Algebra (Bachelor)

zur Vorlesung von Prof. Dr. Tobias Dyckerhoff

5. Januar 2025

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 $\ker(\pi) = N$.

□

Theorem 1.3.13. Isomorphiesätze

1. Isomorphiesatz (Homomorphiesatz): Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus
$$\overline{\phi} : G/\ker(\phi) \to \operatorname{im}(\phi) \tag{1.3.44}$$
$$g\ker(\phi) \mapsto \phi(g). \tag{1.3.45}$$
2. Isomorphiesatz: Sei $H \leq G$ eine Untergruppe und $N \trianglelefteq G$ eine normale Untergruppe. Dann definiert $g(N \cap H) \to gN$ einen Isomorphismus
$$H/(N \cap H) \to NH/N. \tag{1.3.46}$$
3. Isomorphiesatz: Seien $M, N \trianglelefteq G$ und $M \leq N$. Dann ist $N/M \trianglelefteq G/M$ und es existiert ein Isomorphismus
$$(G/M)/(N/M) \to G/N. \tag{1.3.47}$$

Beweis. Zunächst ist Wohldefiniertheit zu zeigen. Für $\widetilde{g} \in gN$, also $\widetilde{g} = gn$ für $n \in \ker(\phi)$, gilt:
$$\phi(\widetilde{g}) = \phi(gn) = \phi(g)\underbrace{\phi(n)}_{=1} = \phi(g), \tag{1.3.48}$$
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:
$$g\ker(\phi) \in \ker(\overline{\phi}) \Leftrightarrow \phi(g) = 1_{G'} \Leftrightarrow g \in \ker(\phi) \Leftrightarrow g\ker(\phi) = \ker(\phi) \tag{1.3.49}$$
□

Beispiel. Wir können die Vorzeichenfunktion
$$\operatorname{sgn} : \mathfrak{S}_n \to \{\pm 1\} \tag{1.3.50}$$
betrachten, dann ist $\ker \operatorname{sgn} = A_n \trianglelefteq \mathfrak{S}_n$, also erhalten wir einen Isomorphismus
$$\mathfrak{S}_n/A_n \to \{\pm 1\}. \tag{1.3.51}$$
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
$$\phi = \iota \circ \overline{\phi} \circ \pi, \tag{1.3.52}$$
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 **??** 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
$$\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^* \tag{1.3.53}$$
einen Isomorphismus
$$\mathrm{GL}(n, \mathbb{K})/\mathrm{SL}(n, \mathbb{K}) \to \mathbb{K}^*. \tag{1.3.54}$$

2. Ein weiterer induzierter Isomorphismus ist
$$\overline{\operatorname{sgn}} : \mathfrak{S}_n/_{A_n} \to \{\pm 1\}. \tag{1.3.55}$$
3. Sei G eine Gruppe mit $g \in G$. Betrachte den Homomorphismus
$$\phi : (\mathbb{Z}, +) \to G, i \mapsto g^i. \tag{1.3.56}$$
(a) Falls $\operatorname{ord}(g) = \infty$, gilt $\ker(\phi) = \{0\}$ und ϕ induziert einen Isomorphismus
$$\mathbb{Z} \xrightarrow[\cong]{\pi} \mathbb{Z}/_{\{0\}} \xrightarrow[\cong]{\overline{\phi}} \langle g \rangle, \quad \mathbb{Z} \xrightarrow[\phi]{} \langle g \rangle$$
(b) Falls $\operatorname{ord}(g) = N < \infty$, dann gilt
$$\ker(\phi) = N \cdot \mathbb{Z} \tag{1.3.57}$$
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
$$\begin{aligned} \mathfrak{S}_M \times M &\to M \\ (\sigma, x) &\mapsto \sigma(x). \end{aligned} \tag{1.4.3}$$
3. Für $n \geq 1$ und einen Körper $\mathbb{K}$ operiert die Gruppe $\mathrm{GL}(n, \mathbb{K})$ auf $\mathbb{K}^n$ via
$$\begin{aligned} \mathrm{GL}(n, \mathbb{K}) \times \mathbb{K}^n &\to \mathbb{K}^n \\ (A, v) &\mapsto Av. \end{aligned} \tag{1.4.4}$$

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

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

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 $\operatorname{ord}(G) < \infty$ hat Gleichung 1.4.17 dann die Form

$$|G| = |Z(G)| + \sum_{[x]\in G\setminus G, C_G(x)\neq G} \underbrace{(G : C_G(x))}_{=|[x]|} \tag{1.4.22}$$

und heißt **Klassengleichung** von G. Alle Summanden der Klassengleichung teilen $\operatorname{ord}(G)$.

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

Satz 1.4.8. Zyklische Zentren geben abelsche Gruppen

Sei G eine Gruppe und $Z(G)$ das Zentrum von G. Falls $G/Z(G)$ zyklisch ist, ist G abelsch.

Beweis. Übung 4.2 □

Bemerkung. Ist $G/Z(G)$ abelsch, ist G nicht notwendigerweise abelsch.

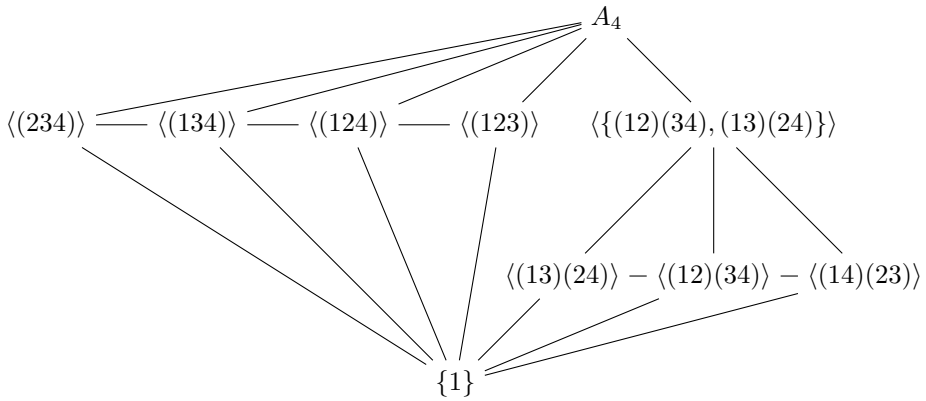
Beispiel. Wir wollen die Untergruppenstruktur von $A_4 \trianglelefteq \mathfrak{S}_4$ verstehen. Dazu bestimmen wir die Klassengleichung der Gruppe. Es gilt $(\mathfrak{S}_4 : A_4) = 2$, da $\mathfrak{S}_4/A_4 = \{\pm 1\}$. Aus dem Satz von Lagrange folgt

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

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.

Definition 1.4.9. Zykeltyp

Sei $\mathfrak{S}_n$ die symmetrische Gruppe. Ein $\sigma \in \mathfrak{S}_n$ kann als Produkt

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \sigma_k \tag{1.4.31}$$

paarweise disjunkter Zykel σ_i der Länge $m_i \geq 2$ geschrieben werden, wobei $(1) = \sigma_0$ gilt. O.B.d.A sei $m_1 \geq m_2 \geq \cdots \geq m_k$. Dann heißt der k-Tupel

$$(m_1, m_2, \cdots, m_k) \tag{1.4.32}$$

Zykeltyp von σ.

Satz 1.4.10. Zykeltyp bestimmt Konjugationsklasse

Zwei Elemente $\sigma, \sigma' \in \mathfrak{S}_n$ sind genau dann in der gleichen Konjugationsklasse, wenn sie den gleichen Zykeltyp haben.

Beweis. Übung 3.2 □

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 $\mu_{A^\mathrm{T}} \circ T =: \widetilde{T} \in E(n)$ 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.

Definition 1.5.7. Kurze exakte Sequenz

Eine **kurze exakte Sequenz** von Gruppen ist gegeben durch

$$\{1\} \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow \{1\},$$

wobei:

- N, G und H Gruppen sind.
- $i : N \to G$ ein injektiver Gruppenhomomorphismus (Monomorphismus) ist.
- $p : G \to H$ ein surjektiver Gruppenhomomorphismus (Epimorphismus) ist.
- $\mathrm{im}(i) = \ker(p)$ gilt.

Eine kurze exakte Sequenz **zerfällt**, falls ein Homomorphismus $s : H \to G$ mit $p \circ s = \mathrm{id}_H$ existiert.

Satz 1.5.8. Kurze exakte Sequenzen und semidirekte Produkte

1. Seien H, N Gruppen und H wirke auf N via Homomorphismen. Dann existiert eine zerfallende kurze exakte Sequenz:

$$\{1\} \longrightarrow N \xrightarrow{i} N \rtimes H \xrightarrow{p} H \longrightarrow \{1\}.$$

2. Sei

$$\{1\} \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow \{1\}.$$

eine zerfallende kurze exakte Sequenz mit Schnitt s. Dann definiert Konjugation mit $s(H)$ eine Wirkung von H auf N via Homomorphismen, sodass $G \cong N \rtimes H$ ist:

$$\begin{array}{ccccccccc} \{1\} & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{p} & H & \longrightarrow & \{1\} \\ & & & & \downarrow{\scriptstyle \phi} & & & & \\ \{1\} & \longrightarrow & N & \xrightarrow{i} & N \rtimes H & \xrightarrow{p} & H & \longrightarrow & \{1\}. \end{array}$$

Beweis. Übung 4.4 □

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

Definition 1.5.9. 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 1.5.10. Drehungen sind spezielle orthogonale Transformationen

Die Bewegungen der Form μ_A mit $A \in \mathrm{SO}(3, \mathbb{R})$ sind genau 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 1.5.11 (Aus Satz 1.5.10)**.** 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.

Theorem 1.6.2. Klassifikation der Drehgruppe

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.

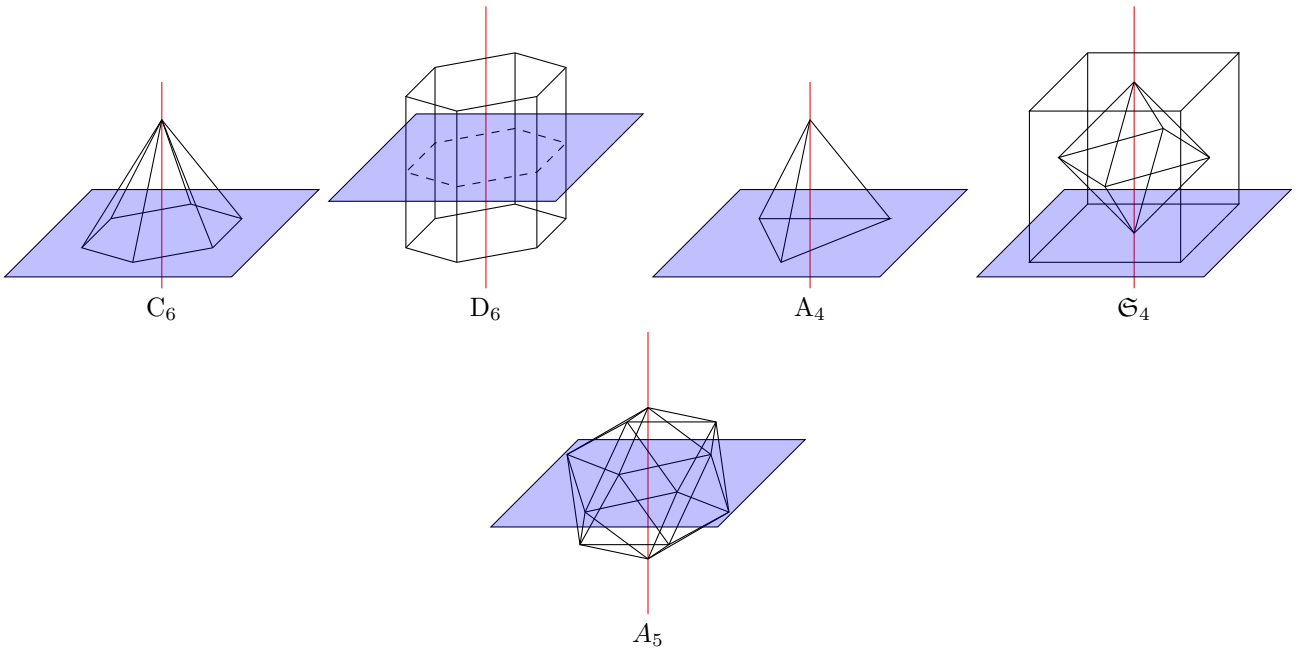


Abbildung 1: Klassifikation der Drehgruppe $\mathrm{SO}(3,\mathbb{R})$.

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 $\mathrm{SO}(2,\mathbb{R})$ 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
$$N := |G| = n_p \cdot r_p. \tag{1.6.6}$$
3. Betrachte die Menge
$$X := \{(p, A) \,|\, p \in P \text{ ist Pol von } A \in G\} \subseteq P \times G. \tag{1.6.7}$$
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
$$\sum_{G.p \in G\backslash P} \left(1 - \frac{1}{r_p}\right) = 2 - \frac{2}{N}. \tag{1.6.9}$$
4. 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 $n_i = (30, 20, 12)$.

5. Jetzt müssen wir noch die verschiedenen Fälle aus dem 4. Schritt genauer untersuchen.

(I) Es existieren zwei Bahnen, bestehend aus je einem Pol, also $P = \{\pm p\}$. Daher ist $G = G_p$ eine endliche Gruppe von Drehungen um die von p erzeugte Achse. Nach Lemma 1.6.3 ist die Gruppe zyklisch, erzeugt durch Drehungen um $\frac{2\pi}{N}$ durch $\overline{(-p)p}$. Sei $C \in \mathrm{SO}(3, \mathbb{R})$ eine Drehung, die die Standardkoordinate e_3 auf p abbildet. Dann ist $C^{-1}GC : e_3 \to p \to p \to e_3$ genau die Drehgruppe P_n der Pyramide.

