**Def:** Eine Untergruppe $U$ von $G$, $U \leq G$, ist eine Teilmenge von $G$, die

- das neutrale Element enthält
- mit jedem Element auch sein Inverses enthält
- und abgeschlossen bzgl. der Gruppenoperation ist.

D.h. $U$ ist mit der eingeschränkten Operation selbst eine Gruppe.

**Bsp:**

- Falls $G$ Gruppe ist, dann ist $G$ selbst Untergruppe von $G$ und die triviale Gruppe $\{e\}$ ist Untergruppe von $G$.
- Falls $U \leq V$ und $V \leq G$, dann auch $U \leq G$.
- $(\mathbb{Z}, +)$ hat Untergruppen $m\mathbb{Z} := \{m \cdot z \mid z \in \mathbb{Z}\}$
  ($m$ fest)

$$\text{denn } 0 = m \cdot 0 \in m\mathbb{Z}$$
$$-(m \cdot t) = m \cdot (-t)$$
$$m \cdot z_1 + m \cdot z_2 = m(z_1 + z_2)$$

$m = 0$ : $m\mathbb{Z} = \{0\}$ triviale Gruppe
$m = 1$ : $m\mathbb{Z} = \mathbb{Z}$ die ganze Gruppe

**Bem:** Falls $V$ ein Vektorraum und $U$ Untervektorraum, dann ist $U$ auch Untergruppe von $V$; die Untervektorräume sind genau die unter Skalarmultiplikation abgeschlossenen Untergruppen.

- Falls $G$ eine Gruppe, so ist das Zentrum von $G$

$$Z(G) := \{ z \in G \mid z \circ g = g \circ z \text{ für alle } g \in G \}$$

Beweis:

Vorbemerkung $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$ $\qquad (g^{-1})^{-1} = g$

Bew: $(h^{-1} \circ \underbrace{g^{-1}) \circ (g}_{= e} \circ h) = h^{-1} \circ h = e$

ebenso $(g \circ h) \circ (h^{-1} \circ g^{-1}) = e$

1) $e \in Z(G)$ : klar

2) $z_1, z_2 \in Z(G)$ : $(z_1 \circ z_2) \circ g = z_1 \circ g \circ z_2 = g \circ z_1 \circ z_2$

3) $z \in Z(G)$ : $z^{-1} \circ g = ((z^{-1} \circ g)^{-1})^{-1} = (g^{-1} \circ z)^{-1} = (z \circ g^{-1})^{-1} = g \circ z^{-1}$ $\quad g \in G$ beliebig

☒

Bsp: $Z(GL(n, \mathbb{R})) = \left\{ \begin{pmatrix} r & & 0 \\ & \ddots & \\ 0 & & r \end{pmatrix} \middle| \, r \in \mathbb{R} \setminus \{0\} \right\} \cong (\mathbb{R} \setminus \{0\}, \cdot)$

$\begin{pmatrix} r & & 0 \\ & \ddots & \\ 0 & & r \end{pmatrix} = r \cdot \mathrm{Id}_n$

Übung!

Satz: Falls $\varphi: G \to H$ ein Gruppenhomomorphismus ist, dann sind $\mathrm{Bild}(\varphi)$ und $\mathrm{Kern}(\varphi) := \{ g \in G \mid \varphi(g) = e_H \}$ sind Untergruppen von $H$ bzw. $G$.

Beweis: $\mathrm{Bild}(\varphi)$: $e_H = \varphi(e_G) \in \mathrm{Bild}(\varphi)$

falls $h_i = \varphi(g_i) \in \mathrm{Bild}(\varphi)$, dann
$(i = 1, 2)$

$h_1 \circ h_2 = \varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 \circ g_2) \in \mathrm{Bild}(\varphi)$

$h_1^{-1} = \varphi(g_1)^{-1} = \varphi(g_1^{-1}) \in \mathrm{Bild}(\varphi)$

Kern $(\varphi)$: $e_G \in \text{Kern}(\varphi)$, da $\varphi(e_G) = e_H$

angenommen $g_1, g_2 \in \text{Kern}(\varphi)$,

dann $\varphi(g_1 \circ g_2) = \varphi(g_1) \circ \varphi(g_2) = e_H \circ e_H = e_H$

