Skript zur Vorlesung Algebra

Wintersemester 2018/19

Catherine Meusburger
Department Mathematik
Friedrich-Alexander-Universität Erlangen-Nürnberg

(Date: 10. März 2021)

Dieses Skript basiert auf dem Skript von Dr. Guido Pezzini (WS 12/13), Prof. Dr. Friedrich Knop (WS 13/14, WS 14/15), Dr. Yasmine B. Sanderson (WS 15/16, WS 16/17), Prof. Dr. Jan Frahm (WS 17/18) und auf den folgenden Lehrbüchern, die ich auch den Studierenden empfehle:

- C. Karpfinger, K. Meyberg, Algebra: Gruppen-Ringe-Körper, Springer Spektrum
- G. Fischer, Lehrbuch der Algebra, Springer Spektrum

Ich bedanke mich bei den Hörerinnen und Hörern der Vorlesung und bei Prof. Dr. Andreas Knauf für Fragen und Hinweise, die mir geholfen haben, das Skript zu verbessern und Tippfehler zu eliminieren. Mein besonderer Dank gilt den Assistenten, Alexander Spies und Thomas Voß, sowie den studentischen Tutorinnen und Tutoren, Benedikt Fritz, Anna-Katharina Hirmer, Hans-Anselm Liegener, Michael Stocker, für ihre Kompetenz und ihren unermüdlichen Einsatz.

Bitte schicken Sie Kommentare und Bemerkungen zu diesem Skript an:

`catherine.meusburger@math.uni-erlangen.de`.

Inhaltsverzeichnis

Inhaltsverzeichnis **3**

1 Gruppentheorie **5**

1.1 Gruppen und Gruppenhomomorphismen 5

1.2 Untergruppen 12

1.3 Faktorgruppen 21

1.3.1 Nebenklassen 21

1.3.2 Normalteiler und Faktorgruppen 25

1.4 Semidirekte Produkte 33

1.5 Gruppenoperationen 38

1.6 Die symmetrischen Gruppen 45

1.7 Endlich erzeugte abelsche Gruppen 53

1.7.1 Zyklische Gruppen 53

1.7.2 Klassifikation der endlich erzeugten abelschen Gruppen 55

1.8 Auflösbare Gruppen 64

1.9 Die Sylowschen Sätze 68

2 Ringtheorie **73**

2.1 Ringe und Ringhomomorphismen 73

2.2 Unterringe 80

2.3 Ideale und Faktorringe 82

2.4 Konstruktion von Körpern 87

2.4.1 Faktorringe maximaler Ideale 88

2.4.2 Integritätsbereiche und Quotientenkörper 90
2.5 Teilbarkeit in Integritätsbereichen 95
2.5.1 Faktorielle Ringe 98
2.5.2 Hauptidealringe 101
2.5.3 Euklidische Ringe 105
2.6 Irreduzibilitätskriterien 110

3 Elementare Zahlentheorie **117**
3.1 Die Eulersche Phi–Funktion 117
3.2 Primzahlen: Die Sätze von Euklid und Wilson 121
3.3 Die Gaußschen Zahlen 123
3.4 Das quadratische Reziprozitätsgesetz 128

A Anhang **141**
A.1 Die komplexen Zahlen 141
A.2 Wichtige Beispiele von kommutativen Ringen 147

Index **148**

Kapitel 1

Gruppentheorie

1.1 Gruppen und Gruppenhomomorphismen

Im ersten Kapitel dieser Vorlesung befassen wir uns mit Gruppen - eine der grundlegendsten Strukturen in der Mathematik. Viele andere mathematische Begriffe wie etwa Vektorräume, Ringe, Körper und Algebren enthalten in ihrer Definition den Begriff der Gruppe. Auch strukturerhaltende Abbildungen wie etwa die invertierbaren Endomorphismen eines Vektorraums bilden häufig Gruppen.

Eine weitere wichtige Anwendungen von Gruppen sind Symmetrien in der Geometrie - Abbildungen, die gewisse geometrische Gebilde wie Geraden, Würfel oder Sphären im Raum bewegen und so auf sich selbst abbilden. Die Gruppenaxiome entsprechen dabei den Eigenschaften solcher Bewegungen: Man kann Bewegungen hintereinander ausführen und erhält so wieder eine neue Bewegung (*Verkettung, Gruppenmultiplikation*). Man kann eine triviale Bewegung ausführen, also ein geometrisches Gebilde nicht bewegen (*neutrales Element*), und man kann eine Bewegung durch eine andere Bewegung rückgängig machen (*Inverse*).

Die Mathematik kennt neben konkreten, geometrischen Symmetrien aber auch abstraktere, weniger offensichtliche Symmetrien von mathematischen Strukturen wie etwa Differentialgleichungen. Solche Symmetrien sind eines der stärksten Werkzeuge zum Lösen mathematischer Probleme. Wir befassen uns aber zunächst nur mit der Struktur und den grundlegenden mathematischen Eigenschaften von Gruppen.

Definition 1.1.1: Eine **Gruppe** $(G, \star)$ ist eine Menge G zusammen mit einer Abbildung $\star\colon G \times G \to G : (g, h) \mapsto g \star h$, die **Verknüpfung** oder **Gruppenmultiplikation**, so dass die folgenden Bedingungen erfüllt sind:

(G1) **Assoziativität:** $g \star (h \star k) = (g \star h) \star k$ für alle $g, h, k \in G$.

(G2) **neutrales Element:** Es gibt ein Element $e \in G$ mit $e \star g = g \star e = g$ für alle $g \in G$. Ein solches Element e heißt **neutrales Element**.

(G3) **Inverse:** Zu jedem Element $g \in G$ gibt es ein Element $h \in G$ mit $h \star g = g \star h = e$ für ein neutrales Element e. Ein solches Element h heißt **Inverses** von g.

Gilt zusätzlich $g \star h = h \star g$ für alle $g, h \in G$ so nennt man die Gruppe $(G, \star)$ **abelsch**.

Ist G eine endliche Menge, so heißt $(G, \star)$ **endliche Gruppe**. Die Anzahl ihrer Elemente heißt dann **Ordnung** von $(G, \star)$ und wird mit $|G|$ bezeichnet.

Bemerkung 1.1.2.

1. Aus (G1) folgt induktiv, dass alle Produkte von Gruppenelementen, die durch Umklammern auseinander hervorgehen, gleich sind. Daher lässt man die Klammern häufig weg.

2. Aus (G2) folgt, dass jede Gruppe G mindestens ein Element besitzt, nämlich das neutrale.

3. Jede Gruppe $(G, \star)$ besitzt genau ein neutrales Element $e \in G$.
   Sind nämlich $e, e' \in G$ neutrale Elemente, so folgt mit (G2) $e = e \star e' = e'$.

4. Jedes Element $g \in G$ einer Gruppe $(G, \star)$ besitzt genau ein Inverses.
   Sind nämlich $h_1, h_2 \in G$ invers zu $g \in G$, so folgt

   $$h_1 \overset{(G2)}{=} h_1 \star e \overset{(G3)}{=} h_1 \star (g \star h_2) \overset{(G1)}{=} (h_1 \star g) \star h_2 \overset{(G3)}{=} e \star h_2 \overset{(G2)}{=} h_2.$$

   Das Inverse eines Elements $g \in G$ wird im Folgenden mit g^{-1} bezeichnet.