(II) (a) Für $n_3 = 2$ und $r_3 = r$ hat die zugehörige Bahn zwei Pole $\{p, p'\}$. Für einen Pol p existiert ein $I_3 \neq A$ mit $A_p = p$. Wegen $G \curvearrowright \{p, p'\}$ induziert $\{p, p'\} \to \{p, p'\}, x \mapsto Ax$ eine Selbstbijektion, also $Ap' = p'$ und damit $p' = -p$. Gemäß Lemma 1.6.3 ist der Stabilisator G_p eine zyklische Gruppe der Ordnung r, erzeugt von einer Drehung δ um die Achse $\overline{0p}$ mit Winkel $\frac{2\pi}{r}$. Sei $tau \in G/G_p$. Dann gilt $\tau.p = -p$, also ist τ eine Drehung um eine zu p orthogonale Achse mit Winkel π. Damit erzeugt $\langle \delta, \tau \rangle \leq G$ eine Diedergruppe der Ordnung $2r$, also $G = \langle \delta, \tau \rangle$. Durch analogen Koordinatenwechsel mit $C \in \mathrm{SO}(3, \mathbb{R})$ wie in (I) gilt: $C^{-1}GC$ ist die Diedergruppe von Z_r.

(b) Es gilt $n_3 = 4$ und $r_3 = 3$. Sei $B = \{p_1, p_2, p_3, p_4\}$ die zugehörige Bahn. Dann gilt $|G_{p_1}| = 3$ und G_{p_1} besteht aus Drehungen um die von p_1 erzeugte Achse. Daher muss G_p nicht trivial auf $\{p_2, p_3, p_4\}$ wirken, also nach der Bahnformel transitiv sein. Da G_{p_1} durch Bewegungen wirkt, muss für die Skalarprodukte gelten:

$$\langle p_1, p_2 \rangle = \langle p_1, p_3 \rangle = \langle p_1, p_4 \rangle. \tag{1.6.15}$$

Dieses Argument kann für jedes $i \in \{1, 2, 3, 4\}$ angewandt werden, wodurch wir Gleichheit von allen $\langle p_i, p_j \rangle$ für alle $1 \leq i \neq j \leq n$ erhalten. Weiterhin gilt $\langle p_i, p_j \rangle = 1$ für alle $1 \leq i \leq n$. Mit der Bijektivität des Skalarprodukts folgt daraus, dass alle Abstände $\|p_i - p_j\|$ für $i \neq j$ gleich sind. Jeweils drei der vier Pole aus B bilden also ein gleichseitiges Dreieck. Das impliziert, dass B die Eckpunkte eines Tetraeders mit Schwerpunkt 0 bildet.

Die Gruppe G permutiert B via Drehungen (lineare Abbildungen), also erhält $G\,T' = \mathrm{Konv}(B)$. Damit gilt $G \leq \mathrm{SO}(T')$. Da $|G| = 12$ und $|\mathrm{SO}(T')| = 12$ gilt, muss $G = \mathrm{SO}(T')$ sein. Durch eine Drehung C lässt sich T überführen in eine Skalarstreckung von T', also $C^{-1}GC = \mathrm{SO}(T)$.

(c) Es gilt $n_3 = 6$, $r_3 = 4$ und $N = 24$. Sei $B := \{p_1, \ldots, p_6\}$ die zugehörige Bahn. Es gilt $|G_{p_1}| = 4$, wobei G_{p_1} die zyklische Gruppe von Drehungen um p_i ist. Wegen der Bahnformel hat die Wirkung von G_{p_1} auf $B \backslash \{p_1\}$ einen Fixpunkt. Dann muss aber $p_2 = -p_1$ sein. Aus Lemma 1.6.3 folgt, dass $G_{p_1} = \langle \delta \rangle$ zyklisch der Ordnung 4 ist. Die Bahnformel erlaubt zwei Möglichkeiten:

(i) $G_{p_1} \curvearrowright \{p_3, \ldots, p_6\}$ zerfällt in zwei Bahnen der Kardinalität zwei. Seien diese Bahnen o.B.d.A. $\{p_3, p_4\}$ und $\{p_5, p_6\}$. Dann gilt aber $\delta.p_3 = p_4$ und $\delta.p_4 = p_3$. Das ist aber unmöglich, da δ eine Drehung um 90 deg beschreibt.

(ii) G_{p_1} wirkt transitiv, es gibt nur eine Bahn. Nach obigem Argument für $p_2 = -p_1$ muss o.B.d.A. gelten: $p_5 = -p_3$ und $p_6 = -p_4$. Es folgt dann, dass p_3, p_4, p_5 und p_6 die Eckpunkte eines Quadrats in der Ebene senkrecht zu p_1 bilden.

Der Rest verläuft analog und ist dem Leser überlassen. □

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**.

Definition 2.1.7. Unterring

Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $U \subseteq R$ heißt **Unterring** von R, falls $(U, +|_U, \cdot|_U)$ wieder ein Ring ist.

Satz 2.1.8. Bild und Kern von Homomorphismen

Sei $\phi : R \to S$ ein Ringhomomorphismus. Dann gelten folgende Aussagen:

(i) $\mathrm{im}(\phi) \subseteq S$ ist ein Unterring.

(ii) $\ker(\phi) \subseteq R$ ist ein Ideal.

Beweis. Wir beweisen (ii): Seien $x, y \in \ker(\phi)$ und $r \in R$. Dann gilt:
1. $\phi(x+y) = \cancel{\phi(x)} + \cancel{\phi(y)} = 0$.
2. $\phi(rx) = \phi(r)\cancel{\phi(x)} = 0$.

□

Übung. Beweise (i).

Korollar 2.1.9 (Aus 2.1.8)**.** Sei $\mathbb{K}$ ein Körper, S ein Ring und $\phi : \mathbb{K} \to S$ ein Ringhomomorphismus. Dann ist ϕ entweder injektiv, oder $S = \{0\}$.

Beweis. Die einzigen Ideale von $\mathbb{K}$ sind $\mathbb{K}$ und $\{0\}$. Für $\ker(\phi) = \{0\}$ ist ϕ injektiv. Für $\ker(\phi) = \mathbb{K}$ ist $\phi \equiv 0$. Also folgt $1 = \phi(1) = 0$ und damit $S = \{0\}$, da der Nullring als einziger diese Eigenschaft aufweist. □

Definition 2.1.10. Restklassen

Sei R ein Ring und $\mathcal{I} \subseteq R$ ein Ideal. Dann definiert

$$r_1 \sim r_2 :\Leftrightarrow r_1 - r_2 \in \mathcal{I} \tag{2.1.18}$$

eine Äquivalenzrelation auf R. Die Äquivalenzklasse eines $r \in R$ hat die Gestalt

$$[r] = \{r + x | x \in \mathcal{I}\}, \tag{2.1.19}$$

genannt **Restklassen modulo** $\mathcal{I}$. Die Menge aller Restklassen modulo $\mathcal{I}$ wird mit $R/\mathcal{I}$ bezeichnet.

Satz 2.1.11. Quotientenringe

Sei R ein Ring und $\mathcal{I} \subseteq R$ ein Ideal.

(i) Die Verknüpfungen

$$\begin{aligned} + : R/\mathcal{I} \times R/\mathcal{I} &\to R/\mathcal{I} \\ ([r_1], [r_2]) &\mapsto [r_1 + r_2] \end{aligned} \tag{2.1.20}$$

und

$$\begin{aligned} \cdot : R/\mathcal{I} \times R/\mathcal{I} &\to R/\mathcal{I} \\ ([r_1], [r_2]) &\mapsto [r_1 \cdot r_2] \end{aligned} \tag{2.1.21}$$

definieren eine Ringstruktur auf $R/\mathcal{I}$, genannt **Quotientenring** von R modulo $\mathcal{I}$.

(ii) Die Abbildung

$$\begin{aligned} \pi : R &\to R/\mathcal{I} \\ r &\mapsto [r] \end{aligned} \tag{2.1.22}$$

ist ein Ringhomomorphismus mit $\ker(\pi) = \mathcal{I}$.

Übung. Man beweise diesen Satz analog zum Fall für Gruppen.

Beispiel. Sei $n \in \mathbb{N}, n \geq 2$. Dann ist $\mathbb{Z}/(n)$ der Restklassenring modulo n. Für $n = p$ prim ist $\mathbb{Z}$

Theorem 2.1.12. Isomorphiesatz

Sei $\phi : R \to S$ ein Ringhomomorphismus. Dann ist die induzierte Abbildung

$$\begin{aligned} \overline{\phi} : R/\ker(\phi) &\to \mathrm{im}(\phi) \\ [r] &\mapsto \phi(r) \end{aligned} \tag{2.1.23}$$

ein Ringisomorphismus.

Übung. Man beweise diesen Satz analog zum Fall für Gruppen.

Satz 2.1.13. Endliche Integritätsbereiche sind Körper

Sei R ein endlicher, nullteilerfreier Ring. Dann ist R ein Körper.

Beweis. Betrachte $r \in R \setminus \{0\}$. Dann existiert ein Isomorphismus

$$\begin{aligned} \mu_r : R\backslash\{0\} &\to R\backslash\{0\} \\ x &\mapsto rx. \end{aligned} \tag{2.1.24}$$

□

2.2 Primelemente und Primideale

Definition 2.2.1. Teiler

Sei R ein Ring und $a, b \in R$. Wir sagen, dass a b **teilt**, wenn ein $r \in R$ mit $b = ar$ existiert, und schreiben $a \mid b$.
Für Ideale gilt

$$a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a). \tag{2.2.1}$$

Damit führen wir *einen* Teilbarkeitsbegriff für Ideale ein:

$$\mathcal{I} \mid \mathcal{J} :\Leftrightarrow \mathcal{J} \subseteq \mathcal{I}. \tag{2.2.2}$$

Definition 2.2.2. Einheit

Sei R ein Ring. Ein $n \in R$ heißt **Einheit**, falls es ein $v \in R$ mit $nv = 1$ gibt. Die Einheiten von R bilden eine abelsche Gruppe unter Multiplikation, bezeichnet mit $R^\times$.

Definition 2.2.3. Primelement

Ein Element $0 \neq p \in R$ mit $p \notin R^\times$ heißt **Primelement**, falls für alle $a, b \in R$ gilt:

$$p \mid ab \Rightarrow p \mid a \text{ oder } p \mid b. \tag{2.2.3}$$

Beispiel. Die Gruppe der Einheiten in $\mathbb{Z}$ ist $\mathbb{Z}^\times = \{\pm 1\}$ und die Primelemente sind die Zahlen $\pm p$ für $p \in \mathbb{N}$ prim.

Satz 2.2.4. Gaußsche Zahlen

Die Einheiten im Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen bilden die Gruppe

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \tag{2.2.4}$$

der vierten Einheitswurzeln.

Beweis. Wir definieren für $a + bi =: \alpha \in \mathbb{Z}[i)$ die Norm

$$N(\alpha) := \alpha\overline{\alpha} = a^2 + b^2 \in \mathbb{N}. \tag{2.2.5}$$

Die Norm ist multiplikativ:

$$N(\alpha\beta) = N(\alpha)N(\beta), \tag{2.2.6}$$

daher gilt für $u, v \in \mathbb{Z}[i)$ mit $uv = 1$ auch $N(u)N(v) = 1$. Die einzige Gaußsche Zahl mit Norm < 1 ist 0. Daher muss jede Einheit Norm 1 haben. Umgekehrt sind daher auch alle Zahlen der Norm 1 Einheiten. □

Definition 2.2.5. Primideal

Sei R ein Ring. Ein Ideal $\mathfrak{p} \subset R$ heißt **Primideal**, falls für alle $x, y \in R$ gilt:

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}. \tag{2.2.7}$$

Satz 2.2.6. Kriterien für Einheit und Primideal

Sei R ein Ring.

(i) Ein Element $a \in R$ ist eine Einheit genau dann, wenn $(a) = R$.

(ii) Ein Element $0 \neq a \in R$ ist ein Primelement genau dann, wenn $(a) \subseteq R$ ein Primideal ist.

Übung. Man beweise den Satz direkt aus den Definitionen.

Übung. Sei R ein Ring. Für Ideale $\mathcal{I}, \mathcal{J} \subseteq R$ definieren wir das **Produktideal** durch

$$\mathcal{I} \cdot \mathcal{J} := (\{xy | x \in \mathcal{I}, y \in \mathcal{J}\}). \tag{2.2.8}$$

Dann ist $\mathfrak{p} \subseteq R$ ein Primideal genau dann, wenn für alle Ideale $\mathcal{I}, \mathcal{J} \subseteq R$ gilt:

$$\mathfrak{p} \mid \mathcal{I} \cdot \mathcal{J} \Rightarrow \mathfrak{p} \mid \mathcal{I} \text{ oder } \mathfrak{p} \mid \mathcal{J}, \tag{2.2.9}$$

das heißt: $\mathcal{I} \cdot \mathcal{J} \subseteq \mathfrak{p} \Rightarrow \mathcal{I} \subseteq \mathfrak{p}$ oder $\mathcal{J} \subseteq \mathfrak{p}$.
Ein (Gegen-)Beispiel ist

$$\mathcal{I} + \mathcal{J} := \{x + y | x \in \mathcal{I}, y \in \mathcal{J}\} = (\mathcal{I} \cup \mathcal{J}) \neq \mathcal{I} \cdot \mathcal{J}. \tag{2.2.10}$$

Definition 2.2.7. Integritätsbereich und Nullteilerfreiheit

Ein Ring R heißt **nullteilerfrei** oder **Integritätsbereich**, falls $R \neq \{0\}$ und für alle $r, s \in R$ gilt:

$$rs = 0 \Rightarrow r = 0 \text{ oder } s = 0. \tag{2.2.11}$$

Satz 2.2.8. Nullteilerfreiheit und Primideale

Sei R ein Ring und $\mathcal{I} \subseteq R$ ein Ideal. Dann sind äquivalent:

(i) $R/_I$ ist nullteilerfrei.

(ii) $\mathcal{I} \subseteq R$ ist ein Primideal.

Übung. Beweise diesen Satz direkt aus den Definitionen.

Definition 2.2.9. Irreduzibilität

Sei R ein Ring. Ein Element $0 \neq r \in R$ mit $r \notin R^\times$ heißt **unzerlegbar** oder **irreduzibel**, falls für alle $a, b \in R$ mit $r = ab$ gilt, dass $a \in R^\times$ oder $b \in R^\times$.

