

# 1 Gruppen

## 1.1 Grundbegriffe

1.1.1 **Definition:** Eine *Gruppe* ist ein Tripel  $(G, \circ, e)$  bestehend aus einer Menge  $G$  mit einer Abbildung

$$\circ: G \times G \rightarrow G, (a, b) \mapsto a \circ b$$

und einem ausgezeichneten Element  $e \in G$ , so dass gilt:

$$\forall a, b, c \in G: \underline{a \circ (b \circ c) = (a \circ b) \circ c} \quad (\text{Assoziativit\u00e4t})$$

$$\forall a \in G: \underline{e \circ a = a} \quad (\text{Linksneutrales Element})$$

$$\forall a \in G \exists a' \in G: \underline{a' \circ a = e} \quad (\text{Linksinverses Element})$$

Die Gruppe heisst *kommutativ* oder *abelsch*, wenn zus\u00e4tzlich gilt:

$$\forall a, b \in G: \underline{a \circ b = b \circ a} \quad (\text{Kommutativit\u00e4t})$$

**1.1.2 Proposition:** In jeder Gruppe  $(G, \circ, e)$  gilt:

(a) Jedes linksneutrale Element  $e$  ist auch rechtsneutral, das heisst, es gilt  $\forall a \in G: a \circ e = a$ . Wir nennen  $e$  darum kurz neutrales Element von  $G$ .

(b) Jedes zu  $a \in G$  linksinverse Element  $a' \in G$  ist auch rechtsinvers, das heisst, es gilt  $a \circ a' = e$ . Wir nennen  $a'$  darum kurz inverses Element zu  $a$ .

(c) Das neutrale Element von  $G$  ist eindeutig bestimmt.

(d) Zu jedem  $a \in G$  ist das inverse Element eindeutig bestimmt. Die Standardbezeichnung dafür ist  $a^{-1}$ .

(e) Für alle  $a \in G$  gilt  $(a^{-1})^{-1} = a$ . ← Beweis:  $a \circ a^{-1} = e$  nach (b). Also ist  $a$  linksinvers zu  $a^{-1}$  ged.

(f) Für alle  $a, b \in G$  gilt  $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ . Bew.  $\rightarrow (b^{-1} \circ a^{-1})(ab) = b^{-1}(a^{-1}b) = b^{-1}eb = b^{-1}b = e$   
 $\Rightarrow b^{-1}$  ist linksinvers zu  $ab$ .

(g) Für alle  $a, b \in G$  existiert ein eindeutiges  $x \in G$  mit  $a \circ x = b$ , nämlich  $x = a^{-1} \circ b$ . s.u.

(h) Für alle  $a, b \in G$  existiert ein eindeutiges  $y \in G$  mit  $y \circ a = b$ , nämlich  $y = b \circ a^{-1}$ . analog

(i) Für alle  $a, b, c \in G$  gilt  $b = c \iff a \circ b = a \circ c$ . (Kürzungsregel links)

(j) Für alle  $a, b, c \in G$  gilt  $b = c \iff b \circ a = c \circ a$ . (Kürzungsregel rechts)

} analog.

(g)  $ax=b \Rightarrow x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b$   
 $x = a^{-1}b \Rightarrow ax = a(a^{-1}b) = (aa^{-1})b = eb = b$

**1.1.3 Proposition:** Für jede natürliche Zahl  $n \geq 1$  und für beliebige  $a_1, \dots, a_n \in G$  gilt: Bei jeder möglichen Klammerung der (a priori nicht wohldefinierten) Formel  $a_1 \circ \dots \circ a_n$  ist das Resultat gleich. Wir dürfen hier also doch auf Klammern verzichten.

**1.1.4 Konvention:** Oft schreibt man nur kurz  $G$  für das ganze Tripel und sieht die Zusatzdaten als implizit mitgegeben an. Wenn dabei keine Notation für die Gruppenoperation angegeben wird, bezeichnet man diese multiplikativ in der Form  $g \cdot h$  oder  $gh$  und das neutrale Element mit  $1_G$  oder einfach  $1$ . Das tun ab sofort auch wir und verwenden ein spezielles Symbol wie  $\circ$  nur, wenn Verwechslungen zu vermeiden sind.

