Ker} f$? Es wird benötigt für die Wohldefiniertheit von $\overline{f}$.

**Satz 7** (2. Isomorphiesatz)**.** Sei $G$ eine Gruppe; $N_1 \lhd G$, $N_2 \lhd G$, $N_1 \subseteq N_2$. Dann gilt $N_1 \lhd N_2$ und $N_2/N_1 \lhd G/N_1$ und es gilt:

$$(G/N_1)/(N_2/N_1) \cong G/N_2$$

durch den Isomorphismus $(gN_1)N_2/N_1 \mapsto gN_2$.

*Beweis.* $G/N_1$ ist Gruppe, weil $N_1 \lhd G$. $N_2/N_1 \subseteq G/N_1$ (Klar!); $G/N_2$ Gruppe, weil $N_2 \lhd G$. $N_1 \subseteq N_2$ und damit $N_1 \lhd N_2$, weil $N_1 \lhd G$. Sei

$$\begin{aligned} f\colon G/N_1 &\to G/N_2 \\ gN_1 &\mapsto gN_2 \end{aligned}$$

Das ist wohldefiert: Seien $g, h \in G$, $gN_1 = hN_1 \Rightarrow g^{-1}h \in N_1 \subseteq N_2 \Rightarrow gN_2 = hN_2 \Rightarrow$ wohldefiniert.

Klar: $f$ ist surjektiv und $gN_1 \in \mathrm{Ker}(f) \Leftrightarrow gN_2 = N_2 \Leftrightarrow g \in N_2$. Also $\mathrm{Ker}(f) = \{gN_1 | g \in N_2\} = N_2/N_1$. Also insbesondere $N_2/N_1 \lhd G/N_1$. Nach dem Korollar des Homomorphiesatzes erhalten wir einen Gruppenhomo

$$\overline{f}\colon (G/N_1)/\mathrm{Ker}f(= N_2/N_1) \to \mathrm{im}f = G/N_2 \text{ (da } f \text{ surjektiv)}$$

Nach Kosntruktion ist $\overline{f}$ injektiv, also erhalten wir den gewünschten Gruppenisomorphismus mit $\overline{f}(gN_1 \cdot (N_2/N_1)) = f(gN_1) = gN_2$. □

**Anwendungen**

1. **Anzahlformel:** $G$ endliche Gruppe, $H < G$, $N \lhd G$. Dann $|HN| = \frac{|H||N|}{|H \cap N|}$. Denn nach Lagrange ist $|H| = |H \cap N|(H : H \cap N)$ und $|HN| = |N|(HN : N)$. Nach dem 1. Isomorphiesatz ist $(H : H \cap N) = (HN : N)$. Also $|HN| = \frac{|N||H|}{|H \cap N|}$ ✓

2. $(G, \circ) = (\mathbb{Z}, +)$, $m, n \in \mathbb{N}$ und $m|n$. Wir wissen: $m\mathbb{Z} < \mathbb{Z}$ und $n\mathbb{Z} < \mathbb{Z}$ (sogar Normalteiler, weil $G$ abelsch ist). Klar ist: $n\mathbb{Z} \subseteq m\mathbb{Z}$ (insbesondere auch $n\mathbb{Z} \lhd m\mathbb{Z}$). Dann gilt

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$$

## 1.3 Zyklische Gruppen

Wir schreiben kurz $\langle g \rangle$ statt $\langle \{g\} \rangle$.

**Satz 1.** Untergruppen von zyklischen Gruppen sind zyklisch.

*Beweis.* Sei $G$ eine zyklische Gruppe; $G = \langle g \rangle$ mit $g \in G$. Sei $H < G$.

Fall 1 $H = \{e\} = \langle e \rangle$, also zyklisch

Fall 2 $H \neq \{e\} \Rightarrow \exists m \in \mathbb{Z} \setminus \{0\} : e \neq g^m \in H \Rightarrow \exists n \in \mathbb{N} : e \neq g^n \in H$ (weil $H < G$). Wähle $n := \min\{j \in \mathbb{N} | e \neq g^j \in H\}$. Behauptung: $H = \langle g^n \rangle$.