5. Es gilt die **Kürzungsregel**: $g \star h = g \star k \Rightarrow h = k$ und $h \star g = k \star g \Rightarrow h = k$.
   Denn aus $g \star h = g \star k$ folgt

   $$h \overset{(G2)}{=} e \star h \overset{(G3)}{=} (g^{-1} \star g) \star h \overset{(G1)}{=} g^{-1} \star (g \star h) = g^{-1} \star (g \star k) \overset{(G1)}{=} (g^{-1} \star g) \star k \overset{(G3)}{=} e \star k \overset{(G1)}{=} k,$$

   und aus $h \star g = k \star g$ folgt

   $$h \overset{(G2)}{=} h \star e \overset{(G3)}{=} h \star (g \star g^{-1}) \overset{(G1)}{=} (h \star g) \star g^{-1} = (k \star g) \star g^{-1} \overset{(G1)}{=} k \star (g \star g^{-1}) \overset{(G3)}{=} k \star e \overset{(G2)}{=} k.$$

6. **Auflösen von Gleichungen:** Die Gleichungen $g \star x = h$ und $y \star g = h$ haben für feste $g, h \in G$ eindeutige Lösungen, nämlich $x = g^{-1} \star h$ und $y = h \star g^{-1}$.

   $$h = g \star x \quad \overset{5.}{\Leftrightarrow} \quad g^{-1} \star h = g^{-1} \star (g \star x) \overset{(G1)}{=} (g^{-1} \star g) \star x \overset{(G3)}{=} e \star x \overset{(G2)}{=} x,$$
   $$h = y \star g \quad \overset{5.}{\Leftrightarrow} \quad h \star g^{-1} = (y \star g) \star g^{-1} \overset{(G1)}{=} y \star (g^{-1} \star g) \overset{(G3)}{=} y \star e \overset{(G2)}{=} y.$$

7. **Rechenregeln für Inverse**:
   Es gilt $e^{-1} = e$, $(g^{-1})^{-1} = g$ und $(g \star h)^{-1} = h^{-1} \star g^{-1}$ für alle $g, h \in G$.

   Denn per Definition ist $e \star e = e$, $g^{-1} \star g = g \star g^{-1} = e$, und für alle $g, h \in G$ gilt

   $$(h^{-1} \star g^{-1}) \star (g \star h) \overset{(G1)}{=} h^{-1} \star (g^{-1} \star g) \star h \overset{(G2)}{=} h^{-1} \star e \star h \overset{(G2)}{=} h^{-1} \star h \overset{(G3)}{=} e$$
   $$(g \star h) \star (h^{-1} \star g^{-1}) \overset{(G1)}{=} g \star (h \star h^{-1}) \star g^{-1} \overset{(G2)}{=} g \star e \star g^{-1} \overset{(G2)}{=} g \star g^{-1} \overset{(G3)}{=} e.$$

Bemerkung 1.1.3.

1. Oft schreibt man G statt $(G, \star)$. Die Verknüpfung $\star$ ist aber Teil der Definition. Zwei Gruppen $(G, \star)$ und $(G', \star')$ sind genau dann gleich, wenn $G = G'$ und $\star = \star'$ gilt.

2. Es gibt zwei übliche Notationen für die Verknüpfung einer Gruppe:

   (a) Die **multiplikative Notation**: Man schreibt $g * h$, $g \cdot h$ oder gh für $g \star h$, bezeichnet mit g^{-1} das Inverse eines Elements $g \in G$ und mit e, e_G oder 1 das neutrale Element, das auch das **Einselement** oder die **Eins** genannt wird.

   Für $n \in \mathbb{N}$ schreibt man $g^n = g \cdot g \cdot \ldots \cdot g$ für das $n$fache Produkt eines Elements $g \in G$ mit sich selbst sowie $g^{-n} = (g^n)^{-1}$ und $g^0 = e$.

   (b) Die **additive Notation** wird nur für *abelsche Gruppen* verwendet:
   Anstatt $g \star h$ schreibt man $g + h$, sowie $-g$ für das Inverse von $g \in G$ und 0 für das neutrale Element, das auch als das **Nullelement** oder die **Null** bezeichnet wird.

   Für $n \in \mathbb{N}$ schreibt man $ng = g + g + \ldots + g$ für das n fache Produkt von $g \in G$ mit sich selbst sowie $(-n)g = -(ng)$ und $0g = 0$.

Da die meisten der im Folgenden betrachteten Gruppen nicht abelsch sind, benutzen wir vorwiegend multiplikative Notation. Wenn es keine Verwechslungsmöglichkeit gibt, werden wir in den folgenden Kapiteln die Verknüpfung häufig nicht explizit erwähnen und auch das Zeichen für die Verknüpfung in Formeln auslassen.

Beispiel 1.1.4.

1. Jede einelementige Menge $M = \{m\}$ ist eine Gruppe mit $\star : M \times M \to M$, $(m, m) \mapsto m$. Eine solche einelementige Gruppe wird als **triviale Gruppe** bezeichnet.

2. Bis auf Umbenennen der Elemente gibt es genau eine Gruppe der Ordnung zwei, die oft mit C_2 bezeichnet wird.

   Denn eine zweielementige Gruppe muss ein neutrales Element e und ein weiteres Element $g \neq e$ enthalten. Damit gilt $g \star g = g$ oder $g \star g = e$, aber aus $g \star g = g$ würde mit der Kürzungsregel $g = e$ folgen. Also muss $g \star g = e$ gelten.

3. Die ganzen Zahlen bilden mit der Addition eine abelsche Gruppe $(\mathbb{Z}, +)$.

4. Für jeden Körper $(\mathbb{K}, +, \cdot)$ sind $(\mathbb{K}, +)$ und $(\mathbb{K}^\times, \cdot)$ abelsche Gruppen.
   Insbesondere gilt dies für den Körper $\mathbb{R}$ der reellen Zahlen, den Körper $\mathbb{Q}$ der rationalen Zahlen und den Körper $\mathbb{C}$ der komplexen Zahlen.

5. Für jeden Vektorraum $(V, +, \cdot)$ über einem Körper $\mathbb{K}$ ist $(V, +)$ eine abelsche Gruppe. Insbesondere gilt dies für die folgenden Vektorräume:
   - die Vektorräume $\mathbb{K}^n$ für $n \in \mathbb{N}$.
   - die Vektorräume $\mathrm{Mat}(n \times m, \mathbb{K})$ der $n \times m$-Matrizen mit Einträgen in $\mathbb{K}$
   - die Vektorräume $\mathrm{Hom}_{\mathbb{K}}(V, W)$ der $\mathbb{K}$-linearen Abbildungen $\varphi : V \to W$

6. Für jeden $\mathbb{K}$-Vektorraum V bilden die bijektiven $\mathbb{K}$-linearen Abbildungen $\varphi : V \to V$ mit der Verkettung eine Gruppe $(\mathrm{GL}_{\mathbb{K}}(V), \circ)$. Falls $\dim_{\mathbb{K}}(V) \geq 2$, ist sie nicht abelsch.

7. Für alle $n \in \mathbb{N}$ und Körper $\mathbb{K}$ bilden die invertierbaren $n \times n$-Matrizen mit Einträgen in $\mathbb{K}$ und der Matrizenmultiplikation eine Gruppe $\mathrm{GL}(n, \mathbb{K})$. Diese ist für $n \geq 2$ nicht abelsch.

8. Für jede Menge M bilden die invertierbaren Abbildungen $f : M \to M$ mit der Verkettung von Abbildungen eine Gruppe $(S_M, \circ)$, die Gruppe der **Permutationen** von M. Falls M mindestens drei Elemente besitzt, ist diese nicht abelsch.