Beispiel. Jedes Primelement $p \in R$ eines nullteilerfreien Rings R ist irreduzibel. Denn aus $p = ab$ folgt $p \mid a$ oder $p \mid b$, also o.B.d.A. $p \mid a$. Dann existiert $t \in R$, sodass $a = tp$. Dann gilt aber $p = ptb \Rightarrow 1 = tb$ wegen der Nullteilerfreiheit, damit also $b \in R^\times$.

Satz 2.2.10. Irreduzible Elemente erzeugen maximale Hauptideale

Sei R ein nullteilerfreier Ring. Dann sind für ein $0 \neq r \in R$ äquivalent:

(i) r ist irreduzibel.

(ii) (r) ist maximal unter den echten[a] Hauptidealen von R.

[a] Ein Hauptideal $\mathcal{I}$ heißt echt, wenn $\mathcal{I} \subset R$.

Beweis. (i) $\Rightarrow$ (ii): Sei r irreduzibel und $(r) \subseteq (s) \subseteq R$. Dann gibt es also $a \in R$ mit $r = as$. Da r irreduzibel ist, ist entweder $a \in R^\times$ oder $b \in R^\times$. Für $a \in R^\times$ folgt direkt $(r) = (s)$, für $s \in R^\times$ folgt hingegen $(s) = R$. In beiden Fällen ist (r) maximal unter den echten Hauptidealen.
(ii) $\Rightarrow$ (i): Sei (r) maximal unter den Hauptidealen und $r = ab$ eine Zerlegung von r. Dann gilt, dass $(r) \subseteq (b) \subseteq R$, also entweder $(r) = (b)$ oder $(b) = R$. Im ersten Fall existiert ein $s \in R$ mit $b = rs$, also $r = asr$. Da R nullteilerfrei ist, folgt $as = 1$, also $a \in R^\times$. Im zweiten Fall ist schon $b \in R^\times$, also ist r immer irreduzibel. □

Definition 2.2.11. Maximale Ideale

Sei R ein Ring und $\mathfrak{m} \subset R$ ein Ideal. Dieses heißt **maximal**, wenn es maximal unter allen echten Idealen von R ist, wenn also gilt:

$$\forall \mathcal{J} \subset R, \mathcal{J} \text{ Ideal} : \mathfrak{m} \subseteq \mathcal{J} \Rightarrow \mathfrak{m} = \mathcal{J} \tag{2.2.12}$$

Satz 2.2.12. Maximale Ideale erzeugen Körper

Sei R ein Ring und $\mathcal{I} \subseteq R$ ein Ideal. Dann sind äquivalent:

(i) $\mathcal{I} \subseteq R$ ist maximal.

(ii) $R/_\mathcal{I}$ ist ein Körper.

Beweis. (i) $\Rightarrow$ (ii): Sei $\mathcal{I} \subset R$ maximal. Sei $[0] \neq [x] \in R/_\mathcal{I}$. Dann gilt: $x \notin \mathcal{I} \Rightarrow \mathcal{I} \subset (I \cup [x]) \subseteq R$ ist ein Ideal. Da $\mathcal{I}$ maximal ist, gilt also $(\mathcal{I} \cup [x]) = R$. Dann existiert ein $y \in \mathcal{I}$ und ein $r \in R$ mit $y + rx = 1$. Also $[r] \cdot [x] = [1]$, womit ein multiplikatives Inverses existiert, also ist $R/_\mathcal{I}$ ein Körper.
(ii) $\Rightarrow$ (i): Sei $R/_\mathcal{I}$ ein Körper und $\mathcal{I} \subset \mathcal{J} \subseteq R$ ein Ideal. Sei $x \in \mathcal{J} \setminus \mathcal{I}$, dann gilt also $0 \neq [x] \in R/_\mathcal{I}$. Also hat $[x]$ ein Inverses $r \in R$ mit $[x] \cdot [r] = [1]$. Daraus folgt, dass $1 = xr + y$, also $1 \in \mathcal{J}$ und damit $\mathcal{J} = R$. □

Korollar 2.2.13 (Aus Satz 2.2.12)**.** Jedes maximale Ideal ist ein Primideal.

Beispiele. 1. Sei $\mathbb{K}$ ein Körper und $\mathbb{K}[x, y] = (\mathbb{K}[x])[y]$ der Polynomring in Variablen x und y. Die Gruppe der Einheiten ist $\mathbb{K}[x, y]^\times = \mathbb{K}^\times$. Das Ideal (y) ist gerade der Kern des Evaluationshomomorphismus

$$\begin{aligned} \mathbb{K}[x, y] &\to \mathbb{K}[x] \\ f(x, y) &\mapsto f(x, 0). \end{aligned} \tag{2.2.13}$$

Nach dem Isomorphiesatz 2.1.12 gilt

$$K[x, y]/(y) \cong \mathbb{K}[x], \tag{2.2.14}$$

und weiterhin, da $\mathbb{K}[x]$ nullteilerfrei ist, dass (y) ein Primideal, also y ein Primelement und damit irreduzibel ist. Also ist (y) maximal unter den Hauptidealen gemäß Satz 2.2.10. Da $\mathbb{K}[x]$ kein Körper ist, kann (y) kein maximales Ideal sein. Dies sehen wir auch explizit sofort ein: Sei z.B.

$$(y) \subset (x, y) \subset \mathbb{K}[x, y]. \tag{2.2.15}$$

Weiterhin ist (x, y) der Kern von

$$\begin{aligned} \mathbb{K}[x, y] &\to \mathbb{K} \\ f(x, y) &\mapsto f(0, 0). \end{aligned} \tag{2.2.16}$$

Also ist $\mathbb{K} \cong \mathbb{K}[x, y]/(x, y)$, woraus folgt, dass (x, y) maximal ist.

2. Für $\mathbb{K} = \overline{\mathbb{K}}$ gilt der **Hilbertsche Nullstellensatz**: Die maximalen Ideale in $\mathbb{K}[x, y]$ sind genau die Ideale der Form $(x - a, y - b)$ mit $a, b \in \mathbb{K}$.

Definition 2.2.14. Hauptidealring

Ein nullteilerfreier Ring R heißt **Hauptidealring**, falls jedes Ideal ein Hauptideal ist.

Satz 2.2.15

Sei R ein Hauptidealring. Dann sind für $r \in R$ äquivalent:

(i) r ist irreduzibel.

(ii) r ist Primelement.

Beweis. (ii) $\Rightarrow$ (i): Schon bewiesen.
(i) $\Rightarrow$ (ii): Sei r irreduzibel. Dann ist (r) maximal unter den Hauptidealen, also ist (r) maximal und damit ein Primideal. Damit muss r ein Primelement sein. □

Definition 2.2.16. Euklidische Ringe

Ein Integritätsbereich R heißt **euklidischer Ring**, falls eine Abbildung

$$\lambda : R \backslash \{0\} \to \mathbb{N} \tag{2.2.17}$$

mit folgender Eigenschaft existiert: Für alle $a, b \in R$ mit $b \neq 0$ existieren Elemente $q, r \in R$, sodass $a = q \cdot b + r$, wobei entweder $r = 0$ oder $\lambda(r) < \lambda(b)$ gilt.

Satz 2.2.17. Euklidische Ringe sind HIR

Jeder euklidische Ring ist ein Hauptidealring.

Beweis. Sei $\{0\} \neq \mathcal{I} \subseteq R$ ein Ideal. Wähle $0 \neq x \in \mathcal{I}$ mit $\lambda(x)$ minimal (Wohlordnung von $\mathbb{N}$). Für $y \in \mathcal{I}$ beliebig existieren $q, r \in R$ mit $y = qx + r$, sodass entweder $r = 0$ oder $\lambda(r) < \lambda(x)$ gilt. Der letztere Fall ist unmöglich, da $\lambda(x)$ minimal ist. Also gilt $r = 0$, woraus $\mathcal{I} = (x)$ folgt. □

Beispiele. Folgende Ringe sind euklidisch:

1. Der Ring $(\mathbb{Z}, +, \cdot)$ mit $\lambda(n) = |n|$.
2. Der Polynomring $\mathbb{K}[x]$ mit $\lambda(f) = \deg(f)$, wobei $\mathbb{K}$ ein Körper sein muss.
3. Die gaußschen Zahlen $\mathbb{Z}[i]$ mit $\lambda(\alpha) = N(\alpha) = a^2 + b^2$.

Beweis. 1. und 2. sind bereits aus der Schule als Division mit Rest und Polynomdivision bekannt. Zeigen wir also 3.: Zu gegebenen $\alpha, \beta \in \mathbb{Z}[i]$, mit $\alpha, \beta \neq 0$ müssen wir $q, r \in \mathbb{Z}[i]$ finden, sodass $\alpha = q\beta + r$, wobei entweder $r = 0$ oder $N(r) < N(\beta)$ gilt. Fasse $\mathbb{Z}[i] \subseteq \mathbb{C}$ auf und betrachte die komplexe Zahl $z := \frac{\alpha}{\beta} \in \mathbb{C}$. Falls $z \in \mathbb{Z}[i]$ gilt, setze $q = z$ und $r = 0$. Andernfalls gilt $r = \alpha - q\beta$ und wir suchen r mit $N(r) < N(\beta)$. Das gilt genau dann, wenn $\frac{N(r)}{N(\beta)} = N\left(\frac{r}{\beta}\right) < 1$, was äquivalent zu $|\underbrace{\frac{\alpha}{\beta}}_{=z\in\mathbb{C}} - \underbrace{q}_{\in\mathbb{Z}[i]}| < 1\,(*)$ ist. Dieses $q \in \mathbb{Z}[i]$ gilt es, zu finden. Die Zahl z liegt in einer der quadratischen Maschen, die vom Gitter $\mathbb{Z}[i]$ aufgespannt werden. Einer der Eckpunkte q dieses Quadrats erfüllt immer die Ungleichung $(*)$, da $\max d(q, z) = \frac{\sqrt{2}}{2} < 1$. □

Definition 2.2.18. assoziiert

Sei R ein Integritätsbereich. Zwei Elemente $a, b \in R$ heißen **assoziiert**, geschrieben $a \sim b$, wenn ein $n \in \mathbb{R}^\times$ mit $a = nb$ existiert.

Satz 2.2.19. Assoziiertheit = gleiche Hauptideale

Es gilt $a \sim b$ genau dann, wenn $(a) = (b)$.

Beweis. Wir zeigen $\Leftarrow$: Es existiert ein $r \in R$ mit $b = ra$ und ein $s \in R$ mit $a = sb$. Dann gilt $b = rsb \Leftrightarrow (1 - rs)b = 0$, wegen der Nullteilerfreiheit also $rs = 1$. □

Definition 2.2.20. faktoriell

Ein Integritätsbereich R heißt **faktoriell**, falls für jede Nichteinheit $a \in R$ mit $a \neq 0$ gilt:

(i) Es gibt eine Faktorzerlegung

$$a = p_1 p_2 \cdots p_m \tag{2.2.18}$$

in m irreduzible Faktoren.

(ii) Falls $a = p_1 p_2 \cdots p_m$ und $a = q_1 q_2 \cdots q_n$ Faktorzerlegungen in irreduzible Faktoren sind, dann gilt:

(a) $m = n$

(b) Nach geeigneter Umbennenung der Faktoren gilt für alle $1 \leq i \leq m$: $p_i \sim q_i$.

Satz 2.2.21. Irreduzible Elemente sind Primelemente in Faktorringen

Sei R ein Integritätsbereich, in dem jede Nichteinheit $a \neq 0$ eine Faktorzerlegung in Form von Gleichung 2.2.18 besitzt. Dann sind äquivalent:

(a) R ist faktoriell.

(b) Jedes irreduzible Element ist ein Primelement.

Beweis. (a) $\Rightarrow$ (b): Sei R faktoriell und $r \in R$ irreduzibel. Seien $a, b \in R$ mit $r \mid ab$. Per Definition gibt es ein $s \in R$ mit $sr = ab$. Zerlege alle Teile der Gleichung in irreduzible Elemente, also

$$s_1 s_2 \cdots s_t r = a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n. \tag{2.2.19}$$

Also ist $r \sim a_i$ für ein $1 \leq i \leq m$ oder $r \sim b_j$ für $1 \leq j \leq n$. Je nachdem gilt also $r \mid a$ oder $r \mid b$.
(b) $\Rightarrow$ (a): Sei $a \in R$ mit $a \neq 0$ und $a \notin R^\times$. Betrachte zwei Zerlegungen

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n. \tag{2.2.20}$$

in irreduzible Elemente. O.B.d.A. sei $m \leq n$. Es gilt $p_1 \mid q_1 q_2 \cdots q_n$ und, da p_i ein Primelement ist, auch, dass ein j mit $p_i \mid q_j$ existiert. O.B.d.A. sei $p_i \mid q_i$. Da aber q_i irreduzibel ist, existiert ein $n \in R^\times$ mit $q_1 = np_1$. Durch Kürzen mit p_1 erhalten wir

$$p_2 p_3 \cdots p_m = \tilde{q}_2 q_3 \cdots q_n \tag{2.2.21}$$

mit $q_2 \sim \tilde{q}_2$. Durch Induktion über m reduzieren wir auf $m = 1$. Dann gilt:

$$p_1 = q_1 q_2 \cdots q_n. \tag{2.2.22}$$

Da aber p_1 irreduzibel ist, muss $n = 1$ und $p_1 = q_1$ gelten. □

Satz 2.2.22. Hauptidealringe sind faktoriell

Sei R ein Hauptidealring. Dann ist R faktoriell.

