Algebra (Bachelor)

zur Vorlesung von Prof. Dr. Tobias Dyckerhoff

15. November 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 $\mathrm{im}(f)$.
- Echte Teilmengen tragen das Symbol $\subset$, allgemeine Teilmengen das Symbol $\subseteq$.

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 ϕ ein Gruppenhomomorphismus, der zusätzlich bijektiv ist. Dann heißt ϕ **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** ϕ und die Teilmenge
$$\ker(\phi) := \{g \in G | \phi(g) = 1_{G'}\} \leq G, \tag{1.3.17}$$
der **Kern von** ϕ.

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) ϕ 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 π, also ist π 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 ϕ 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 ϕ 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 ϕ 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 ϕ 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. □

Korollar 1.4.6 (Aus Satz 1.4.5)**.** Sei $G \curvearrowright M$ eine Wirkung und $|M| < \infty$. Dann gilt:
$$|M| = \sum_{G.x \in G\backslash M} |G.x| = \sum_{G.x \in G\backslash M} (G : G_x). \tag{1.4.16}$$

Bemerkung. Gleichung 1.4.16 lässt sich weiter vereinfachen zu
$$|M| = \left|M^G\right| + \sum_{G.x \in G\backslash M, G_x \neq G} (G : G_x). \tag{1.4.17}$$

Definition 1.4.7. Konjugationsklasse, Zentrum und Zentralisator

Wir definieren die Selbstwirkung $G \curvearrowright G$ Gruppe als
$$\begin{aligned} G \times G &\to G \\ (g,x) &\mapsto gxg^{-1}. \end{aligned} \tag{1.4.18}$$

1. Für $x \in G$ heißt die Bahn
$$[x] := G.x = \{gxg^{-1} | g \in G\} \tag{1.4.19}$$
Konjugationsklasse von x.
2. Die Menge der Fixpunkte
$$Z(G) := G^G = \{x \in G | gx = xg\} \leq G \tag{1.4.20}$$
heißt **Zentrum von** G und bildet eine Untergruppe.
3. Für $x \in G$ heißt der Stabilisator
$$C_G(x) := G_x = \{g \in G | gx = xg\} \tag{1.4.21}$$
auch **Zentralisator von** x.

Für $\mathrm{ord}(G) < \infty$ hat Gleichung 1.4.17 dann die Form
$$|G| = |Z(G)| + \sum_{[x] \in G\backslash G, C_G(x) \neq G} \underbrace{(G : C_G(x))}_{=|[x]|} \tag{1.4.22}$$
und heißt **Klassengleichung** von G. Alle Summanden der Klassengleichung teilen $\mathrm{ord}(G)$.

Übung. Zeigen Sie, dass das Zentrum von G eine Untergruppe bildet.

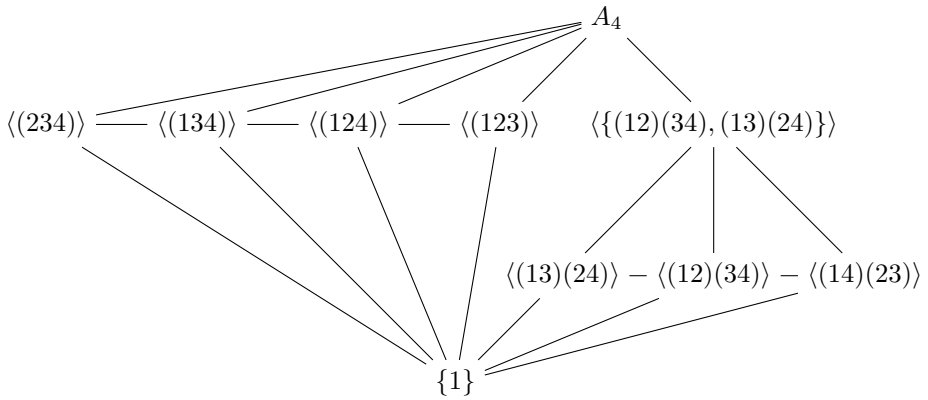
Beispiel. Wir wollen die Untergruppenstruktur von $A_4 \trianglelefteq \mathfrak{S}_4$ verstehen. Dazu bestimmen wir die Klassengleichung der Gruppe. Es gilt $(\mathfrak{S}_4 : A_4) = 2$, da $\mathfrak{S}_4/A_4 = \{\pm 1\}$. Aus dem Satz von Lagrange folgt

$$|A_4| = \frac{|\mathfrak{S}_4|}{(\mathfrak{S}_4 : A_4)} = 12. \tag{1.4.23}$$

Wir listen alle Elemente, sortiert nach Ordnung. Mögliche Ordnungen sind 1, 2, 3, 4, 6 und ~~12~~.