   Für $M = \{1, ..., n\}$ bezeichnet man die Permutationsgruppe auch mit S_n und nennt sie die **symmetrische Gruppe** der Ordnung n. Eine Permutation $\sigma \in S_n$ gibt man entweder in Tupelschreibweise an als $\sigma = [\sigma(1), \sigma(2), ..., \sigma(n)]$ oder in Tabellenschreibweise als:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

9. Für zwei Gruppen $(G, \star_G)$ und $(H, \star_H)$ wird auch die Menge $G \times H$ zu einer Gruppe mit der komponentenweisen Gruppenmultiplikation

$$\star : (G \times H) \times (G \times H) \to G \times H, \qquad (g_1, h_1) \star (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2).$$

   Das neutrale Element ist $e = (e_G, e_H)$ und die Inversen sind $(g, h)^{-1} = (g^{-1}, h^{-1})$ (Übung). Sie heißt das **(äußere) direkte Produkt** von G und H.

Bemerkung 1.1.5. Eine endliche Gruppe $(G, \star)$ kann durch eine **Multiplikationstafel** beschrieben werden. Für eine n-elementige Gruppe $G = \{g_1, ..., g_n\}$ ist dies eine Tabelle mit n Zeilen und n Spalten, wo in die $i$te Zeile und $j$te Spalte das Produkt $g_i \star g_j$ eingetragen wird. Dabei wählt man häufig $g_1 = e$.

$\star$	e	g_2	g_3	$\dots$	g_n
e	e	g_2	g_3	$\dots$	g_n
g_2	g_2	$g_2 \star g_2$	$g_2 \star g_3$	$\dots$	$g_2 \star g_n$
g_3	g_3	$g_3 \star g_2$	$g_3 \star g_3$	$\dots$	$g_3 \star g_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
g_n	g_n	$g_n \star g_2$	$g_n \star g_3$	$\dots$	$g_n \star g_n$

Man erkennt an der Multiplikationstafel leicht, ob eine Gruppe abelsch ist (wie?), und für kleine Gruppenordnungen kann man damit Gruppen relativ effizient untersuchen. Bis auf Umbenennung der Elemente sind beispielsweise die Gruppen der Ordnung ≤ 4 gegeben durch

- Ordnung 1: $G = \{e\}$

$\star$	e
e	e

- Ordnung 2: $G = C_2 = \{e, g_2\}$

$\star$	e	g_2
e	e	g_2
g_2	g_2	e

- Ordnung 3: $G = \{e, g_2, g_3\}$

$\star$	e	g_2	g_3
e	e	g_2	g_3
g_2	g_2	g_3	e
g_3	g_3	e	g_2.

- Ordnung 4: $G = \{e, g_2, g_3, g_4\}$

$\star$	e	g_2	g_3	g_4
e	e	g_2	g_3	g_4
g_2	g_2	g_3	g_4	e
g_3	g_3	g_4	e	g_2
g_4	g_4	e	g_2	g_3.

oder

$\star$	e	g_2	g_3	g_4
e	e	g_2	g_3	g_4
g_2	g_2	e	g_4	g_3
g_3	g_3	g_4	e	g_2
g_4	g_4	g_3	g_2	e.

Diese beiden Gruppen unterscheiden sich dadurch, dass für die zweite Gruppe $g^2 = e$ für alle Gruppenelemente g gilt, während in der ersten nur $g^4 = e$ für alle Gruppenelemente g gilt. Die zweite Gruppe heißt die **Kleinsche Vierergruppe**. Anhand der Multiplikationstabelle erkennt man, dass sie das direkte Produkt $C_2 \times C_2$ der zweielementigen Gruppe $C_2 = (\{1, -1\}, \cdot)$ mit sich selbst ist. Dabei stehen die Elemente e, g_2, g_3, g_4 in der Multiplikationstabelle für $e = (1, 1)$, $g_2 = (-1, 1)$, $g_3 = (1, -1)$ und $g_4 = (-1, -1)$.

Für Gruppen mit mehr Elementen wird die Beschreibung mit Multiplikationstafeln jedoch sehr aufwändig und unübersichtlich. Man erkennt nur schwer, ob verschiedene Multiplikationstafeln die gleiche Gruppe beschreiben, also durch Umbenennen oder Umordnen der Elemente auseinander hervorgehen. Auch andere wichtige Eigenschaften von Gruppen sind in den Multiplikationstafeln dann kaum zu erkennen. Daher wählt man andere Methoden zur Untersuchung von Gruppen, die sich stärker an deren Struktur orientieren und weniger von der konkreten Benennung der Elemente abhängen.

Eine Umbenennung von Gruppenelementen kann man dabei als eine bijektive Abbildung zwischen zwei Gruppen auffassen. Da Gruppen Mengen mit einer zusätzlichen Struktur sind, nämlich die Verknüpfung, ist man dabei allerdings weniger an allgemeinen Abbildungen interessiert als an *strukturerhaltenden Abbildungen*, d. h. Abbildungen, die mit der Gruppenmultiplikation kompatibel sind. Kompatibilität bedeutet, dass man das gleiche Ergebnis erhält, wenn man zuerst zwei Elemente multipliziert und dann das resultierende Element auf ein anderes abbildet und wenn man die zwei Elemente zuerst abbildet und dann ihre Bilder multipliziert.

Definition 1.1.6: Seien $(G, \star_G)$ und $(H, \star_H)$ Gruppen. Eine Abbildung $f : G \to H$ heißt **Gruppenhomomorphismus** oder **Homomorphismus von Gruppen**, falls gilt

$$f(g_1 \star_G g_2) = f(g_1) \star_H f(g_2) \qquad \forall g_1, g_2 \in G.$$

• Ein bijektiver Gruppenhomomorphismus heißt **Gruppenisomorphismus**. Gibt es einen Gruppenisomorphismus $f : G \to H$, so nennt man G und H **isomorph** und schreibt $G \cong H$.

• Ein injektiver Gruppenhomomorphismus heißt auch **Monomorphismus** von Gruppen und ein surjektiver Gruppenhomomorphismus **Epimorphismus** von Gruppen.

• Im Fall $(G, \star_G) = (H, \star_H)$ nennt man f einen **Gruppenendomorphismus** und einen **Gruppenautomorphismus**, falls f bijektiv ist.

Beispiel 1.1.7.

1. Für beliebige Gruppen $(G, \star_G)$ und $(H, \star_H)$ gibt es immer mindestens einen Gruppenhomomorphismus $f : G \to H$, nämlich den **trivialen Gruppenhomomorphismus** $f : G \to H$, $g \mapsto e_H$.

2. Für jedes $g \in G$ ist die **Konjugationsabbildung** $C_g : G \to G$, $h \mapsto g \star h \star g^{-1}$ ein Gruppenautomorphismus. Diese Gruppenautomorphismen heißen auch **innere Automorphismen** von G.

   Denn es gilt für alle $a, b \in G$

   $$\begin{aligned} &C_g(a \star b) = g \star (a \star b) \star g^{-1} = g \star a \star e \star b \star g^{-1} = g \star a \star (g^{-1} \star g) \star b \star g^{-1} \\ &= (g \star a \star g^{-1}) \star (g \star b \star g^{-1}) = C_g(a) \star C_g(b) \\ &C_{g^{-1}} \circ C_g(a) = g^{-1} \star (g \star a \star g^{-1}) \star g = (g^{-1} \star g) \star a \star (g^{-1} \star g) = e \star a \star e = a \\ &= (g \star g^{-1}) \star a \star (g \star g^{-1}) = g \star (g^{-1} \star a \star g) \star g^{-1} = C_g \circ C_{g^{-1}}(a). \end{aligned}$$

   Somit ist $C_g : G \to G$ ein Gruppenhomomorphismus mit Umkehrabbildung $C_{g^{-1}} : G \to G$.