Beweis. Nach obigen Überlegungen genügt es, die Existenz von Zerlegungen wie in Gleichung 2.2.18 nachzuweisen. Angenommen, es gibt $0 \neq a$ mit $a \notin R^\times$, welches keine Faktorzerlegung 2.2.18 zulässt. Dann ist a also reduzibel (nicht irreduzibel), es gibt also eine nichttriviale Zerlegung

$$a = x_1 y_1 \tag{2.2.23}$$

mit $0 \neq x_1, y_1$ und $x_1, y_1 \notin R^\times$. Dann hat entweder x_1 oder y_1 keine Zerlegung gemäß 2.2.18. Sei o.B.d.A. x_1 nichttrivial zerlegbar in

$$x_1 = x_2 y_2. \tag{2.2.24}$$

Rekursive Fortsetzung dieses Prozesses liefert eine Folge

$$(x_1) \subset (x_2) \subset (x_3) \subset \cdots \subset R \tag{2.2.25}$$

von echten Inklusionen. Die Vereinigung

$$\mathcal{U} = \bigcup_{i \geq 0} (x_i) \subseteq R \tag{2.2.26}$$

ist ein Ideal. Da R ein Hauptidealring ist, existiert ein $b \in R$ mit $(b) = \mathcal{U}$. Dann existiert ein $i \geq 0$ mit $b \in (x_i)$, also $(b) = (x_i)$. Dies impliziert aber auch, dass für alle $j > i$ gilt, dass $(b) = (x_j)$, denn $(x_i) \subseteq (x_j) \subseteq (b)$. Dies ist ein Widerspruch zu den echten Inklusionen. □

Übung. Verifiziere:

- Die rekursive Fortsetzung des Prozesses liefert tatsächlich eine wohldefinierte Folge.
- Die Vereinigung ist tatsächlich ein Ideal (Das gilt nicht allgemein!).

Bemerkung. Das Argument aus dem Beweis von Satz 2.2.22 zeigt, dass jeder Hauptidealring die folgende Eigenschaft hat:
Für jede aufsteigende Kette

$$\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots \subseteq R \tag{2.2.27}$$

von Idealen $\mathcal{I}_i$ in R gibt es ein $k_0 \in \mathbb{N}$, sodass für alle $k \geq k_0$ gilt, dass $\mathcal{I}_{k_0} = \mathcal{I}_k$. Man sagt, dass jede aufsteigende Kette von Idealen **stationär** wird. Ringe mit dieser Eigenschaft heißen **Noethersche Ringe**.

Zum Abschluss der Diskussion zur verallgemeinerten Primfaktorzerlegung betrachten wir die Klassifikation der Prim-

ideale in $\mathbb{Z}$.

Definition 2.2.23. Spektrum

Die Menge der Primideale $\mathfrak{p}$ eines Ringes R heißt Spektrum $\mathfrak{P}$ von R.

Bemerkung. Für $R = \mathbb{Z}$ ist $\mathfrak{P} = \{(0), (p)\}$, wobei p eine Primzahl ist.

Lemma 2.2.24. Primzahlen in $\mathbb{Z}$ Sei p eine ungerade Primzahl. Dann sind äquivalent:

(a) Es gibt Zahlen $a, b \in \mathbb{Z}$ mit $a^2 + b^2 = p$.

(b) Es gilt $p \equiv_4 1$.

Beweis. Sei zunächst p eine ungerade Primzahl mit $p = a^2 + b^2$. Die Quadrate in $\mathbb{Z}/(4)$ sind $0^2 = 0$, $1^2 = 1$, $2^2 = 0$ und $3^2 = 1$. Daraus folgt (b).
Sei nun $p = 1 + 4n$ mit $n \in \mathbb{N}$. Wir rechnen zunächst in $\mathbb{Z}/(p)$:

$$[(p-1)!] = [1][2]\cdots[p-1] = [-1] \tag{2.2.28}$$

Dies gilt, da der Restklassenring $\mathbb{Z}/(p)$ ein Körper ist, also jedes von 0 verschiedene Element ein Inverses und die einzigen selbstinversen Elemente sind 1 und -1, die Nullstellen des Polynoms $x^2 - 1 = 0$. Das heißt also, dass $[2][p-2] = [1]$, $[3][p-3] = 1$ usw., sodass die Gleichung erfüllt ist.
Wir rechnen weiter:

$$[-1] = [(p-1)!] = [1][2]\cdots[2n][p-2n]\cdots[p-1] = [(2n)!]^2. \tag{2.2.29}$$

Also ist $x = (2n)!$ eine Lösung der Kongruenz $x^2 \equiv_4 -1$. Die Primzahl p ist also ein Teiler von $x^2 + 1 = (x+i)(x-i)$, aber p teilt weder $(x+i)$ noch $(x-i)$. Daher ist p kein Primelement in den Gaußschen Zahlen. Da $\mathbb{Z}[i]$ ein Hauptidealring und damit faktoriell ist, gibt es also eine Zerlegung

$$p = \alpha\beta \tag{2.2.30}$$

in $\mathbb{Z}[i]$ mit $\alpha, \beta \notin \mathbb{Z}[i]^\times$. Wir gehen über zu Normen:

$$p^2 = N(\alpha) \cdot N(\beta). \tag{2.2.31}$$

Da α und β Nichteinheiten sind, ist $N(\alpha), N(\beta) \neq 1$. Also muss $N(\alpha) = p = N(\beta)$ gelten. Ist $\alpha = a + ib$, so ist $p = a^2 + b^2$. □

Theorem 2.2.25. Das Spektrum der gaußschen Zahlen

Das Spektrum $\mathfrak{P}(\mathbb{Z}[i])$ besteht aus:

(i) $(1 + i)$

(ii) $\{(a + bi) | a^2 + b^2 = p, p \text{ prim}, p \equiv_4 1, a > |b|\}$

(iii) $\{(p) | p \text{ prim}, p \equiv_4 3\}$.

Beweis. Die Erzeuger x der Ideale aus (i) und (ii) sind Primelemente: Für eine Zerlegung $x = \alpha\beta$ gilt $N(\alpha)N(\beta) = p$, wobei p prim ist. Also ist $N(\alpha) = 1$ oder $N(\beta) = 1$, und damit entweder α oder β eine Einheit.
Eine Primzahl p aus (iii) muss irreduzibel sein, da für eine nicht-triviale Zerlegung $p = \alpha\beta$, analog zu Beweis 2.2.24, gelten würde, dass $N(\alpha) = N(\beta) = p = a^2 + b^2$. Dies ist aber ein Widerspruch, da $p \equiv_4 3$.
Es bleibt nur noch zu zeigen, dass diese Liste vollständig ist. Dafür zeigen wir, dass jedes Primelement $\pi \in \mathbb{Z}[i]$ assoziiert zu (genau) einem der Erzeuger aus (i), (ii) oder (iii) ist. Zunächst folgt aus der Primfaktorzerlegung

$$N(\pi) = \pi \cdot \overline{\pi} = p_1 p_2 \cdots p_n \tag{2.2.32}$$

in $\mathbb{N}$, dass eine Zahl $i \in \mathbb{N}$ mit $1 \leq i \leq n$ existiert, sodass $\pi \mid p_i$. Setze $p := p_i$. Dann teilt $N(\pi)$ also auch $N(p) = p^2$. Also ist entweder $N(\pi) = p$ oder $N(\pi) = p^2$. Gilt $N(\pi) = p$, so ist π assoziiert zu einem der Erzeuger aus (i) oder (ii). Ist andererseits $N(\pi) = p^2$, so gilt, dass $N\left(\frac{p}{\pi}\right) = 1$, also ist $\pi \sim p$. In diesem Fall muss gelten, dass $p \equiv_4 3$, denn andernfalls wäre $\pi = \epsilon(a + ib)(a - ib)$ mit $\epsilon \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ reduzibel, im Widerspruch zu Lemma 2.2.24. □

Beispiel. Aus Theorem 2.2.25 erschließt sich also ein präzises Verständnis des Zerlegungsverhaltens von Primidealen beim Übergang von $\mathbb{Z}$ nach $\mathbb{Z}[i]$:

(a) Das Primideal (2) zerfällt in $(1 + i)^2$.

(b) Die Primideale (p) mit $p \equiv_4 1$ zerfallen in ein Produkt $(p) = (a + ib)(a - ib)$ von komplex konjugierten Idealen.

(c) Die Primideale (p) mit $p \equiv_4 3$ bleiben prim.

Definition 2.2.26. Dedekindring

Ein Integritätsbereich R heißt **Dedekindring**, falls R kein Körper ist und für jedes Paar von Idealen $\mathcal{I}, \mathcal{J} \subseteq R$ die folgenden Bedingungen äquivalent sind:

(i) $\mathcal{I} \mid \mathcal{J}$

(ii) Es existiert ein Ideal $\mathcal{K} \subseteq R$ mit $\mathcal{J} = \mathcal{I} \cdot \mathcal{K}$.

Bemerkung. Oftmals ist die folgende, äquivalente Definition nützlicher zur Überprüfung:
Ein Integritätsbereich R ist ein Dedekindring, wenn:

(a) R ist noetherisch.

(b) R ist *ganz abgeschlossen* in seinem *Divisionskörper*

$$(R \setminus \{0\})^{-1}R := \left\{ \frac{r}{s} \middle| r \in R, s \in R \setminus \{0\} \right\} \tag{2.2.33}$$

(c) Die Primideale $\mathfrak{p} \neq (0)$ sind gerade die maximalen Ideale.

Wir geben noch einen Satz ohne Beweis an:

Satz 2.2.27. Reduzibilität in Dedekindringen

Sei R ein Dedekindring und sei $\mathcal{I} \subset R$ ein echtes Ideal mit $\mathcal{I} \neq (0)$. Dann gibt es eine bis aus Permutation der Faktoren eindeutige Zerlegung

$$\mathcal{I} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n \tag{2.2.34}$$

mit $\mathfrak{p}_i \subseteq R$ Primideal.

Übung. Zeige, dass sich die Uneindeutigkeit der Zerlegung

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{2.2.35}$$

in $\mathbb{Z}[\sqrt{-5}]$ nach Übergang zu Idealen

$$\begin{aligned} \mathfrak{p}_1 &= (2, 1 + \sqrt{-5}) \\ \mathfrak{p}_2 &= (2, 1 - \sqrt{-5}) \\ \mathfrak{p}_3 &= (3, 1 + \sqrt{-5}) \\ \mathfrak{p}_4 &= (3, 1 - \sqrt{-5}) \end{aligned} \tag{2.2.36}$$

gilt:

$$\begin{aligned} (2) &= \mathfrak{p}_1\mathfrak{p}_2 \\ (3) &= \mathfrak{p}_3\mathfrak{p}_4 \\ (1 + \sqrt{-5}) &= \mathfrak{p}_1\mathfrak{p}_3 \\ (1 - \sqrt{-5}) &= \mathfrak{p}_2\mathfrak{p}_4, \end{aligned} \tag{2.2.37}$$

also ist $(6) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ eindeutig.

2.3 Faktorisierung in Polynomringen

Beispiele. Sei $\mathbb{K}$ ein Körper. Dann ist $\mathbb{K}[x]$ euklidisch, also insbesondere ein Hauptidealring. Damit ist $\mathbb{K}[x]$ faktoriell, $\mathbb{K}[x]^\times = \mathbb{K}\setminus\{0\} \cdots$. Was sind die irreduziblen Polynome?

1. Sei $\mathbb{K} = \mathbb{C}$. Dann gilt der Fundamentalsatz der Algebra, sodass jedes Polynom $f(x) \in \mathbb{C}[x]$ in Linearfaktoren zerfällt:
$$f(x) = c\prod_{i=1}^{n}(x - \lambda_i). \tag{2.3.1}$$
Die irreduziblen Polynome sind also $(x - \lambda_i)$ mit $\lambda_i \in \mathbb{C}$.
2. Für $\mathbb{K} = \mathbb{R}$ haben wir:
   - $(x - \lambda)$, $\lambda \in \mathbb{R}$ ist irreduzibel.
   - $x^2 + ax + b$ mit $a, b \in \mathbb{R}$ ist irreduzibel, falls für die Diskriminante $a^2 - 4b < 0$ gilt. Ist $\deg(f) \geq 3$, ist f nicht irreduzibel, da in $\mathbb{C}[x]$ gilt:
   $$f(x) = r(x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_n) = r(x - \overline{\lambda}_1)\cdots(x - \overline{\lambda}_n) \tag{2.3.2}$$
   da für $f \in \mathbb{R}[x]$ die Konjugation der Identität entspricht. Also folgt $\lambda_i = \overline{\lambda}_1$. Ist $\lambda_1 = \overline{\lambda}_1$, hat f eine reelle Nullstelle $\lambda = \lambda_1$, also $f = (x - \lambda)g$. Ist hingegen $\lambda_i = \overline{\lambda}_i =: \lambda$ mit $i \neq 1$, so ist
   $$f = (x - \lambda)(x - \overline{\lambda})g = \underbrace{(x^2 - (\lambda + \overline{\lambda})x + \lambda\overline{\lambda})}_{\in\mathbb{R}[x]}\, g. \tag{2.3.3}$$
3. $\mathbb{K} = \mathbb{Q}$ wollen wir sodann näher untersuchen.
4. $\mathbb{K} = \mathbb{F}_2$. Ist $x^2 + +x + 1$ irreduzibel? Ausprobieren aller Elemente von $\mathbb{F}_2$ zeigt, dass das Polynom irreduzibel ist. Daraus folgt auch, dass das Polynom in $\mathbb{Z}[x]$ irreduzibel ist! Auf dieser Idee wollen wir fortan aufbauen.

Unser Ziel ist nun, den Zusammenhang der Irreduzibilität in $\mathbb{Z}[x]$ mit der in $\mathbb{Q}[x]$ zu verstehen.

Definition 2.3.1. Primitivität

Wir nennen ein Polynom

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \tag{2.3.4}$$

primitiv, falls:

(i) $a_n > 0$
(ii) $\mathrm{ggT}(a_0, a_1, \ldots, a_n) = \{\pm 1\}$, also $(a_0, a_1, \ldots, a_n) = \mathbb{Z}$.

Übung. Man zeige, dass $(a_0, a_1, \ldots, a_n) = \mathbb{Z}$.