- Elemente der Ordnung 1: (1)
- Elemente der Ordnung 2: (12)(34), (13)(24), (14)(23)
- Elemente der Ordnung 3: (123) = (12) ∘ (23), (124), (134), (234), (142), (143), (243), (132)

Das es jeweils keine weiteren Elemente gibt, sieht man daran, dass die Ordnungen untereinander unter Verknüpfung abgeschlossen sind. Dass es insgesamt keine weiteren Elemente gibt, ist daran erkennbar, dass wir schon 12 Elemente haben.
Jetzt bestimmen wir das **Gitter** aller Untergruppen von A_4: Nach dem Satz von Lagrange ist die Ordnung der Untergruppen ein Teiler von 12.



Weiter geht es mit den Konjugationsklassen. Ganz allgemein gilt für $\sigma \in \mathfrak{S}_n$ und $(a_1 a_2 \cdots a_k) \in \mathfrak{S}_n$:

$$\sigma \circ (a_1 a_2 \cdots a_k) \circ \sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k)) \ (*), \tag{1.4.24}$$

also z.B.

$$(124) \circ (123) \circ (124)^{-1} = (124) \circ (123) \circ (142) = (1)(234) = (234). \tag{1.4.25}$$

Dies hilft, die Konjugationsklassen zu bestimmen. Diese sind:

$$[(1)] = \{(1)\} = Z(G) \tag{1.4.26}$$
$$[(12)(34)] = \{(12)(34), (13)(24), (14)(23)\} \tag{1.4.27}$$
$$[(123)] = \{(123), (142), (134), (243)\} \tag{1.4.28}$$
$$[(132)] = \{(132), (124), (143), (234)\} \tag{1.4.29}$$

Die Überlegung, dass die unteren beiden Konjugationsklassen nicht eine gemeinsame Konjugationsklasse bilden, folgt daraus, dass die Kardinalität der entstehenden Untergruppe 8 wäre, und 8 nicht 12 teilt. Damit haben wir die Klassengleichung bestimmt:

$$12 = 1 + 3 + 4 + 4 \tag{1.4.30}$$

Daraus können wir direkt ablesen, dass es keine Untergruppen der Ordnung 6 geben kann. Gäbe es nämlich eine solche Untergruppe $A \leq A_4$, hätte diese Index 2, und jede Gruppe von Index 2 ist normal. Damit wäre A normal, also eine Vereinigung von Konjugationsklassen von A_4. Dann müsste die Summe von Summanden der Klassengleichung 6 ergeben, das ist aber unmöglich.

Übung. Verifiziere $(*)$. Beweise, dass Untergruppen mit Index 2 normal sind. Zeige, dass normale Untergruppen als Vereinigung von Konjugationsklassen geschrieben werden können.

1.5 Euklidische Bewegungen

Wir beginnen mit einer Widerholdung von Grundbegriffen:

Definition 1.5.1. Skalarprodukt, Norm, Metrik

Sei $v = (v_1 \cdots v_n)^T, w = (w_1 \cdots w_n)^T \in \mathbb{R}^n$ mit $n \geq 1$. Wir definieren das **Skalarprodukt** von v mit w als

$$\langle v, w\rangle := \sum_{i=1}^{n} v_i w_i \in \mathbb{R} \tag{1.5.1}$$

und die **euklidische Norm**

$$\|v\| := \sqrt{\langle v, v\rangle} \in \mathbb{R}_{\geq 0}. \tag{1.5.2}$$

Dies induziert den **euklidischen Abstand**

$$d(v, w) := \|v - w\| \tag{1.5.3}$$

auf $\mathbb{R}^n$.

Daraus erhalten wir einen speziellen Isometriebegriff für den $\mathbb{R}^n$:

Definition 1.5.2. Euklidische Bewegung

Eine Abbildung

$$T : \mathbb{R}^n \to \mathbb{R}^n \tag{1.5.4}$$

heißt **(euklidische) Bewegung** oder **(euklidische) Isometrie**, falls für alle $v, w \in \mathbb{R}^n$ gilt:

$$d(Tv, Tw) = d(v, w). \tag{1.5.5}$$

Die Menge $E(n)$ der euklidischen Bewegungen mit der Komposition als Verknüpfung bildet eine Gruppe.

Bemerkung. Die Injektivität von $T \in E(n)$ ist klar, die Injektivität folgt aus untenstehendem Korollar 1.5.4.

Beispiele. Wir schauen uns Beispiele für euklidische Isometrien an:

1. Für jedes $b \in \mathbb{R}^n$ sind die **Translationen**
$$\begin{aligned} \tau_b : \mathbb{R}^n &\to \mathbb{R}^n \\ v &\mapsto v + b \end{aligned} \tag{1.5.6}$$
Isometrien.
2. Für jede Matrix $A \in \mathrm{O}(n, \mathbb{R})$ ist die Abbildung
$$\begin{aligned} \mu_A : \mathbb{R}^n &\to \mathbb{R}^n \\ v &\mapsto Av \end{aligned} \tag{1.5.7}$$
eine Isometrie, denn es gilt $\langle v, w\rangle = v^T w$, und damit
$$\langle Av, Aw\rangle = (Av)^T Aw = v^T A^T Aw = v^T w = \langle v, w\rangle. \tag{1.5.8}$$
Für den Abstand gilt dann:
$$d(Av, Aw) = \|Av - Aw\| = \|A(v - w)\| = \sqrt{\langle A(v - w), A(v - w)\rangle} = \|v - w\| = d(v, w), \tag{1.5.9}$$
also ist μ_A tatsächlich eine euklidische Isometrie.