„$\supseteq$": Klar, da $g^n \in H$

„=": Angenommen, Gleichheit gilt nicht. Also $\exists s \in \mathbb{Z} : g^s \in H \setminus \langle g^n \rangle$ (beachte $G = \langle g \rangle$). Schreibe $s = an + r$ für $a, r \in \mathbb{Z}$ und $0 \leq r < n$. Falls $r = 0$, dann $s = an$ und $g^s = g^{an} = (g^n)^a \in \langle g^n \rangle$ Widerspruch!

Falls $r > 0$: Dann $g^r = (g^{an})^{-1} g^{an} g^r = ((g^n)^a)^{-1} g^s \in H$ (Widerspruch zur Minimalität)

Somit war die Annahme falsch und $H$ ist zyklisch.

□

**Lemma 2.** *Bilder von zyklischen Gruppen und Gruppenhomomorphismen sind zyklisch.*

*Beweis.* Sei $f : G \to G'$ ein Gruppenhomomorphismus und sei $G$ zyklisch, also $G = \langle g \rangle$ für ein $g \in G \Rightarrow G = \{g^i | i \in \mathbb{Z}\}$ also $f(G) = \{f(g^i) | i \in \mathbb{Z}\} = \{(f(g^i)) | i \in \mathbb{Z})\} = \langle f(g) \rangle \Rightarrow \operatorname{Im} f = \langle f(g) \rangle$ zyklisch. □

**Lemma 3.** *Sei $G$ endliche Gruppe $|G| = n < \infty$. Sei $g \in G$ mit $G = \langle g \rangle$ (also $G$ zyklisch). Sei* $\operatorname{ord}(g) = \min\{j \in \mathbb{N} | g^j = e\}$. *Dann gilt:* $\operatorname{ord}(g) = n$.

**Definition 1.** Allgemeiner: Sei $G$ irgendeine Gruppe, $g \in G$. Dann definiere

$$\operatorname{ord}(g) := \begin{cases} \min\{j \in \mathbb{N} | g^j = e\} & \text{falls das existiert} \\ \infty & \text{sonst} \end{cases}$$

Wir nennen $ord(g)$ die Ordnung von $g \in G$.

*Beweis von Lemma 3.*

1. Behauptung: $\operatorname{ord}(g)$ existiert. Angenommen es existiert nicht, also $g^j \neq g \; \forall j \in \mathbb{N} \Rightarrow g^i \neq g^j$ falls $i \neq j$, $i, j \in \mathbb{N}$ (denn sonst gilt $g^{i-j} = e = g^{j-i}$ mit $i - j \in \mathbb{N}$ oder $j - i \in \mathbb{N}$). Also $|G| = \infty \Rightarrow$ Widerspruch.

   Jetzt ist noch zu zeigen, dass $n = \operatorname{ord}(g)$ gilt. Dazu sei $S := \left\{g, g^2, ..., g^{\operatorname{ord}(g)} = e\right\} \subset G$.

2. Behauptung: $S < G$. Klar: $e \in S$. Sei $g^a, g^b \in S$. Schreibe $a - b = k \cdot \operatorname{ord}(g) + r$, wobei $k, r \in \mathbb{Z}, 0 \leq r < \operatorname{ord}(g)$. Daraus folgt

   $$g^a \left(g^b\right)^{-1} = g^{a-b} = g^{k \cdot \operatorname{ord}(g) + r} = \left(g^{\operatorname{ord}(g)}\right)^k g^r = e^k g^r = e g^r = g^r \in S$$

   weil $0 \leq r < \operatorname{ord}(g)$. Da $g \in S$, gilt $\langle g \rangle \subset S$. Weil $S < G$ ist klar, dass $S \subset \langle g \rangle$, also $\langle g \rangle = S$.

3. Behauptung: $|S| = \text{ord}(g)$. Seien $g^i, g^j \in S$ mit $1 \leq i, j \leq \text{ord}(g)$ und $g^i = g^j$. Also $g^{i-j} = e = g^{j-i}$, was ein Widerspruch zur Minimaltität von $\text{ord}(g)$ ist außer $i = j$. Folglich sind die $g^i (1 \leq i \leq \text{ord}(g))$ paarweise verschieden, was die Behauptung zeigt.