$\varphi(g_1^{-1}) = \varphi(g_1)^{-1} = e_H^{-1} = e_H$

also $g_1 \circ g_2$ und $g_1^{-1} \in \text{Kern}(\varphi)$ $\boxtimes$

Bem: Jeder Untervektorraum $U \leq V$ ist Kern eines VR-Homom. und Bild eines VR-Homom. (in der Regel anderen)

Sei $\mathcal{B}$, $B$ eine Basis von $U$, ergänze sie durch $B'$ zu Basis von $V$

$\varphi: V \to V$ $\quad \varphi(v) = v$ für $v \in B$, $\quad \varphi(v) = 0$ für $v \in B'$ $\quad$ also $\text{Bild}(\varphi) = U$

$\psi: V \to V$ $\quad \psi(v) = 0$ für $v \in B$, $\quad \psi(v) = v$ für $v \in B'$ $\quad$ also $\text{Kern}(\psi) = U$

Achtung: bei Gruppen ist nicht jede Untergruppe Kern eines Homomorphismus; die Kerne von Homomorphismen haben noch besondere Eigenschaften, „normale Untergruppen".

Bem:

- Der Schnitt von zwei Untergruppen ist wieder eine Untergruppe
  (z.B. $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$)

  die Vereinigung zweier Untergruppen ist in der Regel keine Untergruppe
  (z.B. $2\mathbb{Z} \cup 3\mathbb{Z}$ ist nicht von der Form $m \cdot \mathbb{Z}$)

- Der Schnitt von beliebig vielen Untergruppen ist wieder eine Untergruppe.

  Wenn $A \subseteq G$, dann existiert
  „die kleinste Untergruppe, die $A$ enthält"

  $$\langle A \rangle = \bigcap \{ U \mid A \subseteq U \text{ und } U \leq G \}$$

  Erzeugnis von $A$ „der Schnitt über alle Untergruppen von $G$, die $A$ enthalten"

  $$= \{ a_1^{\pm 1} \cdot \ldots \cdot a_n^{\pm 1} \mid a_i \in A, n \in \mathbb{N} \} \quad (*)$$

  $a^{+1} := a$

  (denn u.a.
  $$(a_1 \cdot a_2^{-1} \cdot a_3^{-1} \cdot a_4 \cdot a_5)^{-1} = a_5^{-1} \cdot a_4^{-1} \circ a_3 \circ a_2 \circ a_1^{-1}$$
  $e = a_1 \cdot a_1^{-1}$ oder $e =$ „das leere Produkt", d.h. $n = 0$)

  mit einigen anderen Überlegungen folgt hieraus, dass $(*)$ eine Untergruppe ist.
  Klar ist: Jede Untergruppe, die $A$ enthält, muss auch $(*)$ enthalten

Notation: statt $\langle \{g_1, \ldots, g_k\} \rangle$ schreibt man kurz $\langle g_1, \ldots, g_n \rangle$

## § Zyklische Gruppen

**Def:** Eine Gruppe heißt zyklisch, falls sie von einem Element erzeugt wird.

Bem: $g^n = (g^{-n})^{-1}$ gilt für alle $n \in \mathbb{Z}$

Bsp: $(\mathbb{Z},+) = \langle 1 \rangle = \langle -1 \rangle$

es gibt 2 Erzeuger: $1$ und $-1$

Sei $G$ eine Gruppe, $g \in G$ und $n \in \mathbb{Z}$. Definiere $g^n$ als:

$$g^n := \underbrace{g \circ g \circ \dots \circ g}_{n \text{ Vorkommen von } g}, \quad \text{d.h.} \quad g^1 := g, \quad g^{n+1} := g^n \circ g \quad \text{für } n \geq 0$$

$$g^0 := e$$

das Inverse

$$g^n := (g^{-n})^{-1} \quad \text{für } n < 0$$

Definition ist nur für

wird deshalb so definiert, damit dieses gilt:

Die Definition ist kompatibel mit der Schreibweise $g^{-1}$ für das Inverse

Man rechnet leicht nach, dass gilt:

$$\boxed{(g^n)^m = g^{n \cdot m} \quad \text{und} \quad g^n \circ g^m = g^{n+m}}$$