Satz 1.5.3. Euklidische Bewegungen sind orthogonale Transformationen

Sei $T \in E(n)$ mit $T(0) = 0$. Dann existiert ein $A \in \mathrm{O}(n, \mathbb{R})$, sodass $T = \mu_A$.

Beweis.

1. Zuerst zeigen wir, dass T das Skalarprodukt erhält:
$$T \in E(n) \Rightarrow \langle Tv - Tw, Tv - Tw\rangle = d(Tv, Tw)^2 = \langle v - w, v - w\rangle\ (*). \tag{1.5.10}$$
Setze $w = 0$. Dann gilt
$$\langle Tv, Tv\rangle = Tv - T0 = \langle v - 0, v - 0\rangle = \langle v, v\rangle \tag{1.5.11}$$
Mit der Bilinearität des Skalarprodukts erhalten wir
$$\langle Tv, Tv\rangle - \langle Tv, Tw\rangle - \langle Tw, Tv\rangle + \langle Tw, Tw\rangle =^{(*)} \langle v, v\rangle - \langle v, w\rangle - \langle w, v\rangle + \langle w, w\rangle. \tag{1.5.12}$$
Da das Skalarprodukt darüber hinaus symmetrisch ist, folgt
$$-2\langle Tv, Tw\rangle = -2\langle v, w\rangle. \tag{1.5.13}$$
2. Falls zusätzlich für alle $1 \leq i \leq n$ gilt, dass $Te_i = e_i$, so ist $T = \mathrm{id}$. Für $v \in \mathbb{R}^n$ gilt dann:
$$(Tv)_i = \langle Tv, e_i\rangle = \langle Tv, Te_i\rangle = \langle v, e_i\rangle = v_i. \tag{1.5.14}$$
3. Sei nun T wieder allgemein mit $T(0) = 0$. Setze
$$A := (Te_1 Te_2 \cdots Te_n) \in \mathbb{R}^{n \times n} \tag{1.5.15}$$
mit Spaltenvektoren Te_i. Wegen $\langle Te_i, Te_j\rangle =^1 \langle e_i, e_j\rangle$ gilt $A \in \mathrm{O}(n, \mathbb{R})$. Zudem ist $\mu_{A^T} \circ T =: \widetilde{T} \in E(n)$ mit $\widetilde{T}(0) = 0$ für alle i. Also $\widetilde{T}e_i = e_i$ und damit $\widetilde{T} = \mathrm{id}$.

□

Korollar 1.5.4 (aus Satz 1.5.3)**.** Jede Isometrie $T \in E(n)$ ist von der Form
$$\begin{aligned} T : \mathbb{R}^n &\to \mathbb{R}^n \\ v &\mapsto Av + b \end{aligned} \tag{1.5.16}$$
für $A \in \mathrm{O}(n, \mathbb{R})$ und $b \in \mathbb{R}^n$.

Beweis. Sei $b := T(0)$. Dann gilt
$$\tau_{-b} \circ T(0) = 0. \tag{1.5.17}$$
Nach Satz 1.5.3 gilt $\tau_{-b} \circ T = \mu_A$ für $A \in \mathrm{O}(n, \mathbb{R})$. Also ist $T = \tau_b \circ \mu_A$. □

Definition 1.5.5. Direktes Produkt

Seien G und G' Gruppen. Dann heißt die Gruppe $G \times G'$ mit der Verknüpfung

$$\begin{aligned}(G \times G') \times (G \times G') &\to G \times G' \\ ((g,h),(g',h')) &\mapsto (g \circ g', h \circ h')\end{aligned} \tag{1.5.18}$$

direktes Produkt von G und G'.

Bemerkung. Es existiert also eine Bijektion

$$E(n) \cong \{(A,b) \mid A \in \mathrm{O}(n,\mathbb{R}), b \in \mathbb{R}^n\}, \tag{1.5.19}$$

wobei das Kompositionsgesetz durch

$$(A,b) \circ (A',b') = (AA', Ab' + b) \tag{1.5.20}$$

gegeben ist. Also ist $E(n) = O(n,\mathbb{R}) \times \mathbb{R}^n$ als Menge, aber nicht als Gruppe!

Definition 1.5.6. Semidirektes Produkt

Seien H und N Gruppen und wirke H auf N via Gruppenhomomorphismen, also:

1. $H \curvearrowright G$.
2. Für jedes $h \in H$ ist die Abbildung $N \to N$, $x \mapsto h.x$ ein Gruppenhomomorphismus.

Dann definieren wir eine Verknüpfung auf $H \times N$ durch:

$$\begin{aligned}\circ : (H \times N) \times (H \times N) &\to H \times N \\ ((h,x),(h',x')) &\mapsto ((hh', x(hx'))\,.\end{aligned} \tag{1.5.21}$$

Dies definiert eine Gruppenstruktur auf $H \times N$, genannt **semidirektes Produkt** $H \ltimes N$ von $(H, N, H \curvearrowright N)$.

