# Algebra (Bachelor)

zur Vorlesung von Prof. Dr. Tobias Dyckerhoff

27. Oktober 2024

## Inhaltsverzeichnis



### Konventionen

- Wir schreiben für einen Körper $\mathbb{K}$ kurz $\mathbb{K}^* := \mathbb{K}\backslash\{0\}$.
- Real- und Imaginärteil werden mit $\mathrm{Re}(\cdot)$ respektive $\mathrm{Im}(\cdot)$ bezeichnet, das Bild einer Abbildung $f$ hingegen mit $\mathrm{im}(f)$.

Dies ist ein inoffizielles Skript zur Vorlesung Algebra bei Prof. Dr. Tobias Dyckerhoff im Wintersemester 24/25. Fehler und Verbesserungsvorschläge immer gerne an rasmus.raschke@uni-hamburg.de.

# 1 Gruppen und Symmetrie

**Bemerkung.** Wir möchten Gruppentheorie zunächst motivieren: Man betrachte einen Tetraeder. Um dessen Symmetrien zu erfassen, könnten wir z.B. schauen, welche Bewegungen diesen in sich selbst überführen. Es gibt vier Rotationsachsen, die eine Ecke und eine Fläche durchdringen und bei Rotation um 120° den Tetraeder in sich selbst überführen. Weiterhin gibt es drei 180°-Rotationsachsen mittig durch gegenüberliegende Kanten. Auch die Identität lässt den Tetraeder unverändert. Also gibt es $1 + 4 \cdot 2 + 3 = 12$ Symmetrien. Gruppen bieten eine Möglichkeit, solche Symmetrien und deren Verkettungen zu erfassen und zu untersuchen.

## 1.1 Grundbegriffe

**Definition 1.1.1. Gruppe**

Eine **Gruppe** ist ein Paar $(G, \circ)$, bestehend aus einer Menge[a] $G$ und einer Abbildung

$$\circ : G \times G \to G \tag{1.1.1}$$

$$(g, h) \mapsto g \circ h \tag{1.1.2}$$

mit folgenden Eigenschaften:

(G1) Für alle $g_1, g_2, g_3 \in G$ gilt das Assoziativgesetz: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

(G2) Es gibt ein Element $e \in G$, sodass gilt:

(2a) Für jedes $g \in G$ gilt $e \circ g = g$.

(2b) Für jedes $g \in G$ existiert ein $g' \in G$ mit $g' \circ g = e$.

Die Abbildung $\circ$ heißt **Verknüpfung**, ein Element $e \in G$ mit den Eigenschaften aus (2G) heißt **neutrales Element**, und ein Element $g' \in G$ zu gegebenem $g \in G$ mit Eigenschaft (2b) heißt **Inverses** von $g$.

[a] im ZFC-Axiomensystem

**Übung.** Sei $(G, \circ)$ eine Gruppe. Dann gelte:

1. Das neutrale Element $e \in G$ ist eindeutig bestimmt, außerdem gelte $\forall g \in G : g \circ e = g$.
2. Zu gegebenem $g \in G$ ist das Inverse $g' \in G$ eindeutig bestimmt und erfüllt zudem $g \circ g' = e$.
3. Für $n \geq 3$ hängt das Produkt von Gruppenelementen $g_1, g_2, \ldots, g_n$ nicht von der Klammerung ab.

**Lösung.** Zuerst zeigen wir Kommutativität des Inversen. Sei $g \in G$, dann gilt:

$$g \circ g^{-1} = (e \circ g) \circ g^{-1} = \left(\left(\left(g^{-1}\right)^{-1} \circ g^{-1}\right) \circ g\right) \circ g^{-1} = \left(\left(g^{-1}\right)^{-1} \circ \left(g^{-1} \circ g\right)\right) \circ g^{-1} \tag{1.1.3}$$

$$= \left(g^{-1}\right)^{-1} \circ \left(e \circ g^{-1}\right) = \left(g^{-1}\right)^{-1} \circ g^{-1} = e = g^{-1} \circ g, \tag{1.1.4}$$

also stimmen Links- und Rechtsinverses in Gruppen überein. Die Kommutativität des neutralen Elements folgt damit direkt aus:

$$g \circ e = g \circ (g^{-1} \circ g) = (g \circ g^{-1}) \circ g = (g^{-1} \circ g) \circ g = e \circ g, \tag{1.1.5}$$

womit auch Links-Einselement und Rechts-Einselement übereinstimmen. Für die Eindeutigkeit des Inversen seien $g^{-1}, g'^{-1} \in G$ zwei Inverse von $g \in G$. Dann gilt:

$$g^{-1} = g^{-1} \circ e = g^{-1} \circ (g'^{-1} \circ g) = g^{-1} \circ (g \circ g'^{-1}) = (g^{-1} \circ g) \circ g'^{-1} = e \circ g'^{-1} = g'^{-1}. \tag{1.1.6}$$

Weiterhin seien $e, e' \in G$ zwei Einselemente. Da $e = e \circ e' = e' \circ e = e$ gilt, ist das neutrale Element eindeutig. □