Sei also  $G$  eine Gruppe.

**1.1.5 Definition:** Für jedes Element  $g \in G$  und jede ganze Zahl  $n$  definieren wir die  $n$ -te Potenz von  $g$  induktiv durch

$$g^n := \begin{cases} 1 & \text{falls } \underline{n = 0}, \\ g & \text{falls } \underline{n = 1}, \\ g \cdot g^{n-1} & \text{falls } \underline{n > 1}, \\ g^{-1} \cdot g^{n+1} & \text{falls } \underline{n < -1}. \end{cases}$$

**1.1.6 Proposition:** Für alle  $g, h \in G$  und alle  $m, n \in \mathbb{Z}$  gilt:

$$\begin{aligned} g^{m+n} &= g^m \cdot g^n \\ g^{m \cdot n} &= (g^m)^n \\ (g \cdot h)^m &= g^m \cdot h^m \quad \text{falls } gh = hg \text{ ist.} \end{aligned}$$

**1.1.7 Konvention:** Eine abelsche Gruppe (und nur eine abelsche) schreibt man oft additiv, das heisst mit dem Operator  $+$ , dem neutralen Element  $0_G$  oder  $0$ , und dem inversen Element  $-g$  zu  $g$ . Für  $g + (-h)$  schreibt man dann auch kürzer  $g - h$ . Anstatt der  $n$ -ten Potenz spricht man von dem  $n$ -ten Vielfachen  $n \cdot g$ . Die obigen Eigenschaften übersetzen sich dann in folgende:

**1.1.8 Proposition:** Jede additiv geschriebene abelsche Gruppe  $G$  ist auf eindeutige Weise ein  $\mathbb{Z}$ -Modul. Insbesondere gilt für alle  $g, h \in G$  und alle  $m, n \in \mathbb{Z}$ :

$$\begin{aligned} 0 \cdot g &= 0 \\ (\pm 1) \cdot g &= \pm g \\ (m \pm n) \cdot g &= m \cdot g \pm n \cdot g \\ (m \cdot n) \cdot g &= m \cdot (n \cdot g) \\ m \cdot (g \pm h) &= m \cdot g \pm m \cdot h \end{aligned}$$

**1.1.9 Beispiel:** (a) Die additive Gruppe eines Rings, eines Körpers, eines Vektorraums.

(b) Die Einheitengruppe eines Rings, eines Körpers.

(c) Die Matrizengruppen  $GL_n(K)$ ,  $SL_n(K)$ ,  $O(n)$ ,  $SO(n)$ ,  $U(n)$ .

(d) Die Symmetriegruppe einer Teilmenge  $X$  des euklidischen Raums  $\mathbb{R}^n$ :

$$\{A \in O(n) \mid A \cdot X = X\} \quad \text{oder} \quad \{A \in SO(n) \mid A \cdot X = X\}.$$



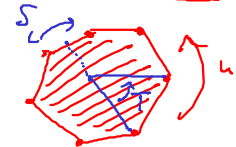
(e) Platonische Körper: Tetraeder, Würfel, Oktaeder, Dodekaeder, Ikosaeder.

(f) Ein regelmässiges ebenes Polygon im  $\mathbb{R}^3$ , aufgefasst als degenerierter regelmässiger Polyeder mit zwei Seitenflächen, heisst **Dieder** (gesprochen Di-Eder). Er ist invariant unter  $n$  Drehungen um seine Symmetrieachse, sowie  $n$  weiteren Drehungen um  $180^\circ$ , nämlich um alle durch den Mittelpunkt und eine Ecke oder Kantenmitte gehenden Geraden. Zusammen bilden diese  $2n$  Symmetrien die **Diedergruppe vom Grad  $n$** , bezeichnet mit  $D_n$ .