□

*Bemerkung.* Sei $G$ irgendeine Gruppe, $g \in G$. Dann gilt: $\text{ord}(g) = |\langle g \rangle|$ und nach Satz von Lagrange dann $\text{ord}(g)$ teilt $|G|$, falls $|G|$ endlich.

**Satz 4** (Zyklische Gruppen)**.** Je zwei zyklische Gruppen der selben Ordnung sind isomorph. Genauer gilt für $G$ zyklische Gruppe:

$$G \cong \begin{cases} \mathbb{Z} & \text{falls } |G| = \infty \\ \mathbb{Z}/n\mathbb{Z} & \text{falls } |G| = n \end{cases}$$

*Beweis.* Sei $G = \langle g \rangle$ mit $g \in G$. Sei $f : \mathbb{Z} \to G : j \mapsto g^j$. Dann ist $f$ ein Gruppenhomomorphismus (nachrechnen) und surjektiv, da $G = \langle g \rangle$.

Fall 1 $|G| = \infty$. Dann muss $f$ injektiv sein, damit $f$ ein Isomorphismus ist und damit $\mathbb{Z} \cong G$. Falls $f$ nicht injektiv ist, dann $\exists i, j \in \mathbb{Z}, i \neq j$ mit $g^i = g^j$, als $g^{i-j} = e = g^{j-i}$. Folglich ist $\text{ord}(g) < \infty$. Damit wäre $G$ nach 3 endlich, was ein Widerspruch ist.

Fall 2 $|G| = n$ endlich. Dann folgt aus 3:

$$\text{ord}(g) = n \Rightarrow g^n = e \Rightarrow g^{nk} = (g^n)^k = e^k = e \ \forall k \in \mathbb{Z} \Rightarrow n\mathbb{Z} \subset \ker F$$

Nach dem Homotopiesatz gilt dann: TODO Diagramm. Also $\overline{f} : \mathbb{Z}/n\mathbb{Z} \to G$. Da $|\mathbb{Z}/n\mathbb{Z}| = n = |G|$ muss diese surjektive Abbildung schon ein Isomorphismus sein.

□

## 1.4 Auflösbare Gruppen

**Definition 1.** Eine Normalreihe eine Gruppe $G$ ist eine Kette von Untergruppen der Form $\{e\} = G_0 \lhd G_1 \lhd ... \lhd G_n = G$. Man nennt die Quotiengruppe $G_i/G_{i-1}$ die Faktoren der Normalreihe.

**Definition 2.** Eine Gruppe heißt auflösbar, falls eine Normalreihe mit abelschen Faktoren existiert.

**Beispiel.**

1. Abelsche Gruppen sind auflösbar: $\{e\} \lhd G$ und $G/\{e\} \cong G$, also abelsch

2. Sei $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(K) \right\} < \mathrm{GL}_2(K)$. Behauptung: $G$ ist auflösbar.

   Dazu betrachtet man $G' = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(K) \right\} < \mathrm{GL}_2(K)$, wobei $G'$ insbesondere eine Gruppe ist.

$$f : G \to G' : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

   was ein Gruppenepimorphismus ist (nachrechnen). Es gilt:

$$\ker f = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in K \right\} \lhd G$$

   Folglich gilt $\ker f \cong (K, +)$, sodass $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mapsto b$, weil $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix}$ als Gruppenhomomorphismus offensichtlich bijektiv ist. Damit ist $\ker f$ abelsch und $G'$ somit auch.

$$\Rightarrow \{e\} = G_0 \lhd \ker f = G_1 \lhd G_2 = G$$

   und $ker f/\{e\}$ abelsch, sowie auch $G/\ker f \cong \mathrm{Im}\, f = G'$ abelsch. Somit ist $G$ auflösbar.