**Beispiele.** Wir geben einige Beispiele für Gruppen:

1. Die Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen $\mathbb{Z}$ mit der Addition $+$.
2. Für einen Körper $\mathbb{K}$ existiert die additive Gruppe $(\mathbb{K}, +)$ und die multiplikative Gruppe $(\mathbb{K}\backslash\{0\}, \cdot)$.
3. Für jede Menge $M$ existiert die **symmetrische Gruppe** $(\mathfrak{S}_M, \circ)$, wobei $\mathfrak{S}_M$ die Menge der bijektiven Selbstabbildungen von $M$ und $\circ$ die Komposition ist. Für $n \geq 1$ vereinbaren wir $\mathfrak{S}_n := \mathfrak{S}_{\{1,2,\ldots,n\}}$. Wir vereinbaren als Konvention die **Zykelschreibweise**. In $\mathfrak{S}_3$ beispielsweise ist ein Zykel

$$\sigma : \{1, 2, 3\} \to \{1, 2, 3\} \tag{1.1.7}$$

$$1 \mapsto 2 \tag{1.1.8}$$

$$2 \mapsto 1 \tag{1.1.9}$$

$$3 \mapsto 3, \tag{1.1.10}$$

   auch darstellbar als

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{1.1.11}$$

   oder einfacher als (12).
4. Für $n \geq 1$ und einen Körper $\mathbb{K}$ ist die **allgemeine lineare Gruppe** $(\mathrm{GL}(n, \mathbb{K}), \circ)$ definiert, wobei

$$\mathrm{GL}(n, \mathbb{K}) := \left\{A \in \mathbb{K}^{n \times n} \mid \det A \neq 0\right\} \tag{1.1.12}$$

   die Menge der invertierbaren $n \times n$-Matrizen mit Einträgen in $\mathbb{K}$ ist. Typische Beispiele für Körper sind $\mathbb{K} =$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$ mit $q = p^n$, $p$ prim.
ÜA: $|\mathrm{GL}(n, \mathbb{F}_q)| = ?$.

**Bemerkung.** Um den alltäglichen Gebrauch von Gruppen zu vereinfachen, machen wir folgende Vereinbarungen:

1. Wir bezeichnen $(G, \circ)$ üblicherweise einfach mit $G$ und lassen $\circ$ implizit.
2. Für $g, h \in G$ schreiben wir $gh = g \circ h$, für $e \in G$ schreiben wir 1 und für $g'$ schlicht $g^{-1}$.
3. Gilt $g \circ h = h \circ g$ für alle $g, h \in G$, so heißt $G$ **abelsch**. In diesem Fall wird die Verknüpfung oft mit $+$, das neutrale Element mit 0 und das inverse Element mit $-g$ bezeichnet.
4. Gemäß obiger ÜA zur Klammerung schreiben wir einfach $g_1 g_2 \cdots g_n \in G$ ohne Klammerung.

**Definition 1.1.2. Ordnung**

Für eine Gruppe $G$ bezeichnen wir die Kardinalität

$$|G| \in \mathbb{N} \cup \{+\infty\} \tag{1.1.13}$$

als **Ordnung** von $G$.

## 1.2 Untergruppen

**Definition 1.2.1. Untergruppe**

Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt **Untergruppe**, falls gilt:
(U1) $H \neq \emptyset$
(U2) Abgeschlossenheit: Für alle $a, b \in H$ gilt $ab^{-1} \in H$.
Wir verwenden dann die Notation $H \leq G$, um Untergruppen zu kennzeichnen.

**Bemerkung.** Übungsaufgabe: Sei $G$ eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt:

1. Aus Eigenschaft 1:Da $H \neq \emptyset$, existiert ein $a \in H$.
2. Aus Eigenschaft 2: $a \cdot a^{-1} = e \in H$.
3. Aus Eigenschaft 2: Für jedes $a \in H$ gilt $a^{-1} = e \cdot a^{-1} \in H$.
4. Aus Eigenschaft 2: Für jedes $a, b \in H$ gilt $ab = a \cdot (b^{-1})^{-1} \in H$.

Also: $H \subseteq G$ ist eine Untergruppe genau dann, wenn folgende alternativen Eigenschaften gelten:

1.* $e_G \in H$
2.* Für alle $a, b \in H$ muss $a \cdot b \in H$ gelten.
3.* Für alle $a \in H$ ist $a^{-1} \in H$.

Die andere Richtung der Äquivalenz ist trivial. Daraus folgt auch, dass $(H, \circ|_{H \times H})$ mit der auf $H$ eingeschränkten Verknüpfung $\circ|_{H \times H}$ eine Gruppe ist.