Übung. Man zeige, dass $H \ltimes N$ tatsächlich eine Gruppe ist.

Beispiele.

1. Falls $H \curvearrowright N$ die triviale Wirkung ist, so ist $H \ltimes N = H \times N$.
2. Betrachte die Wirkung $\mathrm{O}(n,\mathbb{R}) \curvearrowright \mathbb{R}^n$ durch Matrixmultiplikation. Dann gilt $E(n) \cong \mathrm{O}(n,\mathbb{R}) \ltimes \mathbb{R}^n$ als Gruppen.
3. Sei $T \in E(2)$ mit $T(0) = 0$. Dann gilt $T = \mu_A$ mit $A \in \mathrm{O}(n,\mathbb{R})$. Falls T orientierungserhaltend ist, gilt sogar $A \in \mathrm{SO}(2,\mathbb{R})$, also
$$A = \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix} \tag{1.5.22}$$
für $\theta \in \mathbb{R}/2\pi\mathbb{Z}$. Also sind die Isometrien der Form $\mu_A, A \in \mathrm{SO}(2,\mathbb{R})$ genau die Drehungen um den Ursprung. Alle Bewegungen $T \in E(2)$ sind Kompositionen von Translationen, Spiegelungen und Drehungen.

Wir versuchen jetzt, die $\mathrm{O}(3,\mathbb{R}) \supseteq \mathrm{SO}(3,\mathbb{R})$ zu verstehen.

Definition 1.5.7. Drehung

Eine **Drehung von** $\mathbb{R}^3$ um den Ursprung $0 \in \mathbb{R}^3$ ist eine Drehung um einen Winkel $\theta \in R/2\pi\mathbb{Z}$ um eine Achse aufgespannt von $v \in \mathbb{R}^3 \backslash \{0\}$.

Satz 1.5.8. Drehungen sind spezielle orthogonale Transformationen

Die Bewegungen der Form μ_A mit $A \in \mathrm{SO}(3,\mathbb{R})$ sind genaud die Drehungen um 0.

Beweis.

1. A hat einen Eigenvektor $v \neq 0$ zum Eigenwert 1, also $Av = v$. Dafür genügt es, $\det(A - I_3) = 0$ zu zeigen. Wir rechnen schrittweise:
   (i)
   $$\det(A - I_3) = \det\big(A(I_3 - A^{\mathrm{T}})\big) = \det(A)\det\big(I_3 - A^{\mathrm{T}}\big) = \det\big(I_3 - A^{\mathrm{T}}\big) = \det(I_3 - A) \tag{1.5.23}$$
   (ii)
   $$\det(A - I_3) = \det(-(I - A)) = (-1)^3 \det(I_3 - A) \tag{1.5.24}$$
   Aus diesen beiden Gleichungen folgt bereits $\det(A - I_3) = 0$, was zu zeigen war.
2. Sei $v \neq 0$ ein Eigenvektor von A zum Eigenwert 1. O.B.d.A. sei $\|v\| = 1$ (ersetze v durch $\frac{v}{\|v\|}$). Ergänze v mit Gram-Schmidt zu einer ONB (v,p,q) des $\mathbb{R}^3$. Bezüglich dieser Basis hat μ_A die Form
   $$\begin{pmatrix}1 & 0 & 0 \\ 0 & * & * \\ 0 & * & *\end{pmatrix} \in \mathrm{SO}(3,\mathbb{R}). \tag{1.5.25}$$
   Das sehen wir ein, da die erste Spalte der Abbildung des Eigenvektors v entspricht. Nun ist die Abbildung orthogonal, also bleibt das Skalarprodukt erhalten. Damit muss im ersten Eintrag der zweiten und dritten Spalte 0 sein, sonst wäre das Bild der ONB keine ONB. Die untere Blockdiagonalmatrix ist in $\mathrm{SO}(2,\mathbb{R})$, also

gilt

$$\begin{pmatrix} * & * \\ * & * \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}. \tag{1.5.26}$$

Damit ist μ_A eine Drehung um die von v aufgespannte Achse mit Winkel θ. □

Korollar 1.5.9 (Aus Satz 1.5.8)**.** Die Menge der Drehungen von $\mathbb{R}^3$ um $0 \in \mathbb{R}^3$ bildet eine Gruppe unter Verknüpfung, die isomorph zu $\mathrm{SO}(3,\mathbb{R})$ ist.

1.6 Symmetrie im Raum

Definition 1.6.1. Euklidische Symmetriegruppe

Für eine Teilmenge $F \subseteq \mathbb{R}^3$, genannt **Figur**, definieren wir die **euklidische Symmetriegruppe**

$$\mathrm{Sym}(F) := \{T \in E(3) | T(F) = F\} \leq E(3) \tag{1.6.1}$$

und die **euklidische Drehsymmetriegruppe**

$$\mathrm{Sym}^{\mathrm{SO}}(F) := \{A \in \mathrm{SO}(3,\mathbb{R}) | \mu_A(F) = F\} \leq \mathrm{SO}(3,\mathbb{R}) \tag{1.6.2}$$

von F.