Elemente  $1, T, \dots, T^{n-1}$   
 $S, ST, \dots, ST^{n-1}$

$T = \text{Drehung um } \frac{2\pi}{n}$   
 $S = \text{Drehung um } \pi$   
 "Spiegelung in der Ebene"

$$ST = T^{-1}S$$



**1.1.10 Bemerkung:** Niemand beschreibt eine Gruppe mittels ihrer Gruppentafel.

## 1.2 Untergruppen

**1.2.1 Definition:** Eine Untergruppe von  $G$  ist eine Teilmenge  $H \subset G$  mit den Eigenschaften:

- (a)  $1_G \in H$ . ✓
- (b)  $\forall h, h' \in H: hh' \in H$ . ✓
- (c)  $\forall h \in H: h^{-1} \in H$ . ✓

Voricht; dies erlaubt  $H=G$ .

Die Aussage „ $H$  ist eine Untergruppe von  $G$ “ bezeichnet man mit  $H < G$  oder  $G > H$ .

**1.2.2 Proposition:** Eine Teilmenge  $H \subset G$  ist eine Untergruppe genau dann, wenn sie zusammen mit der Restriktion der Gruppenoperation von  $G$  selbst eine Gruppe bildet. Dann ist weiter das Einselement von  $G$  gleich dem Einselement von  $H$ .

$$H \times H \xrightarrow{\quad} \overset{H}{\cancel{H}}, (h, h') \mapsto hh'. \quad \text{für } a \in G$$
$$\downarrow$$

wäre  $e'$  ein Einselement in  $H$ , dann wäre  $e'e' = e' = ee' \Rightarrow e' = e$ .

**1.2.3 Beispiel:** Die triviale Untergruppe  $1 = \{1_G\}$  und  $G$  selbst sind Untergruppen von  $G$ .

**1.2.4 Beispiel:** Die Untergruppen einer additiv geschriebenen abelschen Gruppe sind genau die  $\mathbb{Z}$ -Untermoduln. Insbesondere sind die Untergruppen von  $\mathbb{Z}$  genau die Ideale von  $\mathbb{Z}$ , also die Untergruppen  $n\mathbb{Z}$  für alle  $n \geq 0$ .

**1.2.5 Beispiel:** Die Untergruppen

$$\begin{array}{ccc} \mathrm{SO}_n(K) < & \mathrm{O}_n(K) \\ \wedge & \wedge \\ \mathrm{SL}_n(K) < & \mathrm{GL}_n(K). \end{array}$$

**1.2.6 Beispiel:** Die Untergruppen der Diedergruppe.

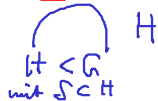
$$\{1, T, \dots, T^{n-1}\}$$

$$\forall i: \{1, ST^i\} \quad \text{mit} \quad (ST^i)^{-1} = ST^i$$

**1.2.7 Proposition:** Jede Untergruppe einer Untergruppe von  $G$  ist eine Untergruppe von  $G$ .

**1.2.8 Proposition:** Der Durchschnitt jeder nichtleeren Kollektion von Untergruppen von  $G$  ist ein Untergruppe von  $G$ .

**1.2.9 Proposition:** Für jede Teilmenge  $S \subset G$  existiert eine eindeutige kleinste Untergruppe von  $G$ , welche  $S$  enthält. Diese besteht aus allen Elementen der Form  $a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$  für alle  $n \geq 0$ , alle  $a_i \in S$ , und alle  $\varepsilon_i \in \{\pm 1\}$ .

Beweis:   $H$   
Ht  $\subset$  G  
mit  $S \subset H$

↑  
In  $G'$  diese Teilmenge.

Damit  $1 \in G'$  für  $n=0$ .

$\Rightarrow G' \cdot G' \subset G'$ .

$(G')^{-1} \subset G'$  weil  $(a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n})^{-1} = a_n^{-\varepsilon_n} \cdots a_1^{-\varepsilon_1} \in G'$ .