**Beispiele.** Einige Beispiele für Untergruppen sind:

1. $(G, \circ) = (\mathbb{R}, +)$ hat $(\mathbb{Z}, +)$ als Untergruppe mit $\mathbb{Z} \subseteq \mathbb{R}$.
2. Sei $n \geq 1$ und $\mathbb{K}$ ein Körper. Die **spezielle lineare Gruppe**
$$\mathrm{SL}(n, \mathbb{K}) := \{A \in \mathrm{GL}(n, \mathbb{K}) \mid \det A = 1\} \leq \mathrm{GL}(n, \mathbb{K}) \tag{1.2.1}$$
ist eine Untergruppe von $\mathrm{GL}(n, \mathbb{K})$.
3. Für $n \geq$ und einen Körper $\mathbb{K}$ ist die **orthogonale Gruppe**
$$\mathrm{O}(n, \mathbb{K}) := \left\{A \in \mathrm{GL}(n, \mathbb{K}) \mid A^T A = I_n\right\} \leq \mathrm{GL}(n, \mathbb{K}) \tag{1.2.2}$$
definiert, die auch eine Untergruppe von $\mathrm{GL}(n, \mathbb{K})$ ist.
4. Seien $H_1, H_2 \leq G$ Untergruppen. Dann ist $H_1 \cap H_2 \leq G$ auch eine Untergruppe. So kann z.B. die **spezielle orthogonale Gruppe**
$$\mathrm{SO}(n, \mathbb{K}) := \mathrm{O}(n, \mathbb{K}) \cap \mathrm{SL}(n, \mathbb{K}) \tag{1.2.3}$$
als Untergruppe von $\mathrm{GL}(n, \mathbb{K})$ konstruiert werden.
5. Etwas allgemeiner: Für jede Familie $\{H_i\}_{i \in I}$ von Untergruppen $H_i \leq G$ gilt, dass
$$\bigcap_{i \in I} H_i \leq G \tag{1.2.4}$$
wieder eine Untergruppe ist.

**Definition 1.2.2. Erzeugte Untergruppe**

Sei $G$ eine Gruppe und $M \subseteq G$ eine beliebige Teilmenge. Dann heißt die **Untergruppe**

$$\langle M \rangle := \bigcup_{M \subseteq H \leq G} H \leq G \tag{1.2.5}$$

die **von $M$ erzeugte Untergruppe** von $G$. Falls $M = \{g\} \leq G$ eine einelementige Menge ist, schreiben wir

$$\langle g \rangle := \langle \{g\} \rangle \leq G. \tag{1.2.6}$$

**Definition 1.2.3. Ordnung eines Elements**

Sei $G$ eine Gruppe und $g \in G$ ein Element. Dann heißt die Kardinalität

$$\operatorname{ord}(g) := |\langle g \rangle| \in \mathbb{N} \cup \{\infty\} \tag{1.2.7}$$

die **Ordnung von** $g$.

**Satz 1.2.4. Charakterisierung von einelementigen Untergruppen**

Sei $G$ eine Gruppe und $g \in G$ ein Element.

1. Falls $\operatorname{ord}(g) < \infty$, dann gilt
$$\operatorname{ord}(g) = \min\{k \geq 1 | g^k = 1\} \tag{1.2.8}$$
und
$$\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}, \tag{1.2.9}$$
wobei $n := \operatorname{ord}(g)$.
2. Falls $\operatorname{ord}(g) = \infty$, dann gilt
$$\langle g \rangle = \{g^i | i \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, 1, g^1, g^2, \dots\}, \tag{1.2.10}$$
wobei die Potenzen $g^i$, $i \in \mathbb{Z}$ paarweise verschiedene Elemente in $G$ sind.

**Beweis.** Zunächst gilt für beliebiges $g \in G$ das Folgende:

$$\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\} = \{g^i | i \in \mathbb{Z}\}, \tag{1.2.11}$$

wobei die Potenzen im Allgemeinen nicht notwendigerweise paarweise verschieden sind. Dies folgt, da, damit $\langle g \rangle$ eine Untergruppe sein kann, zunächst das neutrale Element $1 = g^0$ und $g$ selbst enthalten sein muss. Dann muss aber auch die Selbstverknüpfung und das Inverse (sowie dessen Selbstverknüpfungen) enthalten sein.

1. Sei $\operatorname{ord}(g) < \infty$. Dann gibt es insbesondere $i, j \in \mathbb{Z}$ mit $i \neq j$ und $g^i = g^j$. O.B.d.A. sei $i > j$. Dann ist also $k = i - j \geq 1$ eine natürliche Zahl, für die gilt: $g^k = 1$. Nach dem Wohlordnungssatz existiert eine *kleinste* natürliche Zahl $n \geq 1$, für die gilt: $g^n = 1$. Sei nun $m \in \mathbb{Z}$. Dann gibt es eindeutig bestimmte Zahlen $a \in \mathbb{Z}$ und $0 \leq r < n$, sodass
$$m = an + r. \tag{1.2.12}$$
Damit folgt
$$g^m = g^{an+r} = (\underbrace{g^n}_{=1})^a \cdot g^r = g^r. \tag{1.2.13}$$
Dies impliziert $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$, da $r$ der Rest ist, der bei der Division von $n$ durch $m$ bleibt. Die möglichen Reste für gegebenes $n$ legen also die Elemente von $G$ fest.
Wir müssen noch zeigen, dass $1, g, \dots, g^{n-1}$ paarweise verschieden sind. Dies folgt allerdings direkt aus der Tatsache, dass $n$ minimal ist.
2. Das obige Argument zeigt per Kontraposition auch 2., denn wenn die Potenzen $g^i$, $i \in \mathbb{Z}$ nicht paarweise verschieden sind, dann zeigt obiges Argument, dass $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$ für $n \in \mathbb{N}$, was ein Widerspruch zur Annahme $\operatorname{ord}(g) = \infty$ ist.