Satz 1.6.2. Klassifikation der Drehgruppe in $\mathbb{R}^3$

Jede endliche Untergruppe von $\mathrm{SO}(3,\mathbb{R})$ ist konjugiert zu einer der folgenden Gruppen:

1. $\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$: triviale Gruppe
2. Die zyklische Gruppe C_n der Ordnung n, gegeben durch die Drehgruppe $\mathrm{Sym}^{\mathrm{SO}}(P)$ einer Pyramide P über einem regulären n-Eck mit Mittelpunkt 0.
3. Die Drehgruppe D_n der Ordnung $2n$, gegeben durch die Drehgruppe eines regulären Prismas über einem regulären n-Eck mit $n \geq 2$ und Mittelpunkt 0.
4. Die Gruppe A_4, gegeben als Drehgruppe eines Tetraeders.
5. Die Gruppe $\mathfrak{S}_4$, gegeben als Drehgruppe eines Würfels oder eines Oktaeders.
6. Die Gruppe A_5, gegeben als Drehgruppe eines Dodekaeders oder Ikosaeders.

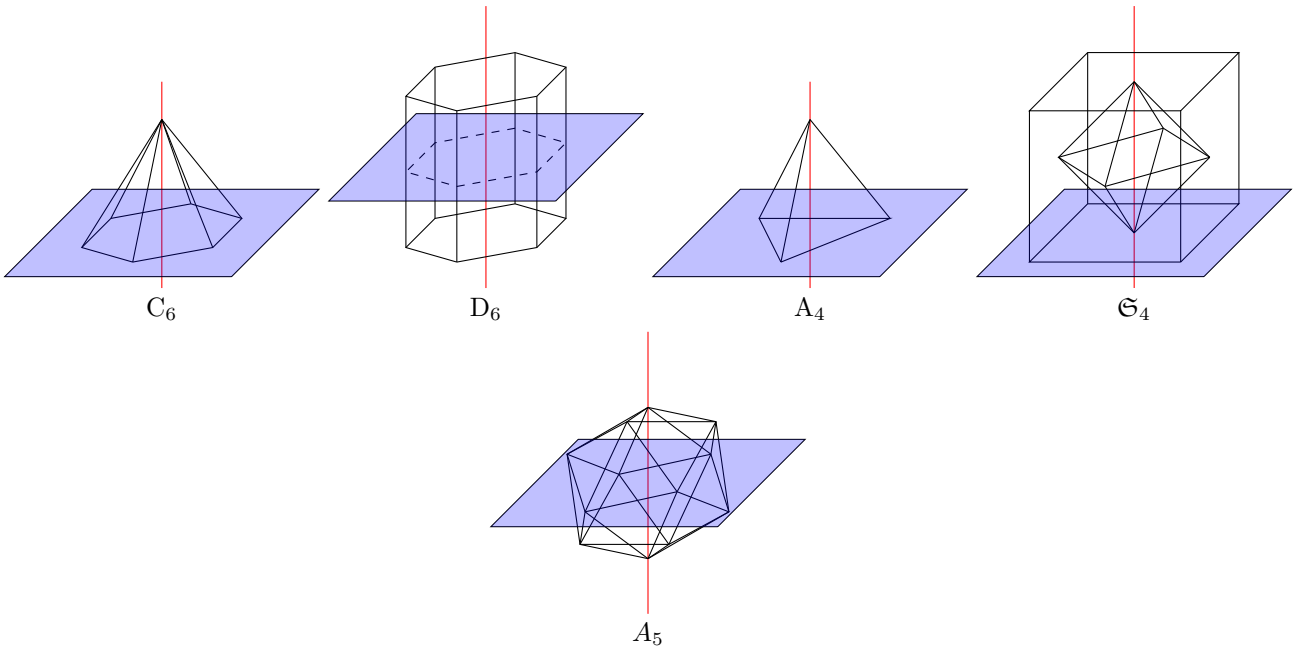


Abbildung 1: Klassifikation der Drehgruppe $\mathrm{SO}(3,\mathbb{R})$.

Beweis. O.B.d.A. sei $G \leq \mathrm{SO}(3,\mathbb{R})$ eine endliche Untergruppe mit $G \neq \{I_3\}$. In Abschnitt 1.5 haben wir gezeigt, dass jedes $A \in \mathrm{SO}(3,\mathbb{R})$, $A \neq I_3$ eine Drehung um eine Achse $l = \langle v \rangle \subseteq \mathbb{R}^3$. Wir bezeichnen die zwei Elemente der Menge $l \cap \mathbb{S}^2$ mit $\mathbb{S}^2 := \{v \in \mathbb{R}^3 | \|v\| = 1\}$ als **Pole von** A. Wir bezeichnen weiterhin mit $P \subseteq \mathbb{S}^2$ die Menge aller Pole aller Elemente $A \in G$, $A \neq I_3$.