3. Die Exponentialabbildung definiert einen Gruppenisomorphismus $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, denn sie ist bijektiv, und es gilt $\exp(x + y) = \exp(x) \cdot \exp(y)$ für alle $x, y \in \mathbb{R}$.

4. Für jeden Körper $\mathbb{K}$ und jedes $n \in \mathbb{N}$ definiert die Determinante einen Gruppenhomomorphismus $\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^\times$, denn es gilt $\det(M) \neq 0$ und $\det(M \cdot N) = \det(M) \cdot \det(N)$ für alle $M, N \in \mathrm{GL}(n, \mathbb{K})$.

5. Für eine Permutation $\sigma \in S_n$ und einen Körper $\mathbb{K}$ definiert man die zugehörige **Permutationsmatrix** $M(\sigma) \in \mathrm{GL}(n, \mathbb{K})$ durch $M(\sigma)_{ij} = 1$ falls $\sigma(j) = i$ und $M(\sigma)_{ij} = 0$ sonst. Dies definiert einen Gruppenhomomorphismus $f : S_n \to \mathrm{GL}(n, \mathbb{K})$, $\sigma \mapsto M(\sigma)$ (Übung).

Da jede Gruppe ein ausgezeichnetes Element enthält - das neutrale Element - ist es naheliegend zu untersuchen, wie sich Gruppenhomomorphismen auf dieses ausgezeichnete Element auswirken. Ebenso stellt sich die Frage, wie sich Gruppenhomomorphismen in Hinblick auf Inverse verhalten, und ob wir ein einfacheres Kriterium für die Injektivität eines Gruppenhomomorphismus finden können. So ließ sich beispielsweise im Fall von linearen Abbildungen zwischen Vektorräumen die Injektivität einer linearen Abbildung durch die Aussage charakterisieren, dass der Kern nur den Nullvektor enthält. Eine analoge Charakterisierung ergibt sich auch im Fall von Gruppenhomomorphismen, nur dass der Kern nun nicht mehr als das Urbild des Nullvektors sondern als das Urbild des neutralen Elements definiert wird.

Definition 1.1.8: Sei $f : (G, \star_G) \to (H, \star_H)$ ein Gruppenhomomorphismus. Der **Kern** und das **Bild** von f sind die Mengen

$$\mathrm{im}(f) = f(G) = \{f(g) \mid g \in G\} \subseteq H \qquad \ker(f) = f^{-1}(e_H) = \{g \in G \mid f(g) = e_H\} \subseteq G.$$

Mit dieser Definition können wir nun auch injektive Gruppenhomomorphismen durch die Trvialität ihres Kerns charakterisieren. Ebenso ergibt sich, dass Gruppenhomomorphismen neutrale Elemente auf neutrale Elemente und Inverse auf Inverse abbilden.

Lemma 1.1.9:

Seien $(G, \star_G)$ und $(H, \star_H)$ Gruppen und $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:

1. f bildet das neutrale Element auf das neutrale Element ab: $f(e_G) = e_H$.
2. f bildet Inverse auf Inverse ab: $f(g^{-1}) = f(g)^{-1}$ für alle $g \in G$.
3. f ist injektiv genau dann, wenn $\ker(f) = \{e_G\}$ gilt.

Beweis:
1. Für die neutralen Elemente $e_G \in G$ und $e_H \in H$ gilt

$$e_H \star_H f(e_G) = f(e_G) = f(e_G \star_G e_G) = f(e_G) \star_H f(e_G) \quad \Rightarrow \quad f(e_G) = e_H.$$

2. Für alle $g \in G$ ergibt sich mit 1.

$$f(g^{-1}) \star_H f(g) = f(g^{-1} \star_G g) = f(e_G) = e_H = f(e_G) = f(g \star_G g^{-1}) = f(g) \star_H f(g^{-1}).$$

3. Ist $g \in \ker(f)$, so gilt nach 1. $f(g) = f(e_G) = e_H$ für alle $g \in \ker(f)$. Ist f injektiv, so folgt $g = e_G$ und damit $\ker(f) = \{e_G\}$. Gilt umgekehrt $\ker(f) = \{e_G\}$ und sind $g_1, g_2 \in G$ Elemente mit $f(g_1) = f(g_2)$, so folgt $f(g_1 \star_G g_2^{-1}) = f(g_1) \star_H f(g_2^{-1}) \overset{2.}{=} f(g_1) \star_H f(g_2)^{-1} = e_H$. Damit ist $g_1 \star_G g_2^{-1} \in \ker(f) = \{e_G\}$ und $g_1 = g_2$. □

Die grundlegenden Eigenschaften von Gruppenhomomorphismen in Lemma 1.1.9 reichen bereits aus, um alle Gruppenendomorphismen der Gruppe $(\mathbb{Z}, +)$ zu bestimmen. Wir werden später sehen, dass dies auch für viele andere abelsche Gruppen ähnlich funktioniert.

Korollar 1.1.10: Jeder Gruppenhomomorphismus $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ ist von der Form $f_m : \mathbb{Z} \to \mathbb{Z}$, $z \mapsto mz$ für ein $m \in \mathbb{Z}$. Er ist ein Isomorphismus genau dann, wenn $m \in \{\pm 1\}$.

Beweis:
Sei $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ ein Gruppenhomomorphismus. Dann gilt $f(0) = 0$ nach Lemma 1.1.9. Für $n \in \mathbb{N}$ folgt induktiv

$$f(n) = f(1 + n - 1) = f(1) + f(n - 1) = 2f(1) + f(n - 2) = ... = (n - 1)f(1) + f(1) = nf(1),$$

und mit Lemma 1.1.9 erhalten wir $f(-n) = -f(n) = -nf(1)$. Also gilt $f(z) = mz$ mit $m := f(1)$ für alle $z \in \mathbb{Z}$. Offensichtlich ist f injektiv für $m \neq 0$ und surjektiv genau dann, wenn $m \in \{\pm 1\}$. □

Isomorphe Gruppen werden in der Algebra als im Wesentlichen gleich oder äquivalent betrachtet. Sie lassen sich mit gruppentheoretischen Mitteln nicht unterscheiden, da sie durch bloße Umbenennungen der Elemente auseinander hervorgehen. Ein Gruppenisomorphismus $f : (H, \star_H) \to (G, \star_G)$ ist nichts anderes als eine solche Umbenennungsvorschrift. Dies suggeriert, dass es sich bei der Isomorphie von Gruppen um eine Äquivalenzrelation handelt. Um zu zeigen, dass Isomorphie von Gruppen tatsächlich reflexiv, symmetrisch und transitiv ist, benötigt man die Aussagen, dass (i) die Identitätsabbildungen Gruppenisomorphismen sind, dass (ii) für jeden Gruppenisomorphismus auch die inverse Abbildung ein Gruppenisomorphismus ist und dass (iii) die Verkettung zweier Gruppenisomorphismen ein Gruppenisomorphismus ist. Diese Aussagen ergeben sich aus dem folgenden Satz.