□

**Definition 1.2.5. zyklische Gruppe**

Sei $G$ eine Gruppe. Existiert ein $g \in G$, sodass sich jedes $h \in G$ als $g^n = h$ für ein $n \in \mathbb{Z}$ schreiben lässt, heißt $G$ **zyklisch der Ordnung** $\operatorname{ord}(g)$. Das Element $g$ heißt **Erzeuger von** $G$.

## 1.3 Homomorphismen

**Definition 1.3.1. Homomorphismus**

Seien $G$ und $G'$ Gruppen. Eine Abbildung

$$\phi : G \to G' \tag{1.3.1}$$

heißt **(Gruppen-)Homomorphismus**, falls gilt:

(H1) Für alle $g, h \in G$ gilt
$$\phi(gh) = \phi(g) \cdot \phi(h). \tag{1.3.2}$$
Die Menge der Homomorphismen von $G$ nach $G'$ wird mit $\operatorname{Hom}(G, G')$ bezeichnet.

**Bemerkung.** Jeder Homomorphismus erfüllt außerdem folgende Eigenschaften, die aus Definition 1.3.1 folgen:

(H2) $\phi(1_G) = 1_{G'}$

(H3) Für alle $g \in G$ gilt $\phi(g^{-1}) = \phi(g)^{-1}$.

Das sieht man schnell, da $\phi(1) = \phi(1g) = \phi(1)\phi(g)$ gilt, also $\phi(1) = 1'$ sein muss. Weiterhin gilt $1' = \phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$, Linksmultiplikation mit $\phi^{-1}(g)$ liefert (H3).

**Beispiele.** 1. Die **Einbettung** $\phi : H \hookrightarrow G$ einer Untergruppe $H \leq G$ ist ein Homomorphismus.

2. Die **Determinantenabbildung**
$$\det : \mathrm{GL}(n, \mathbb{K}) \to (\mathbb{K}\backslash\{0\}, \cdot) \tag{1.3.3}$$
ist ein Homomorphismus.

3. Für $n \geq 1$ und einen Körper $\mathbb{K}$ ist die Permutationsabbildung
$$P : \mathfrak{S}_n \to \mathrm{GL}(n, \mathbb{K}) \tag{1.3.4}$$
$$\sigma \mapsto P_\sigma, \tag{1.3.5}$$
mit der **Permutation**
$$(P_\sigma)_{ij} := \begin{cases} 1 \,\text{falls}\, i = \sigma(j) \\ 0 \,\text{sonst} \end{cases} \tag{1.3.6}$$
ein Homomorphismus. *Der Beweis sei dem Leser überlassen.* Für $\sigma = (123) \in \mathfrak{S}_3$ gilt z.B.
$$P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{1.3.7}$$

4. Sei $G$ eine Gruppe und $g \in G$. Dann ist
$$\gamma_g : G \to G \tag{1.3.8}$$
$$h \mapsto ghg^{-1} \tag{1.3.9}$$
ein Homomorphismus, genannt **Konjugation mit** $g$.

5. Sei $G$ eine Gruppe und $g \in G$. Dann ist
$$\mathbb{Z} \to G \tag{1.3.10}$$
$$i \mapsto g^i \tag{1.3.11}$$
ein Homomorphismus von $(\mathbb{Z}, +)$ nach $(G, \circ)$.

**Definition 1.3.2. Isomorphismus**

Sei $\phi$ ein Gruppenhomomorphismus, der zusätzlich bijektiv ist. Dann heißt $\phi$ **Isomorphismus**. Zwei Gruppen $G$ und $G'$ heißen **isomorph**, in Zeichen $G \cong G'$, falls es einen Isomorphismus zwischen ihnen gibt.

**Bemerkung.** Anschaulich bedeutet das, dass zwei isomorphe Gruppen identisch bis auf Umbenennung ihrer Elemente sind.

**Beispiele.** 1. Die Permutationsabbildung $P$ induziert einen Isomorphismus
$$P : \mathfrak{S}_n \to P(n, \mathbb{K}) \tag{1.3.12}$$
$$\sigma \mapsto P_\sigma \tag{1.3.13}$$
zwischen der symmetrischen Gruppe und der Untergruppe der Permuationsmatrizen. Letztere sind Matrizen, die in jeder Zeile und Spalte *genau eine* 1 und sonst 0 haben. *Der Beweis sei dem Leser überlassen.*

2. Die **Exponentialfunktion**
$$\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot) \tag{1.3.14}$$
und ihre Umkehrfunktion, gegeben durch den **Logarithmus**
$$\ln : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +), \tag{1.3.15}$$
bilden einen Isomorphismus, also gilt $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.

**Definition 1.3.3. Bild und Kern**

Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann heißt die Teilmenge
$$\mathrm{im}(\phi) := \{g' \in G' | \exists g \in G : \phi(g) = g'\} \leq G', \tag{1.3.16}$$
das **Bild von** $\phi$ und die Teilmenge
$$\ker(\phi) := \{g \in G | \phi(g) = 1_{G'}\} \leq G, \tag{1.3.17}$$
der **Kern von** $\phi$.