1. Die Operation $G \curvearrowright \mathbb{R}^3$ via Links-Matrixmultiplikation schränkt sich ein auf eine Operation $G \curvearrowright P$. Sei dazu

P ein Pol von $A \in G$, $A \neq I_3$ und sei $B \in G$. Dann gilt

$$(BAB^{-1})B.p = B(AB^{-1}B).p = BA.p = B.p, \tag{1.6.3}$$

da Pole von A invariant unter A sind. Also ist $B.p$ ein Pol von $A' = BAB^{-1} \in G$.

□

Lemma 1.6.3. Klassifikation von $\mathbf{SO}(2,\mathbb{R})$ Sei $0 \neq p \in \mathbb{R}^3$ und $H \leq \mathrm{Sym}^{\mathrm{SO}}(\mathbb{R}^3)_p$ eine endliche Untergruppe von Drehungen um die Achse $0_p \in \mathbb{R}^3$.[a] Dann ist H zyklisch, erzeugt von der Drehung δ_θ in H um den kleinsten Winkel $0 < \theta \leq 2\pi$ gegen den Uhrzeigersinn.

[a] Notationell ist $\mathrm{Sym}^{\mathrm{SO}}(\mathbb{R}^3)_p$ der Stabilisator von p unter $\mathrm{Sym}^{\mathrm{SO}}(\mathbb{R}^3) \curvearrowright \mathbb{R}^3$.

Beweis. Sei $\delta_\theta \in H$ eine Drehung um den kleinsten Winkel. Diese existiert, da

$$\{\theta \in (0, 2\pi) | \delta_\theta \in H\} \subseteq \mathbb{R} \tag{1.6.4}$$

eine endliche, nicht-leere Teilmenge ist. Wir behaupten, dass $H = \langle \delta_\theta \rangle$. Wäre dem nicht so, gäbe es $\phi \in (0, 2\pi)$ und $n \in \mathbb{N}$, sodass $n\theta < \phi < (n+1)\theta$ mit $\delta_\phi \in H$. Dann gilt aber

$$\delta_{\phi - n\theta} = \delta_\phi (\delta_\theta^n)^{-1} \in H \tag{1.6.5}$$

mit $0 < \phi - n\theta < \theta$, was ein Widerspruch zur Annahme ist. □

Beweis. Wir machen weiter im Beweis von Satz 1.6.2.

2. Für $p \in P$ besteht $G_p \leq G$ genau aus den Drehungen δ_θ mit $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ um die Achsen O_p mit $\delta_\theta \in G$. Gemäß Lemma 1.6.3 gilt also $G_p = \langle \delta_\theta \rangle$, wobei δ_θ der kleinste Winkel mit $\delta_\theta \in G_p$ ist. Da $p \in P$ ein Pol ist, ist $G_p \neq \langle I_3 \rangle$. Es gilt $\theta = \frac{2\pi}{r_p}$ mit $r_p = |G_p|$ und $r_p > 1$, da p ein Pol ist. Wir definieren $n_p := |G.p|$ und betrachten die Bahnformel

$$N := |G| = n_p \cdot r_p. \tag{1.6.6}$$

2. Betrachte die Menge

$$X := \{(p, A) \,|\, p \,\text{ist Pol von}\, A \in G\} \subseteq P \times G. \tag{1.6.7}$$

Da jedes $I_3 \neq A \in G$ genau zwei Pole hat, gilt $|X| = 2N - 2$. Fixieren wir andererseits einen Pol p, dann hat die Menge $\{I_3 \neq A \in G \,|\, p \,\text{Pol von}\, A\} = G_p \backslash \{I_3\}$ die Kardinalität $r_p - 1$. Also gilt $|X| = \sum_{p \in P}(r_p - 1) = 2N - 2$. Für $p' \in G.p$ gilt: $|G_p| = |G_{p'}|$, also $r_p = r_{p'}$. Wir erhalten insgesamt:

$$\sum_{G.p \in G\backslash P} n_p(r_p - 1) = 2N - 2. \tag{1.6.8}$$

Division beider Seiten durch $N = n_p r_p$ liefert

$$\sum_{G.p \in G\backslash P} \left(1 - \frac{1}{r_p}\right) = 2 - \frac{2}{N}. \tag{1.6.9}$$

2. Aus Gleichung 1.6.9 folgt sofort, dass höchstens drei Bahnen existieren können, also $|G\backslash P| \leq 3$.

1. Fall: Sei $|G\backslash P| = 1$. Dann gilt gemäß Gleichung 1.6.9:

$$\underbrace{-\frac{1}{r}}_{<1} = \underbrace{-\frac{2}{N}}_{\geq 1} \tag{1.6.10}$$

für $r = |G_p|$, $p \in P$, was ein Widerspruch ist. Solche Bahnen existieren somit nicht.