Dies bedeutet, dass es einen Gruppenhomomorphismus $g^{\cdots} : (\mathbb{Z},+) \to (G,\circ)$, $n \mapsto g^n$

$$\text{Bild}(g^{\cdots}) = \{ g^n \mid n \in \mathbb{Z} \} = \langle g \rangle$$

Alternativ: $g^0 := e$ für $n \geq 2$: $g^n = \underbrace{g \circ \dots \circ g}_{n \text{ mal } g}$

$g^1 := g$

$g^{-1}$ gibt es schon $g^{-n} = \underbrace{g^{-1} \circ \dots \circ g^{-1}}_{n \text{ mal } g^{-1}}$

---

Bem: a) Falls $G = \langle g \rangle$ zyklisch ist, dann ist $g^{\cdots} : \mathbb{Z} \to G$ surjektiv.

b) Zyklische Gruppen sind kommutativ, denn

$$g^n \circ g^m = g^{n+m} = g^{m+n} = g^m \circ g^n$$

(allgemeiner: „homomorphe Bilder von komm. Gruppen sind kommutativ", d.h. falls $\varphi: G \to H$ ein Homom. und $G$ kommutativ, dann ist Bild$(\varphi)$ kommutativ.)

Def: Die Ordnung einer Gruppe ist die Anzahl ihrer Elemente. Die Ordnung eines $g \in G$ ist di die Ordnung von $\langle g \rangle$.

Bsp:
- $\mathbb{Z}_{12}$ hat Ordnung 12

  $3 \in \mathbb{Z}_{12}$: 3 hat Ordnung 4 in $\mathbb{Z}_{12}$ $\langle 3 \rangle = \{0, 3, 6, 9\}$
- $\mathbb{Z}$ hat unendliche Ordnung

  3 hat Ordnung $\infty$ in $\mathbb{Z}$ $\langle 3 \rangle = 3\mathbb{Z}$
- $S_3$ hat Ordnung 6, Ordnung von $S_n$ ist $n!$

**Satz:** Eine zyklische Gruppe ist

- entweder von unendlicher Ordnung und isomorph zu $(\mathbb{Z}, +)$
- oder von endlicher Ordnung $m$ und isomorph zu $(\mathbb{Z}_m, +_m)$

**Beweis:** Sei $C = \langle g \rangle$ zyklisch. Betrachte $g^{\cdots} : \mathbb{Z} \to G$ (surjektiv)

**1. Fall:** $g^{\cdots}$ ist ein Isomorphismus ($\Leftrightarrow$ $g$ injektiv)

**2. Fall** $g^{\cdots}$ ist nicht injektiv, d.h. es gibt $m, n \in \mathbb{Z}$, $m \neq n$, mit $g^m = g^n$

$$\ker(g^{\cdots}) \neq \{e_G\} \quad \Leftarrow \quad g^{m-n} = g^m \circ g^{-n} = g^n \circ g^{-n} = g^0 = e \qquad (*)$$

o.B.d.A. $m - n > 0$

Wähle $m_0 > 0$ minimal mit $m_0 \in \ker(g^{\cdots})$, d.h. $g^{m_0} = e$

**Beh:** $\ker(g^{\cdots}) = m_0 \mathbb{Z}$

**Bew:** $m_0 \in \ker(g^{\cdots}) \leq \mathbb{Z}$, also $\underset{\langle m_0 \rangle}{m_0 \mathbb{Z}} \subseteq \ker(g^{\cdots})$

angenommen $n \in \ker(g^{\cdots})$. dann schreibe $n = q \cdot m_0 + r$ mit $r \in \{0, \dots, m_0 - 1\}$

$$e = g^n = g^{q m_0 + r} = (\underbrace{g^{m_0}}_{e})^q \circ g^r = g^r \in \ker(g^{\cdots})$$

$\underset{\text{Minimalität von } m_0}{\Rightarrow}$ $r = 0$, $n$ ist Vielfaches von $m_0$, $n \in m_0 \mathbb{Z}$ $\square$

Falls $n \in \mathbb{Z}$ beliebig, $n = q \cdot m_0 + r$ wie oben, $g^n = g^r$

$$\mathrm{Bild}(g^{\cdots}) = \{\underbrace{g^0, g^1, \dots, g^{m_0 - 1}}_{\text{paarweise verschieden, z.B. wegen Rechnung wie } (*)}\} \cong \mathbb{Z}_m$$

$\square$