**Satz 1.3.4. Bild und Kern sind Untergruppen**

Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann sind $\mathrm{im}(\phi) \leq G'$ und $\ker(\phi) \leq G$ Untergruppen der jeweiligen Gruppen $G$ und $G'$.

**Beweis.** Nachrechnen mittels (H1), (H2) und (H3), exemplarisch für den Kern gezeigt:

1. (U1) ist erfüllt, da $1_G \in \ker(\phi)$ wegen (H2) gilt.

2. (U2) kann nachgerechnet werden. Seien dafür $g, h \in \ker(\phi)$:
$$\phi(gh^{-1}) =^{(H1)} \phi(g) \cdot \phi(h^{-1}) =^{(H3)} \phi(g) \cdot \phi(h)^{-1} = 1_{G'}, \tag{1.3.18}$$
also $gh^{-1} \in \ker(\phi)$.

□

**Satz 1.3.5**

Für einen Homomorphismus $\phi : G \to G'$ sind folgende Aussagen äquivalent:

(i) $\phi$ ist injektiv.

(ii) $\ker(\phi) = \{1\}$

**Beweis.** (i) $\Rightarrow$ (ii) ist offensichtlich. Wir zeigen noch (ii) $\Rightarrow$ (i): Sei also $\ker(\phi) = \{1\}$ und $g, h \in G$ mit $\phi(g) = \phi(h)$. Dann gilt $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = 1$, also ist $gh^{-1} \in \ker(\phi) = \{1\}$ und damit $g = h$. □

**Definition 1.3.6. Links- und Rechtsnebenklassen**

Sei $G$ eine Gruppe und $H \leq G$ eine Untergruppen. Dann ist die **Linksnebenklasse von $H$ bezüglich** $g \in G$ als
$$gH := \{gh \,|\, h \in H\} \tag{1.3.19}$$
und die **Rechtsnebenklasse von $H$ bezüglich** $g \in G$ als
$$Hg := \{hg \,|\, h \in H\} \tag{1.3.20}$$
definiert.

**Satz 1.3.7. Nebenklassen sind Äquivalenzklassen**

Sei $G$ eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt:

1. Die Linksnebenklassen sind die Äquivalenzklassen bezüglich der Äquivalenzrelation
$$a \sim_L b :\Leftrightarrow b^{-1}a \in H \tag{1.3.21}$$
auf $G$.
2. Die Rechtsnebenklassen sind die Äquivalenzklassen bezüglich der analogen Äquivalenzrelation
$$a \sim_R b :\Leftrightarrow ab^{-1} \in H. \tag{1.3.22}$$

**Übung.** Beweis des Satzes.

**Lösung.** Zunächst ist zu zeigen, dass tatsächlich eine Äquivalenzrelation definiert wird.

(a) Reflexivität: Sei $a \in G$. Dann gilt $a^{-1}a = 1 \in H$, also ist $a \sim_L a$.

(b) Symmetrie: Seien $a, b \in G$ mit $a \sim_L b$. Dann gilt $a^{-1}b = h$ für ein $h \in H$. Daraus folgt:
$$a = bh \Leftrightarrow ah^{-1} = b \Leftrightarrow a^{-1}b = h^{-1} \in H, \tag{1.3.23}$$
also ist auch $b \sim_L a$, da $H$ abgeschlossen unter Inversenbildung ist.

(c) Transitivität: Seien $a, b, c \in G$ mit $a \sim_L b$ und $b \sim_L c$. Dann gilt $b^{-1}a = h \in H$ und $c^{-1}b = h' \in H$. Also folgt $H \ni h'h = c^{-1}bb^{-1}a = c^{-1}a$ und damit die Behauptung.

Ist nun $g \in G$ und $h \in H$, so besteht die Äquivalenzklasse von $g$ unter $\sim_L$ aus allen Elementen der Form $ah$ mit $a \in G$, $h \in H$. Die Vereinigung aller Äquivalenzklassen muss also per Konstruktion ganz $gH$ sein. Der Beweis für $\sim_R$ ist dual dazu. □

Damit bezeichnen wir die Menge der Linksnebenklassen von $H$ mit $G/H = G/_{\sim_L}$ und die der Rechtsnebenklassen mit $G\backslash H = G/_{\sim_R}$.

**Definition 1.3.8. Index**

Die Kardinalität
$$(G : H) := |G/H| \in \mathbb{N} \cup \{\infty\} \tag{1.3.24}$$
heißt **Index von $H$ in $G$.**

Man beachte, dass $|H/G| = |H\backslash G|$ gilt, da die Abbildung Tafel nicht hochgeschoben.... 