Lemma 2.3.2. Inhalt Sei $f \in \mathbb{Q}[x]$. Dann gilt:

(i) Es existiert ein eindeutiges $c(f) \in \mathbb{Q}$, genannt **Inhalt** von f, und ein eindeutiges primitives Polynom $f_0 \in \mathbb{Z}[x]$, sodass
$$f(x) = c(f) f_0(x). \tag{2.3.5}$$
(ii) Es gilt $f \in \mathbb{Z}[x]$ genau dann, wenn $c(f) \in \mathbb{Z}$.

Beweis. (i) Es existiert $m \in \mathbb{Z}$, sodass $f_0 = mf \in \mathbb{Z}[x]$. Sei t der größte gemeinsame Teilder der Koeffizienten von f_0. Dann ist das Polynom $f_1 = \frac{1}{t} f_o \in \mathbb{Z}[x]$ primitiv. Daraus folgt
$$f = \frac{t}{m} f_1 \tag{2.3.6}$$
mit $\frac{t}{m} \in \mathbb{Q}$ und $f_1 \in \mathbb{Z}[x]$.
Seien $c, d \in \mathbb{Q}$ und $g, h \in \mathbb{Z}[x]$ primitiv mit $f = cg = dh$. O.B.d.A. nehmen wir an, dass $c, d \in \mathbb{Z}$. Für alle $0 \leq i \leq n$ gilt, dass $cb_i = de_i$, also
$$(c) = (cb_0, \ldots, cb_n) = (de_0, \ldots, de_n) = (d). \tag{2.3.7}$$
Damit folgt $c = d$ oder $c = -d$. Mit der Primitivität erhalten wir $c = d$. □

Übung. Beweise (ii).

Lemma 2.3.3. Gauß-Lemma Das Produkt primitiver Polynome ist primitiv.

Beweis. Seien $f, g \in \mathbb{Z}[x]$ primitive Polynome. Der Leitkoeffizient von $f \cdot g$ ist als Produkt der Leitkoeffizienten positiv. Wir betrachten für jede Primzahl p den Ringhomomorphismus
$$\begin{aligned} \pi : \mathbb{Z}[x] &\to \mathbb{F}_p[x] \\ \sum_{i=0}^{n} a_i x^i &\mapsto \sum_{i=0}^{n} [a_i]_p x^i. \end{aligned} \tag{2.3.8}$$
Sind die Leitkoeffizienten von f und g nicht teilerfremd, so existiert ein p mit $\pi(fg) = \pi(f)\pi(g) = 0$. Da $\mathbb{F}_p[x]$ ein Integritätsbereich ist, müsste bereits $\pi(f) = 0$ oder $\pi(g) = 0$ gelten. Das widerspricht allerdings der Primitivität von f und g. □

Korollar 2.3.4 (Aus Lemma 2.3.3)**.** Für $f, g \in \mathbb{Q}[x]$ gilt:
$$c(fg) = c(f)c(g) \tag{2.3.9}$$

Übung. Beweise das Korollar.

Satz 2.3.5. Irreduzibilität in $\mathbb{Z}[x]$

Sei $f \in \mathbb{Z}[x]$ ein Polynom mit positivem Leitkoeffizienten. Dann sind äquivalent:
(i) f ist irreduzibel.
(ii) Entweder ist f eine Primzahl (also von Grad 0) oder f ist primitiv und irreduzibel über $\mathbb{Q}[x]$.

Beweis. (2) ⇒ (1): Ist klar und dem Leser überlassen.
(1) ⇒ (2): Zerlege $f = c(f) f_0$ mit $c(f) \in \mathbb{Z}$ und $f_0 \in \mathbb{Z}[x]$ primitiv. Da f irreduzibel ist, muss entweder $c(f) \in \mathbb{Z}^\times$ oder $f_0 \in \mathbb{Z}[x]^\times$ gelten.
(a) Sei also $f_0 \in \mathbb{Z}[x]^\times$, also $f_0 = 1$. Dann ist $f = c(f) \in \mathbb{Z}$, also ist f eine Primzahl, da f irreduzibel ist.
(b) Sei nun $c(f) \in \mathbb{Z}^\times$, also $c(f) = 1$. Dann gilt $f = f_0$, also ist f primitiv. Angenommen, f ließe sich zerlegen in $f = gh$ mit $g, h \in \mathbb{Q}[x]$. Aus Korrolar 2.3.4 folgt, dass $c(f) = c(g)c(h) = 1$, und damit
$$f = gh = c(g)c(h)g_0 h_0 = g_0 h_0 \tag{2.3.10}$$
mit $g_0, h_0 \in \mathbb{Z}[x]$. Also ist entweder g_0 oder h_0 eine Einheit in $\mathbb{Z}[x]^\times$ und damit $g_0 = 1$ oder $h_0 = 1$. Sei also $g_0 = 1$. Dann ist $f = c(g)h$. Da $c(g)$ eine Einheit in $\mathbb{Q}[x]$ ist, folgt, dass f irreduzibel über $\mathbb{Q}[x]$ ist.
□

Theorem 2.3.6. Faktorisierung ganzzahliger Polynome

Der Ring $\mathbb{Z}[x]$ ist faktoriell.

Beweis. Sei $f \in \mathbb{Z}[x]$, dann können wir f in $\mathbb{Q}[x]$ zerlegen:

$$f = f_1 f_2 \cdots f_n \tag{2.3.11}$$

mit $f_i \in \mathbb{Q}[x]$ irreduzibel für alle $i \in \mathbb{N}$. Es gilt also

$$f = f_1 \cdots f_n = c(f_1 \cdots f_n) \cdot (f_1)_0 \cdots (f_n)_0. \tag{2.3.12}$$

Da Z faktoriell ist, können wir $c(f_1 \cdots f_n)$ in Primfaktoren zerlegen. Da für alle $1 \leq i \leq n$ gilt, dass $f_i = c(f_i)(f_i)_0$, ist auch $(f_i)_0$ irreduzibel in $\mathbb{Q}[x]$. Da $(f_i)_0$ auch primitiv ist, ist es auch irreduzibel in $\mathbb{Z}[x]$. Es bleibt die Eindeutigkeit. Nach Satz ... reicht es, zu zeigen, dass jedes irreduzible Element $f \in \mathbb{Z}[x]$ auch ein Primelement ist. Seien $g, h \in \mathbb{Z}[x]$, sodass $f \mid gh$. Dann gibt es zwei Fälle:

1. Fall: f ist eine Primzahl p. Dann zerlegen wir $g = c(g)g_0$ und $h = c(h)h_0$. Da $g_0 h_0$ primitiv ist, hat $g_0 h_0$ mindestens einen Koeffizienten a, der nicht durch p teilbar ist. Da aber $f \mid gh$, muss $p \mid ac(h)c(g)$ gelten, also entweder $p \mid c(g)$ oder $p \mid c(h)$. Es folgt $p \mid g$ oder $p \mid h$.

□

2.4 Moduln

Definition 2.4.1. Modul

Ein **R-Modul** ist ein Tripel $(M, +, \cdot)$, bestehend aus einer Menge M, einer Addition $+$, die eine abelsche Gruppe $(M, +)$ bildet, und einer **Skalarmultiplikation**

$$\begin{aligned} \cdot : R \times M &\to M \\ (r, m) &\mapsto r \cdot m, \end{aligned} \tag{2.4.1}$$

sodass für alle $m, n \in M$ und alle $r, s \in R$ gilt:

(M1) $r \cdot (s \cdot m) = (rs) \cdot m$.

(M2) $(r + s) \cdot m = r \cdot m + s \cdot m$.

(M3) $r \cdot (m + n) = r \cdot m + r \cdot n$.

(M4) $\exists 1 \in R : 1 \cdot m = m$.

Beispiele.

1. Ist $R = \mathbb{K}$ ein Körper, so sind $\mathbb{K}$-Moduln gerade Vektorräume über $\mathbb{K}$.
2. Für jede natürliche Zahl $n \geq 0$ ist das kartesische Produkt

$$R^n = \underbrace{R \times R \times \cdots \times R}_{n} \tag{2.4.2}$$

ein R-Modul mit der Skalarmultiplikation

$$\begin{aligned} R \times R^n &\to R^n \\ (r, (r_1, \ldots, r_n)) &\mapsto r \cdot (r_1, \ldots, r_n) = (rr_1, \ldots, rr_n), \end{aligned} \tag{2.4.3}$$

genannt **freier Standard-R-Modul von Rang n**.

3. Für R-Moduln M, N ist das kartesische Produkt $M \times N$ ein R-Modul mit der Skalarmultiplikation

$$(r, (x, y)) \mapsto (rx, ry). \tag{2.4.4}$$

Übung. Ein $\mathbb{Z}$-Modul ist eine abelsche Gruppe.

Wir stellen fest, dass sich jedes Element in $M \times N$ eindeutig als Summe $(x, y) = (x, 0) + (0, y)$ mithilfe der kanonischen Inklusionen $x \hookrightarrow (x, 0)$ und $y \hookrightarrow (0, y)$ schreiben lässt. Das rechtfertigt die folgende Definition:

Definition 2.4.2. Direkte Summe (Moduln)

Seien M, N Moduln und $M \times N$ das Produktmodul. Dann schreiben wir

$$M \oplus N := M \times N \tag{2.4.5}$$

und nennen $M \oplus N$ die **direkte Summe** von M und N.

Wir wollen nun bekannte Resultate der linearen Algebra auf Moduln übertragen.

Definition 2.4.3. Lineare Abbildung

Eine Abbildung $\varphi : M \to N$ zwischen R-Moduln M und N heißt **R-linear**, falls für alle $r \in R$ und $m, n \in M$ gilt:

(L1) $\varphi(rm + rn) = r\phi(m) + r\phi(n)$.

Definition 2.4.4. Isomorphismus von Moduln

Sei $\varphi : M \to N$ eine lineare Abbildung zwischen R-Moduln. Ist φ bijektiv, so heißt φ **Isomorphismus von R-Moduln**.

Definition 2.4.5. Untermodul und Erzeugnis

Sei M ein R-Modul.

1. Ein **Untermodul** $N \leq M$ ist eine abelsche Untergruppe von M, die zusätzlich abgeschlossen unter Skalarmultiplikation ist, also $ry \in N$ für alle $y \in M$ und alle $r \in R$. N erbt eine R-Modul-Struktur von M.
2. Für eine Teilmenge $S \subseteq M$ heißt der Untermodul
$$\langle S \rangle := \bigcap_{S \subseteq N \leq M} N \tag{2.4.6}$$
der von S **erzeugte Untermodul**.

Übung. Zeigen Sie, dass das erzeugte Untermodul tatsächlich ein Untermodul ist.

Beispiel. DIe Untermoduln des freien R-Moduls von Rang 1 sin genau die Ideale von R.

Satz 2.4.6. Bild und Kern

Sei $\varphi : M \to N$ eine R-lineare Abbildung zwischen R-Moduln. Dann gilt:

(i) $\mathrm{im}(\varphi) \leq N$ ist ein Untermodul.
(ii) $\ker(\varphi) \leq M$ ist ein Untermodul.
(iii) φ ist injektiv genau dann, wenn $\ker(\varphi) = \{0\}$.

Definition 2.4.7. Quotientenmodul

Sei M ein R-Modul und $N \leq M$ ein Untermodul. Dann ist $(M/N, +, \cdot)$ mit der Verknüpfung
$$\begin{aligned} \cdot : R \times M/N &\to M/N \\ (r, [x]) &\mapsto [rx] \end{aligned} \tag{2.4.7}$$
ein R-Modul, genannt **Quotientenmodul** von M modulo N.

Theorem 2.4.8. Isomorphiesatz

Sei $\varphi : M \to N$ eine R-lineare Abbildung zwischen Moduln. Dann ist die induzierte Abbildung
$$\begin{aligned} \overline{\varphi} : M/\ker(\varphi) &\to \mathrm{im}(\varphi) \\ [x] &\mapsto \varphi(x) \end{aligned} \tag{2.4.8}$$
ein Isomorphismus von R-Moduln.

Definition 2.4.9. Freier Modul

Für eine natürliche Zahl $n \geq 0$ heißt ein R-Modul $\mathcal{F}$ **frei** von Rang n, falls es einen Isomorphismus $R^n \cong \mathcal{F}$ gibt.

Bemerkung.

Sei $\mathcal{F}$ frei von Rang n. Dann besitzt $\mathcal{F}$ eine R-Basis $(x_1, \ldots, x_n)$, sodass sich jedes $m \in \mathcal{F}$ auf eindeutige Weise als
$$m = \sum_{i=1}^{n} \lambda_i x_i \tag{2.4.9}$$
mit $\lambda_i \in R$ schreiben lässt.

Beispiel. In jedem Integritätsbereich R ist für $0 \neq a \in R$ das Ideal $(a) \subseteq R$ ein freier R-Modul von Rang 1 durch die Abbildung
$$\begin{aligned} R &\to (a) \\ r &\mapsto ra. \end{aligned} \tag{2.4.10}$$
Falls zusätzlich a eine Nichteinheit ist, ist der Quotientenmodul $R/(a)$ nicht frei, denn es gibt $0 \neq x \in R/(a)$ und $0 \neq r \in R$ mit $r \cdot x = 0$, z.B.: $R = \mathbb{Z}$, $0 \neq a \neq \{\pm 1\}$, $\mathbb{Z}/(a) \curvearrowright \mathbb{Z}$.

Wir stellen die Vermutung auf, dass endliche, nullteilerfreie Ringe Körper sind.

Definition 2.4.10. endlich erzeugt

Ein R-Modul M heißt **endlich erzeugt**, falls es eine surjektive, R-lineare Abbildung $R^n \to M$ mit $n \geq 0$ gibt.

Bemerkung. Ein Modul M ist genau dann endlich erzeugt, wenn es eine endliche Teilmenge $S \subseteq M$ gibt, sodass $\langle S \rangle = M$ gilt.

Definition 2.4.11. Kurze exakte Sequenz (Moduln)

Eine **kurze exakte Sequenz (KES)** von Moduln ist gegeben durch

$$\{0\} \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow \{0\},$$

wobei:

- M, M' und M'' R-Moduln sind.
- $f : M' \to M$ eine injektive, R-lineare Abbildung (Monomorphismus) ist.
- $g : M \to M''$ eine surjektive, R-lineare Abbildung (Epimorphismus) ist.
- $\mathrm{im}(f) = \ker(g)$ gilt.