2. Fall: Sei $|G\backslash P| = 2$, also

$$\left(1 - \frac{1}{r_1}\right) + \left(1 - \frac{1}{r_2}\right) = 2 - \frac{2}{N} \tag{1.6.11}$$

$$\Leftrightarrow \frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2}. \tag{1.6.12}$$

Es gilt aber $r_i \leq N$, also $r_1 = r_2 = N$ und damit $n_1 = n_2 = 1$. Es gibt somit zwei Pole $P = \{\pm p\}$, die von allen Gruppenelementen stabilisiert werden. Also ist $G \leq \mathrm{Sym}^{\mathrm{SO}}(\mathbb{R}^3)_p$ eine endliche Gruppe von Drehungen um die Achse 0_p (sowie um die Achse $\overline{(-p)p}$). Mit Lemma 1.6.3 folgt

$$G = \langle \delta_\theta \rangle \sim \mathrm{C}_n. \tag{1.6.13}$$

3. Fall: Sei $|G\backslash P| = 3$, also

$$\frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1. \tag{1.6.14}$$

O.B.d.A. sei $r_1 \leq r_2 \leq r_3$. Falls alle $r_i \geq 3$ sind, ist dies ein Widerspruch, also $r_1 = 2$. Wir unterscheiden weitere Fälle:

3.1. Fall: Sei $r_2 = 2$, dann ist $r_3 = \frac{N}{2}$ und $N = 2r_3$ gerade.

3.2. Fall: Sei $r_2 = 3$ und $r_3 = 3$. Dann ist $N = (2, n_i = (6, 4, 4))$.

3.3. Fall: Sei $r_2 = 3$ und $r_3 = 4$, dann ist $N = 24$ und $n_i = (12, 8, 6)$.

3.4. Fall: Sei $r_2 = 3$ und $r_3 = 5$, dann ist $N = 60$ und $n_i = (30, 20, 12)$.

2 Ringe

2.1 Ringe, Ideale und Homomorphismen

Definition 2.1.1. Ring

Ein **Ring** ist ein Tripel $(R, +, \cdot)$, bestehend aus einer Menge R und Abbildungen

$$+ : R \times R \to R \tag{2.1.1}$$

und

$$\cdot : R \times R \to R, \tag{2.1.2}$$

sodass gilt:

(R1) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(R2) Für $a, b \in R$ gilt:

$$\begin{aligned} a \cdot (b \cdot c) &= (a \cdot b) \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \\ a \cdot (b + c) &= a \cdot b + a \cdot c \end{aligned} \tag{2.1.3}$$

(R3) Es existiert ein Einselement $1 \in R$, sodass für alle $a \in R$ gilt:

$$1 \cdot a = a \cdot 1 = a. \tag{2.1.4}$$

Gilt zusätzlich

$$a \cdot b = b \cdot a, \tag{2.1.5}$$

dann heißt der Ring **kommutativ**.

Bemerkung. Manche Autoren definieren Ringe, ohne ein Einselement zu fordern. Dann werden Ringe mit Einselement als **unitale Ringe** bezeichnet.

Beispiele.

1. Der **Nullring** $\{0\}$ ist ein Ring, da wir insbesondere nicht fordern, dass $0 \neq 1$ gelten muss. Jedoch ist der Nullring (bis auf Umbenennung der Elemente) der einzige Ring mit dieser Eigenschaft.
2. $(\mathbb{Z}, +, \cdot)$ bildet einen kommutativen Ring.
3. Jeder Körper bildet einen kommutativen Ring.
4. Für $\alpha \in \mathbb{C}$ ist die Menge
$$\mathbb{Z}[\alpha] := \left\{ \sum_{k=0}^{w} \lambda_k \alpha^k \mid k \in \mathbb{N}, \lambda_k \in \mathbb{Z} \right\} \subseteq \mathbb{C} \tag{2.1.6}$$
abgeschlossen unter Addition und Multiplikation. Die Ringaxiome werden von $(\mathbb{C}, +, \cdot)$ vererbt, also bildet $\mathbb{Z}[\alpha]$ einen kommutativen Ring, den **Polynomring über** $\mathbb{Z}$. Besonders wichtig für die Zahlentheorie is der Fall, wenn α eine *ganze algebraische Zahl* ist, also α als Nullstelle eines monischen Polynoms
$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{2.1.7}$$
mit Koeffizienten $a_i \in \mathbb{Z}$ auftritt. Zum Beispiel ist die imaginäre Zahl $i \in \mathbb{C}$ als Nullstelle des Polynoms $x^2 + 1$ eine ganze algebraische Zahl. Der Ring
$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \tag{2.1.8}$$
heißt **Gaußscher Zahlenring**.
5. Für einen Ring R bildet die Menge $R[x]$ der Polynome mit Koeffizienten in R einen Ring, genannt **Polynomring über** R.
6. Für jeden Körper $\mathbb{K}$ bildet die Menge $M(n, \mathbb{K})$ der $\mathbb{K}$-wertigen $n \times n$-Matrizen einen Ring mit elementweiser Addition und Matrixmultiplikation.
7. Für Ringe R und S ist das Produkt $R \times S$ wieder ein Ring mit komponentenweisen Verknüpfungen.

Definition 2.1.2. Schiefkörper

Sei $(R, +, \cdot)$ ein Ring. Existiert zusätzlich für alle $a \in R$ ein $a^{-1} \in R$ mit

$$a \cdot a^{-1} = a^{-1} a = 1, \tag{2.1.9}$$

so heißt $(R, +, \cdot)$ **Schiefkörper**.