**Theorem 1.3.9. Satz von Lagrange**

Sei $G$ eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt
$$|G| = (G : H) \cdot |H|. \tag{1.3.25}$$
Ist $|G| < \infty$, so gilt insbesonders
$$(G : H) = \frac{|G|}{|H|} = |G/H|\,. \tag{1.3.26}$$

**Beweis.** Dies ist ein direktes Korollar von Satz 1.3.7: Als Äquivalenzklassen bzgl. einer Äquivalenzrelation bilden die Linksklassen eine Partition von $G$, also

$$G = \bigsqcup_{gH \in G/H} gH. \tag{1.3.27}$$

Es gilt zudem für alle $g \in G$, dass $|gH| = |H|$, da Linksmultiplikation mit $g$, definiert durch

$$G \to G \tag{1.3.28}$$

$$x \mapsto gx, \tag{1.3.29}$$

bijektiv ist, also eine Bijektion $H \to gH$ induziert. Insbesondere gilt für jedes $g \in G$, dass $\operatorname{ord}(g) \mid |G|$. □

**Definition 1.3.10. Normalteiler**

Eine Untergruppe $N \leq G$ heißt **normal** oder **Normalteiler**, falls für alle $g \in G$

$$gN = Ng \tag{1.3.30}$$

gilt. Wir schreiben dafür $N \trianglelefteq G$.

**Bemerkung.** Eine Untergruppe $N \leq G$ ist normal genau dann, wenn für alle $g \in G$ und $n \in N$ gilt:

$$gng^{-1} \in N, \tag{1.3.31}$$

also $N$ abgeschlossen unter Konjugation mit beliebigen Elementen aus $G$ ist.

**Satz 1.3.11**

Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann gilt $\ker(\phi) \trianglelefteq G$.

**Beweis.** Sei $g \in G$ und $x \in \ker(\phi)$, also $\phi(x) = 1$. Dann gilt auch

$$\phi(gxg^{-1}) = \phi(g)\underbrace{\phi(x)}_{=1}\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1. \tag{1.3.32}$$

□

**Beispiele.** Wir betrachteten einige Beispiele für Normalteiler:

1. Sei $n \geq 1$ und $\mathbb{K}$ ein Körper. Für
$$\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^* \tag{1.3.33}$$
gilt
$$\ker(\det) = \mathrm{SL}(n, \mathbb{K}) \trianglelefteq \mathrm{GL}(n, \mathbb{K}). \tag{1.3.34}$$
2. Betrachte für $n \geq 1$ die Komposition
$$\mathfrak{S}_n \xrightarrow{P} P(n, \mathbb{Q}) \xrightarrow{\det} \{+1, -1\}.$$
Also ist
$$A_n := \ker(\mathrm{sgn}) \trianglelefteq \mathfrak{S}_n \tag{1.3.35}$$
normal. $A_n$ heißt **alternierende Gruppe**.

**Satz 1.3.12. Gruppenstuktur auf Nebenklassen**

Sei $G$ eine Gruppe und $N \trianglelefteq G$. Dann gilt:

1. Auf der Menge $G/N$ von Nebenklassen von $N$ existiert eine Gruppenstruktur mit Verknüpfung
$$G/N \times G/N \to G/N \tag{1.3.36}$$
$$(aN, bN) \mapsto abN. \tag{1.3.37}$$
2. Die Quotientenabbildung
$$\pi : G \to G/N \tag{1.3.38}$$
$$a \mapsto aN \tag{1.3.39}$$
ist ein Gruppenhomomorphismus mit $\ker(\pi) = N$.

**Beweis.**

1. Zunächst muss die Wohldefiniertheit der Verknüpfung bewiesen werden. Seien $\widetilde{a} \in aN$ und $\widetilde{b} \in bN$ Vertreter der Nebenklassen $aN$ und $bN$ ($\Leftrightarrow \widetilde{a}N = aN$). Dann existieren $m, n \in N$ mit $\widetilde{a} = am$ und $\widetilde{b} = bn$. Nun gilt
$$\widetilde{a} \cdot \widetilde{b} = am \circ bn = ab \circ \underbrace{b^{-1}mb}_{N \trianglelefteq G \Rightarrow \in N} \circ n \in N, \tag{1.3.40}$$
also ist der Ausdruck wohldefiniert.
(G1) Seien $aN, bN, cN \in G/N$. Dann gilt
$$(aN \cdot bN) \cdot cN =^{\text{(G1) für G}} (ab)cN = a(bc)N = aN(bN \cdot cN). \tag{1.3.41}$$
(G2) Neutrales Element: $1 \cdot N = N$

(G3) Inverses Element: $(aN)^{-1} = a^{-1}N$

2. Es gilt
$$\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b) \tag{1.3.42}$$
nach Definition von $\pi$, also ist $\pi$ ein Homomorphismus. Darüber hinaus gilt
$$a \in \ker(\pi) \Leftrightarrow \pi(a) = 1_{G/H} = N \Leftrightarrow aN = N \Leftrightarrow a \in N, \tag{1.3.43}$$
also gilt $\ker(\pi) = N$.