Also ist  $G' < G$  mit  $S \subset G'$ .

$\forall H < G: S \subset H \Rightarrow G' \subset H$ .

qed.

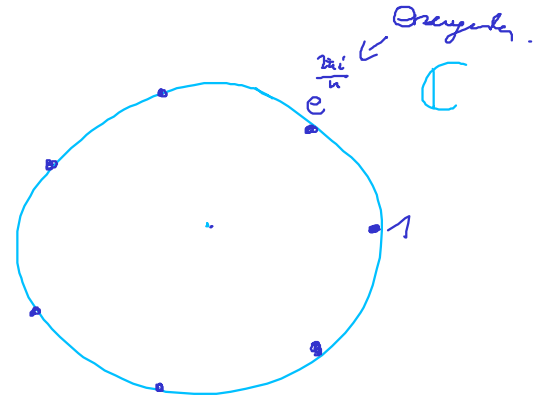
**1.2.10 Definition:** Diese Untergruppe heisst die von  $S$  erzeugte Untergruppe  $\langle S \rangle$ . Im Fall einer endlichen Teilmenge schreiben wir auch kürzer  $\langle a_1, \dots, a_n \rangle = \langle \{a_1, \dots, a_n\} \rangle$  und nennen diese Untergruppe endlich erzeugt. Ist  $G = \langle S \rangle$ , so nennen wir  $G$  von  $S$  erzeugt.



**1.2.11 Definition:** Eine von einem Element erzeugte Gruppe  $G = \langle a \rangle$  heisst zyklisch.

**1.2.12 Beispiel:** Die additiven Gruppen von  $\mathbb{Z}$  und  $\mathbb{Z}/n\mathbb{Z}$  für jedes  $n \geq 1$  sind zyklisch. Die Untergruppen von  $\mathbb{Z}$  sind die  $m\mathbb{Z}$  für alle  $m \geq 0$ ; die Untergruppen von  $\mathbb{Z}/n\mathbb{Z}$  die  $m\mathbb{Z}/n\mathbb{Z}$  für alle  $m|n$ .

**1.2.13 Beispiel:** Die Gruppe der  $n$ -ten Einheitswurzeln  $\mu_n := \{\zeta \in \mathbb{C} \mid \zeta^n = 1\} < \mathbb{C}^\times$  ist zyklisch. Dass diese auf einem Kreis liegen, ist der Ursprung der Bezeichnung „zyklisch“.



Die Kommutativität oder Nichtkommutativität einer Gruppe hat mit einer Reihe von weiteren Untergruppen zu tun:

- 1.2.14 Definition:** (a) Der Kommutator von  $g, h \in G$  ist das Element  $[g, h] := ghg^{-1}h^{-1}$ .  
 (b) Die Kommutatorgruppe von  $G$  ist die von allen Kommutatoren erzeugte Untergruppe.

$$[G, G] := \langle \{[g, h] \mid g, h \in G\} \rangle.$$

- (c) Der Zentralisator eines Elements  $g \in G$  ist die Untergruppe

$$g \in \text{Cent}_G(g) := G_g := \{x \in G \mid xg = gx\} < G$$

- (d) Das Zentrum von  $G$  ist die Untergruppe

$$Z(G) := \{x \in G \mid \forall y \in G: xy = yx\} < G$$

- 1.2.15 Proposition:** (a)  $gh = hg \iff [g, h] = 1$ .

- (b)  $\text{Cent}_G(g)$  ist die eindeutige grösste Untergruppe  $H < G$  mit  $g \in Z(H)$ .

- (c)  $Z(G) = \bigcap_{g \in G} \text{Cent}_G(g) < G$ .

- (d)  $g \in Z(G) \iff \text{Cent}_G(g) = G$ .

- (e)  $G$  ist abelsch  $\iff Z(G) = G \iff [G, G] = 1$ .