Satz 1.1.11:

1. Für jede Gruppe $(G, \star_G)$ ist $\mathrm{id}_G : G \to G$ ein Gruppenautomorphismus.
2. Sind $(G, \star_G)$ und $(H, \star_H)$ Gruppen und $f : G \to H$ ein Gruppenisomorphismus, dann ist auch die Umkehrabbildung $f^{-1} : H \to G$ ein Gruppenisomorphismus.
3. Sind $(G, \star_G)$, $(H, \star_H)$ und $(K, \star_K)$ Gruppen und $f : G \to H$, $f' : H \to K$ Gruppenhomomorphismen, so ist auch die Verkettung $f' \circ f : G \to K$ ein Gruppenhomomorphismus.

Beweis:
1. Die Abbildung id_G ist bijektiv mit $\mathrm{id}_G(g \star_G g') = g \star_G g' = \mathrm{id}_G(g) \star_G \mathrm{id}_G(g')$ für alle $g, g' \in G$.

2. Da $f : G \to H$ ein Gruppenisomorphismus ist, erhält man für alle $h, h' \in H$

$$f^{-1}(h) \star_G f^{-1}(h') = f^{-1}(f(f^{-1}(h) \star_G f^{-1}(h'))) = f^{-1}(f(f^{-1}(h)) \star_H f(f^{-1}(h'))) = f^{-1}(h \star_H h').$$

3. Da $f : G \to H$ und $f' : H \to K$ Gruppenhomomorphismen sind, erhält man für alle $g, g' \in G$

$$\begin{aligned}(f' \circ f)(g \star_G g') &= f'(f(g \star_G g')) = f'(f(g) \star_H f(g')) = f'(f(g)) \star_K f'(f(g')) \\ &= (f' \circ f)(g) \star_K (f' \circ f)(g')\end{aligned}$$

□

Korollar 1.1.12: Für jede Gruppe G bilden die Gruppenautomorphismen mit der Verkettung eine Gruppe. Sie wird als die **Automorphismengruppe** von G und mit $\mathrm{Aut}(G)$ bezeichnet.

Beweis:
1. Nach Satz 1.1.11 ist die Verkettung von Gruppenautomorphismen ein Gruppenendomorphismus von G, und da die Verkettung von bijektiven Abbildungen bijektiv ist, auch ein Gruppenautomorphismus. Damit definiert die Verkettung von Gruppenautomorphismen eine Abbildung $\circ : \mathrm{Aut}(G) \times \mathrm{Aut}(G) \to \mathrm{Aut}(G)$. Diese ist assoziativ mit neutralem Element $\mathrm{id}_G : G \to G$. Nach Satz 1.1.11 ist auch die Umkehrabbildung $f^{-1} : G \to G$ jedes Gruppenautomorphismus $f : G \to G$ wieder ein Gruppenautomorphismus und damit das Inverse von f bezüglich $\circ$. □

Beispiel 1.1.13.

1. Nach Korollar 1.1.10 gilt $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, -\mathrm{id}\} \cong C_2$.
2. Für die zweielementige Gruppe C_2 gilt $\mathrm{Aut}(C_2) = \{\mathrm{id}\}$. Denn jeder Gruppenautomorphismus $f : C_2 \to C_2$ muss das neutrale Element auf sich selbst und wegen der Injektivität dann auch das andere Element von C_2 auf sich selbst abbilden.

1.2 Untergruppen

In diesem Abschnitt befassen wir uns mit Untergruppen - Gruppen, die in anderen Gruppen enthalten sind. Diese können als das Gruppen-Gegenstück von Untervektorräumen aufgefasst werden und lassen sich wie auch Untervektorräume auf zwei verschiedene Arten charakterisieren. Entweder als eine Teilmenge einer Gruppe G, die gewisse vorgegebene Bedingungen erfüllt, oder durch die Forderung, dass diese Teilmenge mit der Einschränkung der Gruppenmultiplikation auf G eine Gruppe bildet. Wir definieren sie zunächst durch konkrete Forderungen an die Teilmenge und zeigen dann, dass diese Forderungen auf die zweite Bedingung hinausläuft.

Definition 1.2.1: Sei $(G, \star)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt **Untergruppe** von G, falls gilt:

(UG1) $h \star h' \in H$ für alle $h, h' \in H$,

(UG2) $e_G \in H$,

(UG3) $h^{-1} \in H$ für alle $h \in H$.

Bemerkung 1.2.2.

1. Aus (UG2) folgt insbesondere, dass eine Untergruppe niemals leer ist. In der Tat könnte man (UG2) durch die äquivalente Forderung $H \neq \varnothing$ ersetzen (warum?).

2. Jede Gruppe G besitzt Untergruppen, nämlich $H = G$ und die **triviale Untergruppe** $H = \{e\}$. Eine Untergruppe H mit $H \neq G$ heißt **echte Untergruppe**. Eine Untergruppe H mit $H \neq \{e\}$ heißt **nichttriviale Untergruppe**.

Satz 1.2.3: Sei $(G, \star_G)$ eine Gruppe. Dann ist eine Teilmenge $H \subseteq G$ genau dann eine Untergruppe von G, wenn sie mit $\star_H \colon H \times H \to H$, $(h_1, h_2) \mapsto h_1 \star_G h_2$ eine Gruppe ist.

Beweis:
Ist $H \subseteq G$ eine Untergruppe, so ist $\star_H$ wohldefiniert, und die Assoziativität folgt aus der Assoziativität von G. Nach (UG2) ist $e_G \in H$, und da $h \star_H e_G = h \star_G e_G = h = e_G \star_G h = e_G \star_H h$ für alle $h \in H$, ist e_G das neutrale Element von H. Wegen (UG3) ist für $h \in H$ auch $h^{-1} \in H$ und $h \star_H h^{-1} = h \star_G h^{-1} = e_G = e_H$. Damit ist h^{-1} auch das Inverse von h in H.

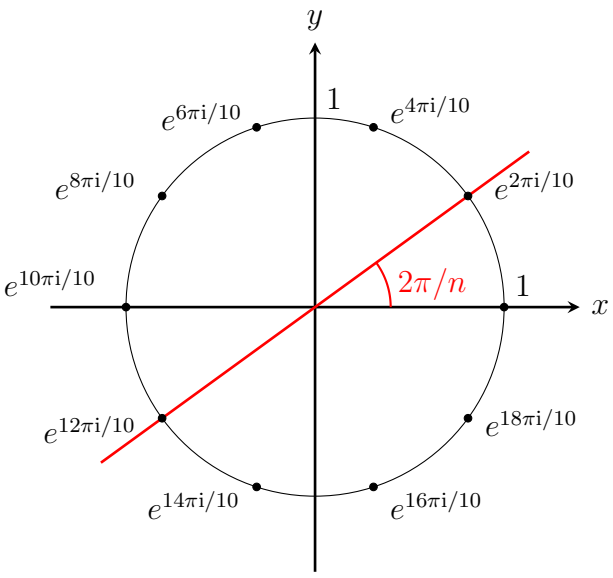
Ist $H \subseteq G$ eine Teilmenge, die mit $\star_H$ eine Gruppe bildet, so gilt $h_1 \star_G h_2 = h_1 \star_H h_2 \in H$ für alle $h_1, h_2 \in H$ (UG1). Ist e_H das neutrale Element von $(H, \star_H)$, so gilt $e_H \star_G e_H = e_H \star_H e_H = e_H = e_H \star_G e_G$, und mit der Kürzungsregel in G folgt $e_H = e_G \in H$ (UG2). Ist h^{-1} das Inverse eines Elements $h \in H$ in $(G, \star_G)$, so folgt $e_H = e_G = h \star_G h^{-1} = h \star_H h^{-1} = h^{-1} \star_G h = h^{-1} \star_H h$. Damit ist h^{-1} auch das Inverse von h in $(H, \star_H)$ und $h^{-1} \in H$ (UG3). □

Beispiel 1.2.4.