□

**Satz 1.3.13. Homomorphiesatz (erster Isomorphiesatz)**

Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann induziert $\phi$ einen Isomorphismus
$$\overline{\phi} : G/\ker(\phi) \to \operatorname{im}(\phi) \tag{1.3.44}$$
$$g\ker(\phi) \mapsto \phi(g). \tag{1.3.45}$$

**Beweis.** Zunächst ist Wohldefiniertheit zu zeigen. Für $\widetilde{g} \in gN$, also $\widetilde{g} = gn$ für $n \in \ker(\phi)$, gilt:
$$\phi(\widetilde{g}) = \phi(gn) = \phi(g)\underbrace{\phi(n)}_{=1} = \phi(g), \tag{1.3.46}$$
also ist die Abbildung wohldefiniert.
Die Surjektivität von $\overline{\phi}$ ist trivial. Wir wissen, dass $\overline{\phi}$ genau dann injektiv ist, wenn $\ker(\overline{\phi}) = \{1_{G/\ker(\phi)}\} = \ker(\phi)$.
Wir rechnen nach:
$$g\ker(\phi) \in \ker(\overline{\phi}) \Leftrightarrow \phi(g) = 1_{G'} \Leftrightarrow g \in \ker(\phi) \Leftrightarrow g\ker(\phi) = \ker(\phi) \tag{1.3.47}$$
□

**Beispiel.** Wir können die Vorzeichenfunktion
$$\operatorname{sgn} : \mathfrak{S}_n \to \{\pm 1\} \tag{1.3.48}$$
betrachten, dann ist $\ker \operatorname{sgn} = A_n \trianglelefteq \mathfrak{S}_n$, also erhalten wir einen Isomorphismus
$$\mathfrak{S}_n/A_n \to \{\pm 1\}. \tag{1.3.49}$$
Insbesondere gilt $\mathfrak{S}_n : A_n = 2$.

**Korollar 1.3.14** (Korollar aus Satz 1.3.13)**.** Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann lässt sich $\phi$ schreiben als
$$\phi = \iota \circ \overline{\phi} \circ \pi, \tag{1.3.50}$$
wobei:

1. $\pi : G \to G/\ker(\phi)$ der surjektive Quotientenkern ist.
2. $\overline{\phi} : G/\ker(\phi) \to \operatorname{im}(\phi)$ der Isomorphismus aus 1.3.13 ist.
3. $\iota : \operatorname{im}(\phi) \hookrightarrow G'$ die injektive Einbettung von $\operatorname{im}(\phi) \leq G'$ ist.

Das ist äquivalent dazu, dass folgendes Diagramm kommutiert:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \iota} \\ G/\ker(\phi) & \xrightarrow[\overline{\phi}]{\cong} & \operatorname{im}(\phi) \end{array}$$

Ausgedrückt in Elementen:

$$\begin{array}{ccc} g & \longmapsto & \phi(g) \\ \downarrow & & \uparrow \\ g\ker(\phi) & \longmapsto & \phi(g) \end{array}$$

**Beispiele.**

1. Für $n \geq 1$ und einen Körper $\mathbb{K}$ induziert der Homomorphismus
$$\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^* \tag{1.3.51}$$
einen Isomorphismus
$$\mathrm{GL}(n, \mathbb{K})/\mathrm{SL}(n, \mathbb{K}) \to \mathbb{K}^*. \tag{1.3.52}$$
2. Ein weiterer induzierter Isomorphismus ist
$$\overline{\operatorname{sgn}} : \mathfrak{S}_n/A_n \to \{\pm 1\}. \tag{1.3.53}$$
3. Sei $G$ eine Gruppe mit $g \in G$. Betrachte den Homomorphismus
$$\phi : (\mathbb{Z}, +) \to G, i \mapsto g^i. \tag{1.3.54}$$
   (a) Falls $\operatorname{ord}(g) = \infty$, gilt $\ker(\phi) = \{0\}$ und $\phi$ induziert einen Isomorphismus

$$\mathbb{Z} \xrightarrow[\cong]{\pi} \mathbb{Z}/\{0\} \xrightarrow[\cong]{\overline{\phi}} \langle g \rangle \qquad \phi$$

(b) Falls $\operatorname{ord}(g) = N < \infty$, dann gilt

$$\ker(\phi) = N \cdot \mathbb{Z} \tag{1.3.55}$$

und $\phi$ induziert einen Isomorphismus

$$\overline{\phi} : \mathbb{Z}/_{N\mathbb{Z}} \xrightarrow{\cong} \langle g \rangle.$$

# 1.4 Gruppenwirkung

**Definition 1.4.1. Gruppenoperation**

Eine **Operation** oder **Wirkung** einer Gruppe $G$ auf einer Menge $M$ ist eine Abbildung

$$G \times M \to M \tag{1.4.1}$$
$$(g, x) \mapsto g.x, \tag{1.4.2}$$

sodass gilt:

(O1) Für alle $g, h \in G$ und $x \in M$ gilt: $g.(h.x) = (g \cdot h).x$.

(O2) Für alle $x \in M$ gilt: $1.x = x$.

Dann sagen wir, dass $G$ auf $M$ **operiert** und schreiben $G \curvearrowright M$.