Eine kurze exakte Sequenz **zerfällt**, falls eine R-lineare Abbildung $s : M' \to M$ mit $g \circ s = \mathrm{id}_{M''}$ existiert.

Satz 2.4.12. Zerfällungskriterium

Sei

$$\{0\} \longrightarrow N \xrightarrow{f} M \xrightarrow{g} \mathcal{F} \longrightarrow \{0\},$$

eine KES von Moduln, wobei $\mathcal{F}$ ein freier R-Modul ist. Dann zerfällt die KES mit $s : \mathcal{F} \to M$, $g \circ s = \mathrm{id}_{\mathcal{F}}$. Für jeden solchen Schnitt ist

$$\begin{aligned} \varphi : N \oplus \mathcal{F} &\to M \\ (x, y) &\mapsto f(x) + s(y) \end{aligned} \tag{2.4.11}$$

ein Isomorphismus.

Beweis. Wähle für die Elemente $x_1, \ldots, x_n$ einer R-Basis von $\mathcal{F}$ Elemente $y_1, \ldots, y_n \in M$ mit $g(y_i) = x_i$. Dann erfüllt der Schnitt die Eigenschaft

$$s\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i s(x_i). = \sum_{i=1}^{n} \lambda_i y_i. \tag{2.4.12}$$

1. φ ist injektiv: Sei $(x, y) \in N \oplus \mathcal{F}$ mit $\varphi(x, y) = f(x) + s(g)$. Anwendung von g liefert
$$0 = g\left(f(x)\right) + g\left(g(y)\right) = y \tag{2.4.13}$$
und damit $f(x) = 0$, also $x = 0$, da f injektiv ist.
2. φ ist surjektiv: Sei $m \in M$, also $g(m - s(g(m))) = 0$. Da $\ker(g) = \mathrm{im}(f)$ gilt, existiert $x \in M$ mit $m - s(y) = f(x)$, also
$$m = f(x) + s(y) = \varphi(x, y). \tag{2.4.14}$$

□

Beispiele. 1. Ganzzahlen:

$$\{0\} \longrightarrow \mathbb{Z} \xrightarrow{\cdot 5} \mathbb{Z} \longrightarrow \underbrace{\mathbb{Z}/(5)}_{\text{nicht frei}} \longrightarrow \{0\},$$

2. Kanonische Inklusion und Projektion:

$$\{0\} \longrightarrow M' \xrightarrow{\iota_{M'}} M' \oplus M'' \xrightarrow{\pi_{M''}} M'' \longrightarrow \{0\},$$

2.5 Endlich erzeugte Moduln über Hauptidealringen

⚠ In diesem Abschnitt bezeichnet R einen Hauptidealring (also insbesondere einen Integritätsbereich).

Lemma 2.5.1. Freie Moduln haben freie Untermoduln Sei $\mathcal{F}$ ein freier R-Modul von Rang $n \geq 0$ und $\mathcal{M} \leq \mathcal{F}$ ein Untermodul. Dann ist $\mathcal{M}$ auch frei von Rang n.

Beweis. Sei zunächst $n = 1$, also $\mathcal{F} \cong R$. O.B.d.A. also $\mathcal{F} = R$. Ein Untermodul von R ist ein Ideal $\mathcal{I} \subseteq R$, also insbesondere ein Hauptideal $\mathcal{I} = (a)$. Für $a \neq 0$ ist die Abbildung

$$\begin{aligned} R &\to (a) \\ r &\mapsto ra \end{aligned} \tag{2.5.1}$$

ein Isomorphismus, da R nullteilerfrei ist. Für $a = 0$ ist $\mathcal{I} = 0$ frei von Rang 0. Sei nun $\mathcal{F} \cong R^n$, also o.B.d.A. $\mathcal{F} = R^n$ mit $n > 1$. Betrachte die Projektionsabbildung

$$\begin{aligned} \pi : R^n &\to R \\ (r_1, r_2, \ldots, r_n) &\mapsto r_1 \end{aligned} \tag{2.5.2}$$

mit $\ker(\pi) \cong R^{n-1}$. Dies ist gerade der Untermodul von Tupeln mit $r_1 = 0$. Wir schränken nun π auf $\mathcal{M}$ ein und erhalten so eine KES

$$\{0\} \longrightarrow \ker(\pi(\mathcal{M})) \xrightarrow{\iota} \mathcal{M} \xrightarrow{\pi|_{\mathcal{M}}} \pi(\mathcal{M}) \longrightarrow \{0\}.$$

Nach Induktionsvoraussetzung ist $\pi(\mathcal{M})$ frei von Rang ≤ 1. Es gilt weiterhin:

$$\ker(\pi(\mathcal{M})) = \ker(\pi) \cap \mathcal{M} \leq \ker(\pi) \cong R^{n-1}. \tag{2.5.3}$$

Per Induktion nach n ist $\ker(\pi(\mathcal{M}))$ also frei von Rang $\leq n-1$, und nach Satz 2.4.12 spaltet die KES 2.5, sodass

$$M \cong \underbrace{\pi(\mathcal{M})}_{\text{frei} \leq 1} \oplus \underbrace{\ker(\pi(\mathcal{M}))}_{\text{frei} \leq n-1} \tag{2.5.4}$$

frei von Rang $\leq n$. □

Definition 2.5.2. Torsionsmodul

Sei M ein R-Modul.

1. Der **Torsionsmodul** von M ist definiert als
$$T(M) := \{x \in M | \exists r \in R, r \neq 0 : r \cdot x = 0\} \leq M. \tag{2.5.5}$$
2. Für $p \in R$ prim ist der **p-Torsionsuntermodul** oder **p-primäre Torsionsuntermodul** definiert als
$$T_p(M) := \{x \in M | \exists n \geq 0 : p^n \cdot x = 0\} \leq T(M). \tag{2.5.6}$$
3. M heißt **Torsionsmodul** bzw. **p-Torsionsmodul**, falls $T(M) = M$ bzw. $T_p(M) = M$.
4. M heißt **torsionsfrei**, falls $T(M) = 0$.

Übung. Zeige, dass der Torsionsmodul tatsächlich ein Untermodul ist. Dafür benötigt man die Nullteilerfreiheit von R.

Beispiel. Sei $R = \mathbb{Z}$ und betrachte

$$M = \mathbb{Z} \oplus \overbrace{\underbrace{\mathbb{Z}/(2)}_{T_2(M)} \oplus \underbrace{Z/(9)}_{T_3(M)}}^{T(M)}. \tag{2.5.7}$$

Lemma 2.5.3. Endlich torsionsfreie Module sind frei Sei M ein endlich erzeugter, torsionsfreier R-Modul. Dann ist M ein freier R-Modul.

Beweis. Nach Lemma 2.5.1 genügt es, zu zeigen, dass M ein Untermodul eines freien Moduls ist. Sei M erzeugt von der endlichen Menge $S \subseteq M$. Wir wählen eine maximale, R-linear unabhängige Teilmenge

$$\mathcal{B} = \{x_1, x_2, \ldots, x_d\} \subseteq S, \tag{2.5.8}$$

d.h. für alle $\lambda_1, \ldots, \lambda_d \in R$ gilt, dass

$$\sum_{i=1}^{d} \lambda_i x_i = 0 \Rightarrow \forall i : \lambda_i = 0 \tag{2.5.9}$$

und die Teilmenge $\mathcal{B} \subseteq S$ ist maximal mit dieser Eigenschaft. Wir setzen $N := \langle \mathcal{B} \rangle \leq M$. Dann ist die Abbildung

$$\begin{aligned} R^d &\to N \\ (\lambda_1, \lambda_2, \ldots, \lambda_d) &\mapsto \sum_{i=1}^{d} \lambda_i x_i \end{aligned} \tag{2.5.10}$$

ein Isomorphismus. Wegen der Maximalität von $\mathcal{B}$ existiert für jedes $s \in S \backslash \mathcal{B}$ ein $a_s \in R$, $a_s \neq 0$ mit $a_s \cdot s \in N$ $(*)$. Setze

$$a := \prod_{s \in S \backslash \mathcal{B}} a_s \in R \backslash \{0\} \, (**). \tag{2.5.11}$$

Da M torsionsfrei ist, ist die R-lineare Abbildung

$$\begin{aligned} \mu_a : M &\to M \\ x &\mapsto a \cdot x \end{aligned} \tag{2.5.12}$$

injektiv. Also ist

$$M \cong \mathrm{im}(\mu_a) \leq N \cong R^d, \tag{2.5.13}$$

und damit ist M frei. □

Übung. Zeige, dass der konstruierte Isomorphismus tatsächlich ein solcher ist. Zeige, dass $(*)$ und $(**)$ gilt.

Lemma 2.5.4. Torsionszerlegung Sei M ein endlich erzeugter R-Modul mit Torsionsuntermodul $T \leq M$. Dann ist T endlich erzeugt, M/T ist ein freier R-Modul und es gibt einen Isomorphismus

$$M \cong T \oplus M/T. \tag{2.5.14}$$

Beweis. Wir zeigen zunächst, dass M/T torsionsfrei ist. Sei dazu $[x] \in M/T$ und sei $r \in R$, $r \neq 0$ mit $[r \cdot x] = 0$. Dann gilt $rx \in T$, es gibt also $s \in R$, $s \neq 0$ mit:

$$s(rx) = 0 \Rightarrow \underbrace{(sr)}_{\neq 0} x = 0 \Rightarrow x \in T \Rightarrow [x] = 0. \tag{2.5.15}$$

Also ist der Quotient torsionsfrei. Da $M \twoheadrightarrow M/T$ und M endlich erzeugt ist, ist auch M/T endlich erzeugt. Mit Lemma 2.5.3 folgt, dass M/T frei ist. Also spaltet die KES

$$\{0\} \longrightarrow T \longrightarrow B \longrightarrow M/T \longrightarrow \{0\},$$

woraus $M \cong T \oplus M/T$ folgt. Damit existiert eine Abbildung $M \twoheadrightarrow T$, also ist T endlich erzeugt. □

Definition 2.5.5. Annihilator

Sei M ein R-Modul und $S \subseteq M$ eine nichtleere Teilmenge. Dann heißt das Ideal

$$\mathrm{Ann}_R(S) := \{r \in R | \forall s \in S : r \cdot s = 0\} \subseteq R \tag{2.5.16}$$

Annihilator oder **Annihilatorideal** von S. Für $S = \{x\}$ schreiben wir $\mathrm{Ann}_R(x)$.

Übung. Zeige, dass $\mathrm{Ann}_R(S)$ tatsächlich ein Ideal ist.

Satz 2.5.6. Torsionsprimfaktorzerlegung

Sei $\{0\} \neq M$ ein endlich erzeugter Torsionsmodul über R. Dann gelten:

(i) Für eine Nichteinheit $d \neq 0$ gilt $\mathrm{Ann}_R(M) = (d)$.

(ii) Sei $d = \epsilon p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ die Primfaktorzerlegung mit paarweise nicht-assoziierten Primelementen $p_i \nsim p_j$ für $i \neq j$ und $\epsilon \in R^\times$. Dann gilt

$$M \cong \bigoplus_{i=1}^{k} T_{p_i}(M). \tag{2.5.17}$$

Beweis.

(i) Sei $S = \{x_1, x_2, \ldots, x_n\} \subseteq M \backslash \{0\}$ eine erzeugende Teilmenge. da M ein Torsionsmodul ist, gibt es für jedes $1 \leq i \leq n$ ein $r_i \in R$, $r_i \neq 0$ mit $r_i \cdot x_i = 0$. Dann ist $0 \neq r_1 r_2 \cdots r_n \in \mathrm{Ann}_R(M)$. Da R ein Hauptidealring ist, folgt daraus $\mathrm{Ann}_R(M) = (d)$ mit $d \neq 0$. Außerdem ist $d \notin R^\times$, da andernfalls $M = \{0\}$ gelten würde.

(ii) Wir setzen $I := \{1, 2, \ldots, k\}$ und betrachten die Abbildung

$$\begin{aligned} \varphi : \bigoplus_{i \in I} T_{p_i}(M) &\to M \\ (x_i)_{i \in I} &\mapsto \sum_{i \in I} x_i. \end{aligned} \tag{2.5.18}$$

Mit $d_i := d/p_i^{n_i}$ gilt (da $[d_i]$ teilerfremd):

$$(d_1, d_2, \ldots, d_k) = (1) = R, \tag{2.5.19}$$

es gibt also Elemente r_i, $1 \leq i \leq k$, mit $\sum_i r_i d_i = 1$. Für beliebiges $x \in M$ gilt dann für alle $i \in I$: $x_i = r_i d_i x \in T_{p_i}(M)$ und $x = \sum_{i \in I} x_i$. Rest des Beweises nachtragen.

□

Beispiel. Für $d = \epsilon p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \in R$ wie in Satz 2.5.6 gilt der **Chinesische Restsatz (CRT)**:

$$R/(d) \cong R/(p_1^{n_1}) \oplus R/(p_2^{n_2}) \oplus \cdots \oplus R/(p_k^{n_k}) \tag{2.5.20}$$

mit

$$T_{p_i}\left(R/(d)\right) \cong R/(p_i^{n_i}). \tag{2.5.21}$$

Vorsicht: Dies ist kein direktes Korollar von Satz 2.5.6, sondern ein Spezialfall.