1. Der **Einheitskreis** $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ ist eine Untergruppe der Gruppe $(\mathbb{C}^\times, \cdot)$.

2. Für jedes $n \in \mathbb{N}$ bilden die n**ten Einheitswurzeln** in $\mathbb{C}$ eine Untergruppe der Gruppen $(\mathbb{C}^\times, \cdot)$ und $(S^1, \cdot)$ (Übung). Diese Gruppe wird mit bezeichnet mit

$$C_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{2\pi \mathrm{i} k/n} \mid k = 0, 1, ..., n-1\}.$$



Der komplexe Einheitskreis S^1 und die $n$ten Einheitswurzeln für $n = 10$.

3. Für jeden Körper $\mathbb{K}$ und $n \in \mathbb{N}$ ist $\mathrm{SL}(n,\mathbb{K}) = \{M \in \mathrm{GL}(n,\mathbb{K}) \mid \det(M) = 1\}$ eine Untergruppe der Gruppe $\mathrm{GL}(n,\mathbb{K})$. Sie heißt die **spezielle lineare Gruppe**.

   Denn es gilt $\mathbb{1} \in \mathrm{SL}(n,\mathbb{K})$ (UG2). Für $M, N \in \mathrm{SL}(n,\mathbb{K})$ gilt $\det(M^{-1}) = \det(M)^{-1} = 1$ und $\det(M \cdot N) = \det(M) \cdot \det(N) = 1 \cdot 1 = 1$, also $M^{-1} \in \mathrm{SL}(n,\mathbb{K})$ (UG3) und $M \cdot N \in \mathrm{SL}(n,\mathbb{K})$ (UG1).

4. Die orthogonalen $n \times n$-Matrizen mit Einträgen in $\mathbb{K}$ bilden ebenfalls eine Untergruppe der Gruppe $\mathrm{GL}(n,\mathbb{K})$, die **orthogonale Gruppe** $\mathrm{O}(n,\mathbb{K}) = \{M \in \mathrm{GL}(n,\mathbb{K}) \mid M^T = M^{-1}\}$.

5. Die unitären komplexen $n \times n$-Matrizen bilden eine Untergruppe der Gruppe $\mathrm{GL}(n,\mathbb{C})$, die **unitäre Gruppe** $\mathrm{U}(n) = \{M \in \mathrm{GL}(n,\mathbb{C}) \mid M^\dagger = M^{-1}\}$.

6. Sei $(G,\star)$ eine Gruppe und $U \subseteq G$ eine Teilmenge. Dann ist der **Zentralisator** von U $Z(U) = \{g \in G \mid gug^{-1} = u \ \forall u \in U\}$ eine Untergruppe von G.

   Insbesondere gilt das für die Zentralisatoren $Z_g := Z(\{g\})$ jedes Elements $g \in G$ und für den Zentralisator $Z(G)$, der auch das **Zentrum** von G genannt wird. (Übung).

7. Für jede Menge M und Teilmenge $U \subseteq M$ sind

   $$\mathrm{Stab}(U) = \{\varphi \in S_M \mid \varphi(u) = u \ \forall u \in U\} \quad \text{und} \quad \mathrm{Symm}(U) = \{\varphi \in S_M \mid \varphi(U) = U\}$$

   Untergruppen der Permutationsgruppe S_M.

Da nach Korollar 1.1.12 auch die Gruppenautomorphismen einer gegebenen Gruppe wieder eine Gruppe bilden, können wir auch Untergruppen der Automorphismengruppe betrachten. Auch wenn wir die Gruppe nicht kennen, wissen wir aus Beispiel 1.1.7, dass zumindest die Konjugationsautomorphismen in der Automorphismengruppe enthalten sein müssen. Tatsächlich bilden sie eine Untergruppe der Automorphismengruppe, die *innere Automorphismengruppe*.

Beispiel 1.2.5. Für jede Gruppe $(G,\star)$ bilden die Konjugationsabbildungen $C_h : G \to G$, $g \mapsto h \star g \star h^{-1}$ für $h \in G$ eine Untergruppe der Automorphismengruppe $\mathrm{Aut}(G)$. Sie wird als **innere Automorphismengruppe** und mit $\mathrm{Inn}(G)$ bezeichnet.

Beweis:
Denn es gilt $C_e(g) = e \star g \star e^{-1} = g$ für alle $g \in G$ und damit $C_e = \mathrm{id}_G$. Also ist das neutrale Element von $\mathrm{Aut}(G)$, die Identitätsabbildung id_G in $\mathrm{Inn}(G)$ enthalten (UG2). Für alle $h, k, g \in G$ gilt $C_h \circ C_k(g) = h \star (k \star g \star k^{-1}) \star h^{-1} = (h \star k) \star g \star (k^{-1} \star h^{-1}) = (h \star k) \star g \star (h \star k)^{-1} = C_{h \star k}(g)$ und damit $C_h \star C_k = C_{h \star k} \in \mathrm{Inn}(G)$ (UG1). Nach Beispiel 1.1.7 gilt außerdem $C_{h^{-1}} = C_h^{-1}$ für alle $h \in G$ und damit $C_h^{-1} = C_{h^{-1}} \in \mathrm{Inn}(G)$ für alle $h \in G$ (UG3). □

Im Fall der abelschen Gruppe $(\mathbb{Z},+)$ können wir sogar *alle* Untergruppen explizit bestimmen. Jede Untergruppe besteht genau aus den Vielfachen einer nicht-negativen Zahl $n \in \mathbb{N}_0$. Diese Aussage wird sich im Verlauf der Vorlesung noch als sehr nützlich erweisen.

Beispiel 1.2.6. Die Untergruppen der Gruppe $(\mathbb{Z},+)$ sind genau die Teilmengen

$$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} \quad \text{mit} \quad n \in \mathbb{N}_0.$$

Jede Untergruppe $n\mathbb{Z}$ für $n \neq 0$ ist isomorph zu $\mathbb{Z}$.

Beweis:
1. Die Teilmengen $n\mathbb{Z}$ sind Untergruppen. Denn aus $h_1, h_2 \in n\mathbb{Z}$ folgt $h_1 = nz_1$ und $h_2 = nz_2$ mit $z_1, z_2 \in \mathbb{Z}$. Daraus ergibt sich $h_1 + h_2 = nz_1 + nz_2 = n(z_1 + z_2) \in n\mathbb{Z}$ (UG1) und $-h_2 = -nz_2 = n(-z_2) \in \mathbb{Z}$ (UG3). Außerdem gilt $0 = n0 \in \mathbb{Z}$ (UG2).