3. $S_4$ ist auflösbar. Betrachte

$$S_4 > A_4 := \{\pi \in S_4 | \operatorname{sgn}(\pi) = 1\}$$

   Nach LA 1 ist sgn ein Gruppenhomomorphismus und damit $A_4 = \ker(\operatorname{sgn}) < S_4$. Es gilt $S_4 \lhd A_4$, weil $A_4 = \ker(\operatorname{sgn})$ oder weil $(S_4 - A_4) = 2$, was dann nach Blatt 2 folgt. Betrachte nun

$$A_4 > V_4 := \left\{ e, \underbrace{(1,2)(3,4)}_{a}, \underbrace{(1,3)(2,4)}_{b}, \underbrace{(1,4)(2,3)}_{c} \right\}$$

   Gruppentafel:

|   | a | b | c |
|---|---|---|---|
| a | e | c | b |
| b | c | e | a |
| c | b | a | e |

   Dann gilt $A_4 \lhd V_4$, da folgendes gilt:

$$\forall \pi \in S_4 : \pi \circ \underbrace{(a_1, a_2)(a_3, a_4)}_{\tau} \circ \pi^{-1} = (\pi(a_1), \pi(a_2))(\pi(a_3), \pi(a_3))$$

weil

$$\begin{aligned}
\pi(a_1) &\xmapsto{\pi^{-1}} a_1 \overset{\tau}{\mapsto} a_2 \overset{\pi}{\mapsto} \pi(a_2)\\
\pi(a_2) &\longmapsto a_2 \mapsto a_1 \mapsto \pi(a_1)\\
\pi(a_3) &\longmapsto a_3 \mapsto a_4 \mapsto \pi(a_4)\\
\pi(a_4) &\longmapsto a_4 \mapsto a_3 \mapsto \pi(a_3)
\end{aligned}$$

also $V_4 \lhd A_4$. Folglich haben wir

$$\{e\} = G_0 \lhd V_4 = G_1 \lhd A_4 = G_2 \lhd S_4 = G_3 \tag{1}$$

$G_1/G_0 \cong V_4$ ablesch

$G_2/G_1 \cong \mathbb{Z}/2\mathbb{Z}$ also abelsch, da jede Gruppe $H$ der Ordunung 2 zyklisch mit $H = \langle g \rangle (g \neq e)$ ist und dann nach Klassifikationssatz $H \cong \mathbb{Z}/2\mathbb{Z}$

$G_3/G_2$ Wir wissen, dass $|G_3/G_2| = 3$. Dann behaupten wir, dass $G_3/G_2 \cong \mathbb{Z}/3\mathbb{Z}$. Jede Gruppe $H$ mit $|H| = 3$ ist zyklisch, denn $\langle g \rangle < H(g \neq e)$. Nach dem Satz von Lagrange gilt $\langle g \rangle = H$, weil $\langle g \rangle \neq e$ und 3 prim ist. Also folgt die Aussage aus dem Klassifikationssatz.

Daraus folgt, dass $S_4$ auflösbar ist.

**Satz 1.** Untergruppen und Bilder unter Gruppenhomomorphismen von auflösbaren Gruppen sind auflösbar.

*Beweis.* Sei $G$ auflösbare Gruppe. Dann existiert eine Auflösung

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G \; G_i/G_{i-1} \text{ abelsch}$$

1. Sei $U < G$. Behauptung: $\{e\} = G_0 \cap U \lhd (G_1 \cap U) \lhd \ldots \lhd (G_n \cap U) = U$. Es ist klar, dass $(G_{i-1} \cap U) \subset (G_1 \cap U)$. Auch klar ist, dass $G_i \cap U$ eine Gruppe ist und $(G_{i-1}) < (G_1 \cap U)$. Jetzt ist noch zu zeigen, dass $(G_{i-1} \cap U) \lhd (G_i \cap U)$. Sei $x \in G_{i-1} \cap U$ und sei $y \in G_i \cap U$. Dann folgt, dass $\underbrace{yxy^{-1}}_{\in G_{i-1}} \in U$, weil $x, y \in U, U < G$, weil $x \in G_{i-1}, y \in G_i$ und $G_{i-1} \lhd G_i$. Daraus folgt, dass $yxy^{-1} \in U \cap G_{i-1}$, was zu zeigen war.

2. Behauptung: $G_i \cap U/G_{i-1} \cap U$ abelsch. Es gilt $G_i \cap U/G_{i-1} \cap U \overset{\text{1. Iso}}{\cong} (U \cap G_i)G_i/G_i \lhd G_i/G_{i-1}$ abelsch. Daraus folgt die Behauptung.

□