Theorem 2.5.7. Klassifikationssatz für endlich erzeugte Torsionsmodule

Sei $p \in R$ ein Primelement und T ein endlich erzeugter p-Torsionsmodul. Dann gibt es eindeutig bestimmte Zahlen $m \geq 0$, $0 < l_1 \leq l_2 \leq \cdots \leq l_m$, sodass

$$T \cong \bigoplus_{i=1}^{m} R/(p^{l_i}). \tag{2.5.22}$$

Beweis. Sei $T = \langle x_1, x_2, \ldots, x_m \rangle$, sodass m minimal ist. Zunächst wollen wir die Existenz des Isomorphismus zeigen. Für $m = 1$ folgt die Aussage direkt aus dem CRT, sei also $m > 1$. Für jedes $1 \leq i \leq m$ gilt: Wegen des CRT ist der Annihilator durch $\mathrm{Ann}_R(x_i) = (p^{n_i})$ mit $n_i > 0$ gegeben. Sei o.B.d.A. $\mathrm{Ann}_R(x_m) = (p^e)$, wobei e maximal unter den n_i ist (wäre das nicht für x_m der Fall, sortieren wir um). Dann gilt auch, dass $\mathrm{Ann}_R(T) = (p^e)$. Betrachte die KES

$$\{0\} \longrightarrow \underbrace{\langle x_m \rangle}_{\cong R/(p^e)} \hookrightarrow T \longrightarrow T/\langle x_m \rangle \longrightarrow \{0\}.$$

Die maximale Anzahl von Erzeugern von $T/\langle x_m \rangle =: \overline{T}$ ist $m-1$, da m minimal ist. Induktiv folgt, dass

$$\overline{T} \cong \bigoplus_{i=1}^{n-1} R/(p^{l_i}). \tag{2.5.23}$$

Jetzt brauchen wir ein Lemma. □

Lemma 2.5.8. Hochhebung des Annihilators Sei $\overline{T}$ wie oben. Für jedes $y \in \overline{T}$ mit $\mathrm{Ann}_R(y) = (p^f)$ existiert ein Element $\tilde{y} \in T$ mit $\mathrm{Ann}_R(\tilde{y}) = (p^f)$ und $\pi(\tilde{y}) = y$.

Beweis. Klar ist, dass $f \leq e$. Sei $z \in T$ mit $\pi(z) = y$ beliebig. Dann gilt $p^f z = r \cdot x_m$. Weiterhin gilt:

$$0 = p^e z = p^{e-f} p^f z = p^{e-f} r x_m. \tag{2.5.24}$$

Da $\mathrm{Ann}_R(x_m) = (p^e)$ gilt, muss auch $r = sp^f$ für $s \in R$ gelten. Wir setzen nun

$$\tilde{y} := z - s \cdot x_m. \tag{2.5.25}$$

Dann gilt $\pi(\tilde{y}) = y$, sodass $p^j \tilde{y} \neq 0$ für $j < f$. Außerdem ist

$$p^f \tilde{y} = p^f z - p^f s x_m = r x_m - r x_m = 0, \tag{2.5.26}$$

was zu zeigen war. Also ist $\tilde{y}$ die gesuchte Hochhebung. □

Jetzt machen wir weiter im Beweis von Theorem 2.5.7:

Beweis. Betrachte den Isomorphismus

$$\begin{aligned} \bigoplus_{i=1}^{n-1} R/(p^{l_i}) &\to \overline{T} \\ (0,\dots,0,\underbrace{1}_{j\text{-ter Eintrag}},0,\dots,0) &\mapsto y_j \end{aligned} \tag{2.5.27}$$

mit der Projektion $\pi : T \twoheadrightarrow \overline{T}$. Jedes Element $z \in \overline{T}$ löasst sich auf eindeutige Weise schreiben als

$$z = \sum_{i=1}^{n-1} r_i y_j. \tag{2.5.28}$$

Wir definieren

$$\begin{aligned} s : \overline{T} &\to T \\ \sum_{k=1}^{n-1} r_i y_i &\mapsto \sum_{i=1}^{n-1} r_i \tilde{y}_i \end{aligned} \tag{2.5.29}$$

mit $\pi(\tilde{y}) = y$. Dies ist eine wohldefinierte, R-lineare Abbildung, da $\mathrm{Ann}_R(y_i) = \mathrm{Ann}_R(\tilde{y}_i)$. Damit zerfällt die KES, woraus die Existenz des Isomorphismus 2.5.22 folgt.
Jetzt zeigen wir die Eindeutigkeit. Die Zahl m ist eindeutig bestimmt als minimale Erzeugerzahl von T. Alternativ gilt:

$$m = \dim_{R/(p)} T/pT, \tag{2.5.30}$$

da $R/(p)$ ein Körper ist. Analog können wir die Anzahl von Exponenten e_i, die größer als 1 sind, beschreiben als

$$\dim_{R/(p)} pT/p^2T. \tag{2.5.31}$$

Weiter ist also die Anzahl von Exponenten $e_i > e^j$ allgemein gegeben durch

$$\dim_{R/(p)} p^jT/p^{j+1}T. \tag{2.5.32}$$

Damit ist auch die Eindeutigkeit gezeigt. □

Übung. Zeige die Aussage für $m = 1$ mit dem CRT. Zeige die letzte Gleichheit von Annihilatoren.

Korollar 2.5.9 (Klassifikation endlich erzeugter Moduln)**.** Sei M ein endlich erzeugter R-Modul. Dann gibt es eindeutig bestimmte $r, m \in \mathbb{N}$ und Primelementpotenzen $p_1^{e_1}, \dots, p_m^{e_m}$ (wobei nicht notwendigerweise $p_i \nsim p_j$ für $i \neq j$ gilt) mit

$$M \cong R^r \oplus R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_m^{e_m}). \tag{2.5.33}$$

Korollar 2.5.10 (Hauptsatz von endlich erzeugten, abelschen Gruppen)**.** Jede endlich erzeugte, abelsche Gruppe A besitzt eine eindeutige, direkte Summenzerlegung der Form

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/(p_1^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p_m^{e_m}). \tag{2.5.34}$$

Beispiel. Jordansche Normalform

Sei $\mathbb{K}$ ein algebraisch abgeschlossener Körper und $\mathbb{K}[x]$ der Polynomring über $\mathbb{K}$. Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum und $\varphi : V \to V$ ein Endomorphismus. Wir betrachten V als $\mathbb{K}[x]$-Modul, wobei wir für $f(x) \in \mathbb{K}[x]$ und $v \in V$ eine Skalarmultiplikation durch

$$f(x) \cdot v = f(\varphi)(v) = (a_n\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0\mathrm{id})(v). \tag{2.5.35}$$

Damit ist V ein endlich erzeugter $\mathbb{K}[x]$-Modul, der vollständig nicht-torsionsfrei ist. Also folgt:

$$V \cong \bigoplus_{i=1}^{m} \mathbb{K}[x]/(x - a_i)^{e_i} \tag{2.5.36}$$

als $\mathbb{K}[x]$-Moduln. Wir müssen noch verstehen, wie φ auf einem der Blöcke $\mathbb{K}[x]/(x - a_j)^{e_j}$ wirkt. Betrachte dazu einen $\mathbb{K}[x]$-Modul der Form $\mathbb{K}[x]/(x - a)^x$. Wähle die Basis $\mathcal{B} = \big((x - a)^{e-1}, (x - a)^{e-2}, \ldots, x - a, 1\big)$, dann hat die darstellende Matrix von φ Blockdiagonalgestalt:

$$\begin{pmatrix} a & 1 & 0 & 0 & \cdots & 0 \\ 0 & a & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a \end{pmatrix} \tag{2.5.37}$$

3 Galoistheorie

3.1 Galoisgruppen

Definition 3.1.1. Galoisgruppe

Sei $f(x) \in \mathbb{Q}[x]$ ein Polynom mit rationalen Koeffizienten von Grad $\deg f = n \geq 1$ und seien $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ die komplexen Nullstellen (mit Vielfachheiten) von $f(x)$. Die **Galoisgruppe**

$$\mathrm{Gal}(f) \leq \mathfrak{S}_n \tag{3.1.1}$$

von f über $\mathbb{Q}$ ist die Untergruppe der Permutationen $\sigma \in \mathfrak{S}_n$, die die folgende Bedingung erfüllen:
Für jedes $r(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ mit $r(\lambda_1, \ldots, \lambda_n) = 0$ gilt auch

$$r(\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(n)}) = 0. \tag{3.1.2}$$

Anders ausgedrückt ist $\mathrm{Gal}(f)$ also die Untergruppe derjenigen Permutationen, die alle algebraischen Relationen über $\mathbb{Q}$ der Nullstellen von $f(x)$ erhalten.

Beispiel. Betrache $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ mit Nullstellen $a = \sqrt[4]{2}$, $b = i\sqrt[4]{2}$, $c = -\sqrt[4]{2}$ und $c = -i\sqrt[4]{2}$. Aus $x^4 - 2 = (x-a)(x-b)(x-c)(x-d)$ folgen die Relationen:

$$\begin{aligned} abcd &= -2 \\ abc + abd + acd + bcd &= 0 \\ ab + ac + ad + bc + bd + cd &= 0 \\ a + b + c + d &= 0. \end{aligned} \tag{3.1.3}$$

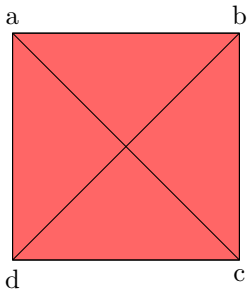
Zusätzlich gilt

$$\begin{aligned} a^2b^2 &= -2 \\ b^2c^2 &= -2 \\ c^2d^2 &= -2 \\ d^2a^2 &= -2. \end{aligned} \tag{3.1.4}$$

sowie

$$\begin{aligned} a^2c^2 &= 2 \\ b^2d^2 &= 2. \end{aligned} \tag{3.1.5}$$

Also definiert $\{a, b, c, d\}$ die Eckpunkte eines Quadrats:



wobei die ersten vier Gleichungen die Kanten und die letzten zwei Gleichungen die Diagonalen repräsentieren. Die Relationen können also nur von Permutationen der Diedergruppe erhalten werden, sodass

$$\mathrm{Gal}(f) \leq D_4 = \langle (1234), (12)(34) \rangle \leq \mathfrak{S}_4 \tag{3.1.6}$$

gelten muss. Unklar ist (noch), ob tatsächlich $\mathrm{Gal}(f) = D_4$ gilt.

3.2 Körpererweiterungen

Definition 3.2.1. Unterkörper und Körpererweiterung

Sei $\mathbb{L}$ ein Körper. Ein **Unterkörper** $\mathbb{K} \subseteq \mathbb{L}$ ist eine Teilmenge, die beide neutralen Elemente von $(\mathbb{L}, +, \cdot)$ enthält und mit den auf $\mathbb{K}$ eingeschränkten Verknüpfungen wieder einen Körper bildet.
Anders herum nennen wir bei gegebenem $\mathbb{K}$ den Körper $\mathbb{L}$ **Körpererweiterung** von $\mathbb{K}$ und schreiben $\mathbb{L} \mid \mathbb{K}$.

Definition 3.2.2. Grad der Körpererweiterung

Seien $\mathbb{L}$ und $\mathbb{K}$ Körper mit $\mathbb{L} \mid \mathbb{K}$. Dann können wir $\mathbb{L}$ als $\mathbb{K}$-Vektorraum auffassen und bezeichnen mit

$$[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}} \mathbb{L} \tag{3.2.1}$$

den **Grad** von $\mathbb{L} \mid \mathbb{K}$. Darüber hinaus nennen wir $\mathbb{L} \mid \mathbb{K}$ **endlich**, falls $[\mathbb{L} : \mathbb{K}]$ endlich ist.

Lemma 3.2.3. Faktorisierung des Grades Seien $\mathbb{M} \mid \mathbb{L}$ und $\mathbb{L} \mid \mathbb{K}$ Körpererweiterungen. Dann ist $\mathbb{M} \mid \mathbb{K}$ genau dann endlich, wenn $\mathbb{M} \mid \mathbb{L}$ und $\mathbb{L} \mid \mathbb{K}$ endlich sind. Insbesondere gilt dann:

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]. \tag{3.2.2}$$

Beweis. Betrachte Teilmengen $P := \{m_1, \dots, m_r\} \subseteq \mathbb{M}$ und $Q := \{l_1, \dots, l_s\} \subseteq \mathbb{L}$ sowie

$$QP := \{l_i m_j \mid 1 \leq i \leq s, 1 \leq j \leq r\}. \tag{3.2.3}$$

Die Aussage folgt direkt aus den beiden Erkenntnissen:

1. Sei P linear unabhängig über $\mathbb{L}$ und Q über $\mathbb{K}$, dann ist QP linear unabhängig über $\mathbb{K}$.
2. Sei P erzeugend über $\mathbb{L}$ und Q über $\mathbb{K}$, dann ist QP erzeugend über $\mathbb{K}$.

Diese Behauptungen folgen direkt aus der Umformung

$$\sum_{i,j} \lambda_{ij} l_i m_j = \sum_j \left(\sum_i \lambda_{ij} l_i \right) m_j. \tag{3.2.4}$$

□

Beispiele.

1. $\mathbb{C} \mid \mathbb{R}$ ist eine Körpererweiterung von Grad 2.
2. $\mathbb{R} \mid \mathbb{Q}$ ist eine Körpererweiterung unendlichen Grades. Betrachte dazu z.B. die linear unabhängige Teilmenge $\{1, \pi, \pi^2, \dots\} \subseteq \mathbb{R}$ über $\mathbb{Q}$.
3. Sei $\mathbb{K}$ ein Körper und $\mathbb{K}(x) = (\mathbb{K}[x] \backslash \{0\})^{-1}\mathbb{K}[x]$ der zugehörige Quotientenkörper. Letzterer wird in diesem Fall als **Körper der rationalen Funktionen** bezeichnet. Dann ist $\mathbb{K}(x) \mid \mathbb{K}$ eine Körpererweiterung mit $[\mathbb{K}(x) : \mathbb{K}] = \infty$. Betrachte dafür z.B. die über $\mathbb{K}$ linear unabhängige Teilmenge $\{1, x, x^2, \dots\}$.
4. Sei $f(x) \in \mathbb{Q}[x]$ ein Polynom von Grad $n \geq 1$ mit Nullstellen $\lambda_1, \dots, \lambda_n \in \mathbb{C}$. Sei $\mathbb{Q}(f)$ das Bild des Ringhomomorphismus

$$\begin{aligned} \phi : \mathbb{Q}[x_1, \dots, x_n] &\to \mathbb{C} \\ f(x_1, \dots, x_n) &\mapsto f(\lambda_1, \dots, \lambda_n). \end{aligned} \tag{3.2.5}$$

   Dann ist $\mathbb{Q}(f) \mid \mathbb{Q}$ eine endliche Körpererweiterung von Grad $\leq n^n$.