2. Sei nun H eine Untergruppe von $\mathbb{Z}$. Dann gilt entweder $H = \{0\} = 0\mathbb{Z}$, oder es gibt ein Element $0 \neq h \in H$. Da aus $h \in H$ mit (UG3) auch $-h \in H$ folgt, gibt es dann ein Element $h \in H \cap \mathbb{N}$. Sei nun $n = \min\{h > 0 \mid h \in H\}$. Aus $n \in H$ folgt dann induktiv mit (UG1) $kn = n + ... + n \in H$ für alle $k \in \mathbb{N}$ und mit (UG2) $-nk \in H$ für alle $k \in \mathbb{N}$. Da außerdem $0 \in H$ (UG2), ist gezeigt, dass $nz \in H$ für alle $z \in \mathbb{Z}$ und damit $n\mathbb{Z} \subseteq H$. Gäbe es ein Element $h \in H \setminus n\mathbb{Z}$, so wäre $h = np + q$ mit $p \in \mathbb{Z}$ und $q \in \{1, ..., n-1\}$ (Division mit Rest). Daraus folgt mit (UG1) und (UG3) $q = h - np \in H$, im Widerspruch zu $n = \min\{h > 0 \mid h \in H\}$. Also gilt $H = n\mathbb{Z}$.

3. Für $n \neq 0$ ist nach Korollar 1.1.10 die Abbildung $f_n : \mathbb{Z} \to \mathbb{Z}$, $z \mapsto nz$ ein injektiver Gruppenhomomorphismus mit Bild $f_n(\mathbb{Z}) = n\mathbb{Z}$. Damit ist die Koeinschränkung $f'_n : \mathbb{Z} \to n\mathbb{Z}$, $z \mapsto nz$ ein Gruppenisomorphismus für $n \neq 0$. □

Weitere Beispiele von Untergruppen erhalten wir, indem wir sie mit Hilfe von bekannten Strukturen systematisch konstruieren. So können wir beispielsweise Untergruppen zweier Gruppen G und H zu Untergruppen ihres direkten Produkts $G \times H$ zusammensetzen.

Beispiel 1.2.7. Seien G und H Gruppen und $U \subseteq G$ und $V \subseteq H$ Untergruppen. Dann ist $U \times V$ eine Untergruppe des direkten Produkts $G \times H$.

Beweis:
Nach (UG2) gilt $e_G \in U$ und $e_H \in V$ und damit auch $e = (e_G, e_H) \in U \times V$ (UG2). Sind $(u_1, v_1), (u_2, v_2) \in U \times V$, so gilt $u_1, u_2 \in U$ und $v_1, v_2 \in V$. Mit (UG1) folgt $u_1u_2 \in U$, $v_1v_2 \in V$ und damit auch $(u_1, v_1)(u_2, v_2) = (u_1u_2, v_1v_2) \in U \times V$ (UG1). Ebenso ergibt sich mit (UG3) $u_1^{-1} \in U$, $v_1^{-1} \in V$ und damit auch $(u_1, v_1)^{-1} = (u_1^{-1}, v_1^{-1}) \in U \times V$ (UG3). □

Um weitere Beispiele zu konstruieren, könen wir analog zur linearen Algebra vorgehen und bekannte Konstruktionen für Vektorräume auf Gruppen verallgemeinern. Ein wichtiger Satz aus der linearen Algebra besagt, dass Bilder und Urbilder von Untervektorräumen Untervektorräume sind. Dies suggeriert, dass Bilder und Urbilder von Untergruppen unter Gruppenhomomorphismen Untergruppen sein sollten.

Lemma 1.2.8: Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:

1. Für jede Untergruppe U von G ist $f(U)$ eine Untergruppe von H.
2. Für jede Untergruppe V von H ist $f^{-1}(V)$ eine Untergruppe von G.
3. Insbesondere ist das Bild $\mathrm{im}(f) = f(G)$ eine Untergruppe von H und der Kern $\ker(f) = f^{-1}(e_H)$ eine Untergruppe von G.

Beweis:
1. Ist U eine Untergruppe von G so gilt $e_G \in U$, und mit Lemma 1.1.9 folgt $f(e_G) = e_H \in f(U)$ (UG2). Sind $h_1, h_2 \in f(U)$, so gibt es $u_1, u_2 \in U$ mit $h_1 = f(u_1)$ und $h_2 = f(u_2)$. Da U eine

Untergruppe von G ist, gilt $u_1^{-1}, u_1u_2 \in U$. Da f ein Gruppenhomomorphismus ist, folgt daraus $h_1h_2 = f(u_1)f(u_2) = f(u_1u_2) \in f(U)$ (UG1) und $h_1^{-1} = f(u_1)^{-1} = f(u_1^{-1}) \in U$ (UG3).

2. Ist V eine Untergruppe von H, so folgt mit Lemma 1.1.9 $e_H = f(e_G) \in V$ und damit $e_G \in f^{-1}(V)$ (UG2). Sind $g_1, g_2 \in f^{-1}(V)$, so gilt $f(g_1), f(g_2) \in V$. Da V eine Untergruppe von H ist und f ein Gruppenhomomorphismus, ergibt sich $f(g_1)f(g_2) = f(g_1g_2) \in V$ und mit Lemma 1.1.9 $f(g_1)^{-1} = f(g_1^{-1}) \in V$. Damit ist $g_1g_2 \in f^{-1}(V)$ (UG1) und $g_1^{-1} \in f^{-1}(V)$ (UG3).

3. Dies folgt direkt aus 1. und 2., indem man $U = G$ und $V = \{e_H\}$ setzt. □

Eine weitere Konstruktion aus der linearen Algebra, die Untervektorräume liefert, ist der Schnitt von Untervektorräumen eines gegebenen Vektorraums. Analog kann man im Fall von Gruppen beliebige Schnitte von Untergruppen betrachten.

Satz 1.2.9: Sei G eine Gruppe, I eine Indexmenge und $H_i \subseteq G$ eine Untergruppe von G für alle $i \in I$. Dann ist auch ihr **Schnitt** $\cap_{i\in I} H_i$ eine Untergruppe von G.

Beweis:
Seien $g, h \in \cap_{i\in I} H_i$. Dann gilt $g, h \in H_i$ für alle $i \in I$, und damit auch $gh, e, g^{-1} \in H_i$ für alle $i \in I$. Daraus folgt $gh, e, g^{-1} \in \cap_{i\in I} H_i$, und damit ist $\cap_{i\in I} H_i$ eine Untergruppe. □

Beispiel 1.2.10.

1. Die **spezielle orthogonale Gruppe** $\mathrm{SO}(n, \mathbb{K})$ ist eine Untergruppe von $\mathrm{GL}(n, \mathbb{K})$
$$\mathrm{SO}(n, \mathbb{K}) = \{M \in \mathrm{GL}(n, \mathbb{K}) \mid M^T = M^{-1}, \det M = 1\} = \mathrm{O}(n, \mathbb{K}) \cap \mathrm{SL}(n, \mathbb{K}).$$
2. Der Schnitt der Untergruppen $n\mathbb{Z} \subseteq \mathbb{Z}$ und $m\mathbb{Z} \subseteq \mathbb{Z}$ ist die Untergruppe $\mathrm{kgV}(n, m)\mathbb{Z}$.

Man beachte, dass die *Vereinigung* von Untergruppen im Allgemeinen keine Untergruppe ist. Ein einfaches Gegenbeispiel sind die Untergruppen $2\mathbb{Z}$ und $3\mathbb{Z}$ der Gruppe $(\mathbb{Z}, +)$, die die Vielfachen von 2 und 3 enthalten. Die Vereinigung $2\mathbb{Z} \cup 3\mathbb{Z}$ enthält genau die Zahlen, die Vielfache von 2 oder 3 sind. Offensichtlich gilt also $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ und $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, aber $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$, und damit kann $2\mathbb{Z} \cup 3\mathbb{Z}$ keine Untergruppe von $(\mathbb{Z}, +)$ sein.