**Beispiele.**

1. Jede Gruppe $G$ operiert auf sich selbst via
   (a) **Linkstranslation**: $G \times G \to G$, $(g, h) \mapsto gh$ und
   (b) **Rechtstranslation**: $G \times G \to G$, $(g, h) \mapsto hg^{-1}$, aber auch durch
   (c) **Konjugation**: $G \times G \to G$, $(g, h) \mapsto ghg^{-1}$.
2. Für jede Menge $M$ operiert die symmetrische Gruppe $\mathfrak{S}_M$ auf $M$ via
$$\mathfrak{S}_M \times M \to M$$
$$(\sigma, x) \mapsto \sigma(x). \tag{1.4.3}$$
3. Für $n \geq 1$ und einen Körper $\mathbb{K}$ operiert die Gruppe $\mathrm{GL}(n, \mathbb{K})$ auf $\mathbb{K}^n$ via
$$\mathrm{GL}(n, \mathbb{K}) \times \mathbb{K}^n \to \mathbb{K}^n$$
$$(A, v) \mapsto Av. \tag{1.4.4}$$

**Definition 1.4.2. Äquivarianz**

Für Operationen $G \curvearrowright M$ und $G \curvearrowright N$ heißt eine Abbildung (von Mengen) $f : M \to N$ $G$-**äquivariant**, falls für alle $g \in G$ und $x \in M$ gilt:

$$f(g.x) = g.f(x). \tag{1.4.5}$$

**Definition 1.4.3. Bahnen**

Sei $G \curvearrowright M$ eine Operation von $G$ auf $M$. Die Relation

$$x \sim_G g :\Leftrightarrow \exists g \in G : g.x = g \tag{1.4.6}$$

definiert eine Äquivalenzrelation auf $M$. Die Äquivalenzklassen sind die Mengen der Form

$$G.x := \{g.x | g \in G\} \tag{1.4.7}$$

für $x \in M$, die **Bahnen** von $x$ unter $G \curvearrowright M$ genannt werden. Die Quotientenmenge

$$M\backslash G := M/_{\sim_G} \tag{1.4.8}$$

heißt **Bahnenraum von** $G \curvearrowright M$.

**Beweis.** *Das Nachweisen der Relationseigenschaften der Äquivalenzrelation ist dem Leser überlassen.* □

**Beispiel.** Betrachte die Rotationsgruppe

$$G = \mathrm{SO}(2, \mathbb{R}) := \mathrm{SL}(2, \mathbb{R}) \cap O(2, \mathbb{R}) = \left\{ \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \,\middle|\, \phi \in \mathbb{R}/_{2\pi\mathbb{Z}} \right\} \leq \mathrm{GL}(2, \mathbb{R}). \tag{1.4.9}$$

Wir erhalten Operationen

$$\mathrm{SO}(2, \mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2$$
$$(A, v) \mapsto Av, \tag{1.4.10}$$

deren Bahnen konzentrische Kreise im $\mathbb{R}^2$ sind. Dadurch wird eine Partition von $\mathbb{R}^2$ erreicht.

**Definition 1.4.4. Stabilisator, Fixpunkte und Transitivität**

Sei $G \curvearrowright M$ eine Operation.

(i) Für $x \in M$ heißt die Untergruppe
$$G_x := \{g \in G | g.x = x\} \leq G \tag{1.4.11}$$
der **Stabilisator von** $x$.

(ii) Ein Punkt $x \in M$ heißt **Fixpunkt von** $G \curvearrowright M$, falls $G_x = G$. Die Menge aller Fixpunkte wird mit
$$M^G \subseteq M \tag{1.4.12}$$
bezeichnet.

(iii) Die Operation $G \curvearrowright M$ heißt **transitiv**, falls für jedes $x \in M$ gilt, dass $G.x = M$ ist, also genau eine Bahn existiert.

**Beispiel.** Bleiben wir bei vorigem Beispiel, so hat ein Vektor $v \neq (0,0)$ nur die Identität id als Stabilisator. Der Nullvektor wird hingegen von ganz $\mathrm{SO}(2,\mathbb{R})$ stabilisiert. Es scheint einen Zusammenhang zwischen der Größe des Stabilisators und der Bahn zu geben.

**Satz 1.4.5. Bahnformel**

Sei $G \curvearrowright M$ eine Operation auf $M$ und $x \in M$. Dann definiert
$$\begin{aligned} G/_{G_x} &\to G.x \\ gG_x &\mapsto g.x \end{aligned} \tag{1.4.13}$$
eine bijektive, $G$-äquivariante Abbildung, wobei $G \curvearrowright G.x$ durch Einschränkung von $G \curvearrowright M$ gegeben ist. Insbesondere gilt die **Bahnformel**
$$|G.x| = (G : G_x). \tag{1.4.14}$$
Eine Wirkung $G \curvearrowright G/_{G_x} = \{gG_x | g \in G\}$ erhält man durch $g'.gG_x := g'g.G_x$.

**Beweis.** Die Abbildung ist wohldefiniert: Sei $g \in G$ und $h \in G_x$, dann gilt
$$(gh).x = g.(h.x) = g.x. \tag{1.4.15}$$
Weiterhin ist die Abbilung injektiv, denn falls $g_1.x = g_2.x$, so ist $(g_1^{-1}).g_2.x = x$, also ist $(g_1^{-1}).g_2 \in G_x$, also $g_1 G_x = g_2 G_x$. Surjektivität ist per Konstruktion durch Einschränkung auf die Bahn gegeben. □