Übung. Zeige die Behauptung in Beispiel 4. Zeige insbesondere, dass $\mathbb{Q}(f)$ ein Körper ist.

3.3 Körperautomorphismen

Definition 3.3.1. Körperautomorphismus

Sei $\mathbb{L}$ ein Körper. Ein bijektiver Ringhomomorphismus $\sigma : \mathbb{L} \to \mathbb{L}$ heißt **Körperautomorphismus** von $\mathbb{L}$. Die Menge der Körperautomorphismen von $\mathbb{L}$ wird mit $\mathrm{Aut}(\mathbb{L})$ bezeichnet.

Definition 3.3.2. Galoisgruppe der Körpererweiterung

Sei $\mathbb{L} \mid \mathbb{K}$ eine Körpererweiterung. Dann ist die **Galoisgruppe von $\mathbb{L}$ über $\mathbb{K}$** definiert als

$$\mathrm{Gal}(\mathbb{L} \mid \mathbb{K}) := \{\sigma \in \mathrm{Aut}(\mathbb{L}) \mid \forall x \in \mathbb{K} : \sigma(x) = x\} \leq \mathrm{Aut}(\mathbb{L}). \tag{3.3.1}$$

Satz 3.3.3. Kardinalität der Galoisgruppe ist beschränkt

Sei $\mathbb{L} \mid \mathbb{K}$ eine Körpererweiterung. Dann gilt

$$|\mathrm{Gal}(\mathbb{L} \mid \mathbb{K})| \leq [\mathbb{L} : \mathbb{K}]. \tag{3.3.2}$$

Lemma 3.3.4. Dedekind-Lemma Seien $\mathbb{L}$ und $\mathbb{E}$ Körper, $\sigma_i : \mathbb{L} \to \mathbb{E}$ paarweise verschiedene Ringhomomorphismen mit $1 \leq i \leq n$ und $\lambda_i \in \mathbb{E}$ mit

$$\sum_{i=1}^{n} \lambda_i \sigma_i = 0 \in \mathrm{Abb}(\mathbb{L}, \mathbb{E}). \tag{3.3.3}$$

Diese Gleichung ist im $\mathbb{E}$-Vektorraum $\mathrm{Abb}(\mathbb{L}, \mathbb{E})$ aufzufassen. Dann gilt für alle $1 \leq i \leq n$, dass $\lambda_i = 0$.

Beweis. Wir beweisen durch vollständige Induktion nach n. Für $n = 1$ folgt die Behauptung aus $0 = \lambda_1 \sigma_1 = \lambda_1$. Sei nun $n > 1$. Angenommen, es gäbe eine nichttriviale Linearkombination $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$. O.B.d.A. sei $\lambda_1 \neq 0$. Wähle

$a \in \mathbb{L}$ mit $\sigma_1(a) \neq \sigma_n(a)$. Dann gilt für alle $x \in \mathbb{L}$:

$$0 = \sum_{i=1}^{n} \lambda_i \sigma_i(ax) - \sigma_n(a) \sum_{i=1}^{n} \lambda_i \sigma_i(x) = \sum_{i=1}^{n-1} \lambda_i (\sigma_i(a) - \sigma_n(a)) \sigma_i(x). \tag{3.3.4}$$

Dies ist aber eine kürzere Linearkombination der $\sigma_1, \ldots, \sigma_{n-1}$ zu 0, welche nicht-trivial ist, da $\lambda_1(\sigma_1(a) - \sigma_n(a)) \neq 0$ nach Konstruktion. Dies ist ein Widerspruch. □

Satz 3.3.5. Ringhomomorphismen beschränken Erweiterungsgrad

Seien $\mathbb{L} \mid \mathbb{K}$ und $\mathbb{E} \mid \mathbb{K}$ Körpererweiterungen. seien weiterhin $\sigma_1, \sigma_2, \ldots, \sigma_n$ paarweise verschiedene Ringhomomorphismen $\sigma_i : \mathbb{L} \to \mathbb{E}$ mit $\sigma_i|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$. Dann gilt:

$$n \leq [\mathbb{L} : \mathbb{K}]. \tag{3.3.5}$$

Beweis. Falls $[\mathbb{L} : \mathbb{K}] = \infty$ gilt, ist die Aussage trivial. Sei also $[\mathbb{L} : \mathbb{K}] = m < \infty$ und sei $(e_1, e_2, \ldots, e_m)$ eine $\mathbb{K}$-Basis von $\mathbb{L}$. Das LGS

$$\mathbb{E}^{m \times n} \ni \begin{pmatrix} \sigma_1(l_1) & \cdots & \sigma_n(l_1) \\ \sigma_1(l_2) & \cdots & \sigma_n(l_2) \\ \vdots & \vdots & \vdots \\ \sigma_1(l_m) & \cdots & \sigma_n(l_m) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{3.3.6}$$

Falls $n > m$ gilt, existiert eine nicht-triviale Lösung $(\lambda_1, \ldots, \lambda_n) \in \mathbb{E}^n$, also

$$\sum_{i=1}^{n} \lambda_i \sigma_i = 0. \tag{3.3.7}$$

Dies ist ein Widerspruch zu Lemma 3.3.4. □

Korollar 3.3.6 (Aus Satz 3.3.5)**.** Satz 3.3.3 folgt direkt.

3.4 Galoiserweiterungen

Definition 3.4.1. Galoiserweiterung

Eine endliche Körpererweiterung $\mathbb{L} \mid \mathbb{K}$ heißt **Galoiserweiterung**, falls

$$|\operatorname{Gal}(\mathbb{L} \mid \mathbb{K})| = [\mathbb{L} : \mathbb{K}]. \tag{3.4.1}$$

Definition 3.4.2. Fixkörper

Sei $\mathbb{L}$ ein Körper und $G \leq \operatorname{Aut}(\mathbb{L})$. Der Unterkörper

$$\mathbb{L}^G := \{x \in \mathbb{L} | \forall \sigma \in G : \sigma(x) = x\} \subseteq \mathbb{L} \tag{3.4.2}$$

heißt **Fixkörper** von G.

Übung. Zeige, dass $\mathbb{L}^G$ tatsächlich ein Unterkörper ist.

Satz 3.4.3. Fixkörper ist Grundkörper

Sei $\mathbb{L} \mid \mathbb{K}$ eine Galoiserweiterung mit $G = \operatorname{Gal}(\mathbb{L} \mid \mathbb{K})$. Dann gilt $\mathbb{L}^G = \mathbb{K}$.

Beweis. Direkt aus den Definitionen folgt, dass $\operatorname{Gal}(\mathbb{L} \mid \mathbb{K}) = \operatorname{Gal}(\mathbb{L} \mid \mathbb{L}^G)$. Weiterhin gilt $\mathbb{K} \subseteq \mathbb{L}^G \subseteq \mathbb{L}$. Da $\mathbb{L} \mid \mathbb{K}$ galoissch ist, gilt $|G| = [\mathbb{L} : \mathbb{K}]$. Aus Satz 3.3.3 folgt, dass

$$[\mathbb{L} : \mathbb{K}] = |G| = |\operatorname{Gal}(\mathbb{L} \mid \mathbb{L}^G)| \leq [\mathbb{L} : \mathbb{L}^G] \tag{3.4.3}$$

gilt, also

$$[\mathbb{L} : \mathbb{L}^G] = [\mathbb{L} : \mathbb{K}] \Rightarrow [\mathbb{L}^G : K] = 1 \Rightarrow \mathbb{L}^G = \mathbb{K}. \tag{3.4.4}$$

□

Übung. Begründe, warum die letzte Implikation gelten muss.

Satz 3.4.4. Satz von Artin

Sei $\mathbb{L}$ ein Körper und $G \leq \operatorname{Aut}(\mathbb{L})$. Dann gilt

$$[\mathbb{L} : \mathbb{L}^G] = |G|. \tag{3.4.5}$$

Falls G endlich ist, ist damit insbesondere die Körpererweiterung $\mathbb{L} \mid \mathbb{L}^G$ galoissch mit Galoisgruppe G.

Beweis. Sei $\mathbb{K} := \mathbb{L}^G$. Wegen $G \leq \operatorname{Gal}(\mathbb{L} \mid \mathbb{K})$ gilt

$$|G| \leq |\operatorname{Gal}(\mathbb{L} : \mathbb{K})| \leq [\mathbb{L} : \mathbb{K}]. \tag{3.4.6}$$

Wir zeigen nun $[\mathbb{L} : \mathbb{K}] \leq |G|$. Ist $|G| = \infty$, ist die Aussage trivial, also sei $|G| = n < \infty$. Wir zeigen, dass je $n + 1$

Elemente $x_1, x_2, \ldots, x_{n+1} \in \mathbb{L}$ linear abhängig über $\mathbb{K}$ sind. Betrachte dazu für $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ das $\mathbb{L}$-lineare Gleichungssystem

$$\sum_{j=1}^{n+1} y_j \sigma_i(x_j) = 0 \tag{3.4.7}$$

für $1 \leq i \leq n$. Dieses LGS hat $n+1$ Variablen und n Gleichungen, also existiert eine nicht-triviale Lösung $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1}) \in \mathbb{L}^{n+1}$. Sei o.B.d.A. $\lambda_1 \neq 0$. Für $1 \leq i \leq n$ wenden wir σ_i^{-1} auf die i-te Gleichung an und erhalten

$$\sum_{j=1}^{n+1} \sigma_i^{-1}(\lambda_j) \cdot x_j = 0 \tag{3.4.8}$$

für $1 \leq i \leq n$. Summiere über alle Gleichungen:

$$\sum_{j=1}^{n+1} \underbrace{\alpha_j}_{\in \mathbb{K}} x_j = 0 \tag{3.4.9}$$

mit

$$\alpha_j = \sum_{i=1}^{n} \sigma_i^{-1}(\lambda_j) = \sum_{\sigma \in G} \sigma(\lambda_j) \in \mathbb{L}^G, \tag{3.4.10}$$

da für die Gruppe G Inversenbildung $g \mapsto g^{-1}$ eine Bijektion ist und die Summe invariant unter Wirkung von G ist. Es bleibt noch, zu zeigen, dass die Koeffizienten α nicht-trivial sind. Wegen des Dedekind-Lemmae gilt $\sum_{\sigma \in G} \sigma \neq 0$, es gibt also $l \in \mathbb{L}$ mit $\sum_{\sigma \in G} \sigma(l) \neq 0$. Ersetze den Lösungsvektor $(\lambda_1, \lambda_2, \ldots, \lambda_{n+1})$ durch die Reskalierung $l \cdot \lambda_1^{-1} \in \mathbb{L}$, also:

$$\left((l\lambda_1^{-1})\lambda_1, (l\lambda_1^{-1})\lambda_2, \ldots, (l\lambda_1^{-1})\lambda_{n+1}\right) \in \mathbb{L}^{n+1}. \tag{3.4.11}$$

Daraus folgt, dass

$$\alpha_1 = \sum_{\sigma \in G} \sigma(l) \neq 0, \tag{3.4.12}$$

also liegt eine nicht-triviale $\mathbb{K}$-Linearkombination vor. □

Korollar 3.4.5 (Aus Satz 3.4.4)**.** Sei $\mathbb{L} \mid \mathbb{K}$ eine endliche Körpererweiterung. Dann gilt:

$$|\operatorname{Gal}(\mathbb{L} \mid \mathbb{K})| \mid [\mathbb{L} : \mathbb{K}] \tag{3.4.13}$$

Beweis. Aus dem Satz von Artin folgt, dass

$$|\operatorname{Gal}(\mathbb{L} \mid \mathbb{K})| = |\operatorname{Gal}(\mathbb{L} \mid \mathbb{L}^G)| = [\mathbb{L} : \mathbb{L}^G] \mid [\mathbb{L} : \mathbb{K}] \tag{3.4.14}$$

□

3.5 Galoiskorrespondenz

Sei $\mathbb{L} \mid \mathbb{K}$ eine Körpererweiterung mit Galoisgruppe $\operatorname{Gal}(\mathbb{L} \mid \mathbb{K}) =: G$. Betrachte die Mengen

$$\mathcal{U}(G) = \{H | H \leq G\} \tag{3.5.1}$$

der Untergruppen von G und

$$\mathcal{Z}(\mathbb{L} \mid \mathbb{K}) := \{\mathbb{M} | \mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}\}. \tag{3.5.2}$$

der Zwischenkörper von $\mathbb{K}$ und $\mathbb{L}$. Die Körper $\mathbb{K}$ und $\mathbb{M}$ heißen Unterkörper, $\mathbb{M}$ heißt Zwischenkörper von $\mathbb{K}$ und $\mathbb{L}$.

Theorem 3.5.1. Galoiskorrespondenz

Sei $\mathbb{L} \mid \mathbb{K}$ eine Galoiserweiterung mit Galoisgruppe $Gal(\mathbb{L} \mid \mathbb{K})$. Dann sind die Abbildungen

$$\begin{aligned} \mathcal{U}(G) &\to \mathcal{Z}(\mathbb{L} \mid \mathbb{K}) \\ H &\mapsto L^H \end{aligned} \tag{3.5.3}$$

und

$$\begin{aligned} \mathcal{Z}(\mathbb{L} \mid \mathbb{K}) &\to \mathcal{U}(G) \\ M &\mapsto \operatorname{Gal}(\mathbb{L} \mid \mathbb{M}) \end{aligned} \tag{3.5.4}$$

zueinander inverse Bijektionen.

Beispiel. Sei $\mathbb{L} \mid \mathbb{K}$ eine Galoiserweiterung mit $\operatorname{Gal}(\mathbb{L} \mid \mathbb{K}) \cong \mathfrak{S}_3$. Diese Gruppe verstehen wir bereits: (Diagramm einfügen)

Beweis. $g \circ f = \mathrm{id}$ ist klar, da

$$H = \operatorname{Gal}(\mathbb{L} \mid \mathbb{L}^H) \tag{3.5.5}$$

nach dem Satz von Artin. □