Beispiel. Die **Quaternionen** $\mathbb{H}$ bilden einen nicht-kommutativen Ring. Da jedes $q \in \mathbb{H} \backslash \{0\}$ allerdings ein multiplikatives Inverses besitzt, ist $\mathbb{H}$ ein Schiefkörper.

Bemerkung. Historisch wurde der Begriff des Rings und zugehörige Definitionen wie Ideale und Moduln in der algebraischen Zahlentheorie des 19. Jahrhunderts eingeführt und entwickelt (*Kummer*, *Noether*, *Dedekind*, *Hilbert*, ...).
Ziel der Einführung der Ringstruktur ist die Verallgemeinerung des Primzahlbegriffs und der Primfaktorzerlegung für

ganze algebraische Zahlen. Zum Beispiel zerfällt die Primzahl 2 in ein Produkt

$$2 = (1+i)(1-i), \tag{2.1.10}$$

welches in $\mathbb{Z}[i]$ die neue Primfaktorzerlegung von 2 wird. Die Tatsache, dass $\mathbb{Z}[i]$ noch immer eindeutige Primfaktorzerlegung besitzt, hat direkte zahlentheoretische Konsequenzen. Ein Beispiel dafür ist der sehr elegante Beweis des folgenden Satzes.

Satz 2.1.3. Quadratsumme

Eine ganze Zahl $n \in \mathbb{Z}$ ist genau dann eine Summe $a^2 + b^2$ von Quadraten mit $a, b \in \mathbb{Z}$, falls gilt: Jeder Primfaktor $p \mid n$ mit $p \equiv_4 3$ kommt mit gerader Vielfachheit vor.

Umgekehrt gibt es algebraische Zahlenringe ohne eindeutige Primfaktorzerlegung, z.B. $\mathbb{Z}[\sqrt{-5}]$:

$$6 = 2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5}). \tag{2.1.11}$$

Ab jetzt vereinbaren wir, dass alle vorkommenden Ringe kommutativ sind.

Definition 2.1.4. Ideal

Sei R ein Ring. Eine nicht-leere Teilmenge $\mathcal{I} \subseteq R$ heißt **Ideal**, falls gilt:

(I1) Für alle $x, y \in \mathcal{I}$ gilt: $x + y \in \mathcal{I}$.

(I2) Für alle $r \in R$ und $x \in \mathcal{I}$ gilt: $r \cdot x \in \mathcal{I}$.

Beispiel. Hauptideale
Sei R ein Ring und $x \in R$. Dann bildet

$$(x) := Rx = \{rx | r \in R\} \subseteq R \tag{2.1.12}$$

ein Ideal, das von x erzeugte **Hauptideal**. Allgemeiner ist für jede Teilmenge $M \subseteq R$

$$(M) := \bigcap_{M \subseteq \mathcal{I} \subseteq R} \mathcal{I} \subseteq R \tag{2.1.13}$$

das von M **erzeugte Ideal**.

Bemerkung. Jeder vom Nullring verschiedene Ring R besitzt mindestens zwei unterschiedliche Ideale, nämlich $\{0\}$ und R selbst.

Satz 2.1.5. Ring = Körper?

Ein Ring R ist genau dann ein Körper, wenn R genau zwei verschiedene Ideale besitzt.

Beweis. Sei $\mathbb{K}$ ein Körper und $\{0\} \subset \mathcal{I} \subseteq \mathbb{K}$ ein Ideal. Wähle $0 \neq x \in \mathcal{I}$. Dann existiert ein $r \in R$ mit $rx = 1 \in \mathcal{I}$. Also gilt für alle $s \in \mathbb{K}$: $s \cdot 1 = s \in \mathcal{I}$, und somit $\mathcal{I} = \mathbb{K}$.
Angenommen, R hat genau zwei Ideale. Sei $0 \neq x \in R$, dann ist $\{0\} \subset (x) \subseteq R$ ein Ideal. Daraus folgt aber, dass $(x) = R \ni 1$, also existiert ein $r \in R$ mit $rx = 1$. □

Definition 2.1.6. Ringhomomorphismus

Eine Abbildung $\phi : R \to S$ zwischen Ringen R und S heißt **(Ring-)Homomorphismus**, falls gilt:

(H1) Für alle $r_1, r_2 \in R$ gilt:

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \tag{2.1.14}$$

$$\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2). \tag{2.1.15}$$

(H2) Für $1 \in R$, $1' \in S$ gilt:

$$\phi(1) = 1'. \tag{2.1.16}$$

Beispiel. Sei R ein Ring, $R[x]$ der zugehörige Polynomring über R und $\alpha \in R$. Dann ist die **Auswertungsabbildung**

$$\begin{aligned} \mathrm{ev}_\alpha : R[x] &\to R \\ f(x) &\mapsto f(\alpha) \end{aligned} \tag{2.1.17}$$

ein Homomorphismus, genannt **Einsetzungshomomorphismus**.