$[g, h] = 1$   
 $\iff ghg^{-1}h^{-1} = 1$   
 $\iff ghg^{-1} = h$   
 $\iff gh = hg$

$\iff gx^{-1} = x^{-1}g$

$\forall y \in G: x \in \text{Cent}_G(y)$

$g \in Z(\text{Cent}_G(g))$ .

$\iff \forall h \in H: gh = hg \implies h \in \text{Cent}_G(g)$   
 Also ist  $H \subset \text{Cent}_G(g)$ .

1.2.16 Beispiel: (a) Die Kommutatorgruppe von  $GL_n(K)$  ist  $SL_n(K)$  ausser für  $|K| = n = 2$ .

(b) Sei  $g \in GL_n(K)$  eine Diagonalmatrix mit paarweise verschiedenen Diagonaleinträgen. Dann ist  $\text{Cent}_{GL_n(K)}$  die Gruppe aller invertierbarer Diagonalmatrizen.

(c) Das Zentrum von  $GL_n(K)$  ist die Untergruppe aller Skalarmatrizen  $K^\times \cdot I_n$ .

(b)  $g = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$ ,  $B = (b_{ij})_{i,j} \in GL_n(K)$ :  $gB = Bg$  g.d.w.  $\forall i,j$ :  
 $\begin{matrix} \parallel & \parallel \\ (a_i b_{ij})_{i,j} & (a_j b_{ij})_{i,j} \end{matrix}$   $a_i b_{ij} = a_j b_{ij}$

$\Leftrightarrow \forall i,j: \underbrace{(a_i - a_j)}_{\neq 0 \text{ für } i \neq j} b_{ij} = 0. \Leftrightarrow \forall i \neq j: b_{ij} = 0. \Leftrightarrow B \text{ Diagonalmatrix.}$

(c)  $I_n + E_{ij} =: g$  für  $i \neq j$ .  $g \in GL_n(K) \Rightarrow gB = Bg$  g.d.w.  $\underline{(I_n + E_{ij})B} = \underline{B(I_n + E_{ij})}$   
 $\begin{pmatrix} 1 & & \\ & \ddots & \\ 1 & & \end{pmatrix} \quad E_{ij} = e_i \begin{pmatrix} & & 1 \\ & & \\ & & \end{pmatrix} = e_i e_j^T$   
 $\Leftrightarrow E_{ij} B = B E_{ij}$   
 $\Leftrightarrow e_i \cdot \underbrace{(e_j^T B)}_{\text{jetz hier}} = \underbrace{(B e_j)}_{\text{jetz hier}} e_i^T$   
 $\Leftrightarrow \dots B = \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$

$$(a) \quad \underbrace{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{\parallel} \underbrace{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}}_{\parallel} \\ \parallel \quad \begin{pmatrix} a & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a^{-1} \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow \forall a \in K^\times \text{ ist } \begin{pmatrix} 1 & a^{-1} \\ 0 & 1 \end{pmatrix} \in [a, a].$$

$$|K| > 2 \Rightarrow \forall b \in K: \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in [a, a].$$

$b \neq -1$ : schreibe  $b = a^{-1} \Rightarrow a \in K^\times$ .

$$\text{Wähle } c \in K \setminus \{0, 1\} \Rightarrow -1 = c - (c+1) \Rightarrow \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c+1 \\ 0 & 1 \end{pmatrix}^{-1} \in [a, a].$$

Analog:  $\forall b \in K: \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \in [a, a].$

$$\Rightarrow a, b, c, d \in K: \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}$$

Zeige: kann jedes Element von  $SL_2(K)$  so darstellen.

$$\Rightarrow [a, a] \supset SL_2(K).$$

$$\forall g, h \in GL_2(K): \det([g, h]) = \det(g h g^{-1} h^{-1}) = \det(g) \cdot \det(h) \cdot \det(g)^{-1} \cdot \det(h)^{-1} = 1$$

$$\text{Also } [h, h] \subset SL_2(K).$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(K).$$

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in SL_2(K), a \neq 0$$