Dies ist nicht überraschend, denn auch die Vereinigung von Untervektorräumen ist im Allgemeinen nur eine Teilmenge des Vektorraums und nicht notwendigerweise ein Untervektorraum. Es gibt aber eine Konstruktion, die aus beliebigen Teilmengen eines Vektorraums einen Untervektorraum konstruiert, nämlich den *Spann* oder die *lineare Hülle*. Diese kann abstrakt definiert werden als der Schnitt aller Untervektorräume, die eine gegebene Teilmenge eines Vektorraums enthalten, oder konkret als Untervektorraum aller Linearkombinationen von Vektoren aus der Teilmenge. Eine analoge Konstruktion gibt es auch für Untergruppen.

Definition 1.2.11: Sei G eine Gruppe und sei $M \subseteq G$ eine Teilmenge. Die **von M erzeugte Untergruppe** ist die kleinste Untergruppe, die M enthält:

$$\langle M \rangle = \bigcap_{\substack{H \text{ Untergruppe von G} \\ \text{mit } M \subseteq H}} H$$

Ist $M = \{g_1, ..., g_k\}$ endlich, schreibt man auch $\langle M \rangle = \langle g_1, ..., g_k \rangle$.

Man kann für M dabei auch die leere Menge wählen, die eine Teilmenge *jeder* Menge ist. In diesem Fall nimmt auch die triviale Untergruppe $\{e\}$ am Schnitt teil, und es folgt $\langle\varnothing\rangle = \{e\}$. Allgemeiner gilt: ist $H \subseteq G$ eine Untergruppe mit $M \subseteq H$, so nimmt die Untergruppe H am Schnitt der Untergruppen in Definition 1.2.11 teil, und der Schnitt $\langle M\rangle$ ist damit in H enthalten. Dies rechtfertigt die Bezeichnung *kleinste Untergruppe, die M enthält.*

Anstatt sie abstrakt als Schnitt von Untergruppen zu charakterisieren, können wir die von M erzeugte Untergruppe auch konkret angeben. Dies ist wieder analog zu der Situation für Vektorräume. Dort enthält die lineare Hülle einer Teilmenge gerade die Linearkombinationen von Vektoren aus der Teilmenge. Im Fall von Gruppen sind in der Untergruppe $\langle M\rangle$ gerade die Produkte von Elementen aus M und ihren Inversen enthalten sowie das neutrale Element.

Lemma 1.2.12: Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge. Dann gilt:

$$\langle M\rangle = \{g_1 g_2 \dots g_n \in G \mid \ n \geq 0, g_1, \dots, g_n \in M \cup M^{-1}\},$$

wobei $M^{-1} = \{g^{-1} \mid g \in M\}$ und $g_1 \cdots g_n := e$ für $n = 0$. Insbesondere gilt für alle $g \in G$

$$\langle g\rangle = \{..., g^{-2}, g^{-1}, e, g, g^2, ...\} = \{g^n \mid n \in \mathbb{Z}\}.$$

Beweis:
1. Wir zeigen, dass $U := \{g_1 \dots g_n \in G \mid n \geq 0, g_1, \dots, g_n \in M \cup M^{-1}\}$ eine Untergruppe von G ist. Per Definition von U gilt $e \in U$ (UG2). Für $g, h \in U$ gibt es $g_1, \dots, g_k, h_1, \dots, h_l \in M \cup M^{-1}$ mit $g = g_1 \dots g_k$ und $h = h_1 \dots h_l$. Daraus folgt $gh = g_1 \dots g_k h_1 \dots h_l \in U$ (UG1). Außerdem gilt $g_1^{-1}, \dots, g_k^{-1} \in M \cup M^{-1}$, denn $g_i \in M^{\pm 1}$ impliziert $g_i^{-1} \in M^{\mp 1}$. Damit ist $g^{-1} = g_k^{-1} \dots g_1^{-1} \in U$ (UG3), und U ist eine Untergruppe von G.

2. Wir zeigen, dass $U = \langle M\rangle$. Per Definition von U gilt $M \subseteq U$. Damit nimmt U am Schnitt in Definition 1.2.11 teil, und es folgt $\langle M\rangle \subseteq U$. Um $U \subseteq \langle M\rangle$ zu beweisen, zeigen wir, dass für alle Untergruppen $H \subseteq G$ mit $M \subseteq H$ auch $U \subseteq H$ gilt. Ist H eine Untergruppe von G mit $M \subseteq H$, so gilt $e \in H$ (UG2), $g \in H$ und $g^{-1} \in H$ für alle $g \in M$ (UG3). Mit (UG1) folgt induktiv $g_1 \cdots g_n \in H$ für alle $g_1, ..., g_n \in M \cup M^{-1}$. Damit ist gezeigt, dass $U \subseteq H$ für alle Untergruppen $H \subseteq G$ mit $M \subseteq H$. Damit ist U auch im Schnitt aller solchen Untergruppen H enthalten, und es folgt $U \subseteq \langle M\rangle$. □

Insbesondere ist man an Teilmengen einer Gruppe interessiert, die die ganze Gruppe erzeugen. Diese sind im Allgemeinen nicht eindeutig. Wie auch ein Vektorraum viele verschiedene Erzeugendensysteme besitzen kann, so kann es viele verschiedene Teilmengen geben, die eine Gruppe erzeugen. Das Auffinden solcher Teilmengen ist im Allgemeinen viel schwieriger als bei Vektorräumen, und es gibt kein Analogon von Basen. Zwischen den einzelnen Elementen einer erzeugenden Teilmenge können komplizierte multiplikative Relationen bestehen, und es ist oft auch schwierig zu sehen, ob eine gegebene Teilmenge die ganze Gruppe erzeugt. Dennoch hat man die Situation gut unter Kontrolle für Gruppen, die von einem einzigen Element erzeugt werden. Diese werden wir in Abschnitt 1.7.1 bis auf Isomorphie vollständig bestimmen.

Definition 1.2.13: Eine Gruppe G heißt **endlich erzeugt**, wenn es eine endliche Teilmenge $M \subseteq G$ gibt mit $G = \langle M\rangle$, und **zyklisch**, wenn sie von einem Element erzeugt wird.

Beispiel 1.2.14.

1. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch: $\mathbb{Z} = \langle 1 \rangle$.

   Denn für $n \in \mathbb{N}$ gilt $n = 1 + ... + 1 = n1$ und $-n = -(1 + ... + 1) = -1 - ... - 1$.

2. Die Gruppe $C_n = \{e^{2\pi ik/n} \mid k = 0, 1, ..., n-1\}$ der $n$ten Einheitswurzeln aus Beispiel 1.2.4, 5. ist zyklisch mit $C_n = \langle e^{2\pi i/n} \rangle$, denn $e^{2\pi ik/n} = (e^{2\pi i/n})^k$.

3. Die Gruppe $(\mathbb{Q}, +)$ ist nicht endlich erzeugt.

   Gäbe es rationale Zahlen $x_1, ..., x_n$ mit $\mathbb{Q} = \langle x_1, ..., x_n \rangle$, so könnten wir diese als gekürzte Brüche $x_i = p_i/q_i$ schreiben. Jede endliche Summe der Zahlen x_i und $-x_i$ ließe sich dann als (nicht notwendigerweise gekürzter) Bruch mit Nenner $\mathrm{kgV}(q_1, ..., q_n)$ schreiben. Damit ist aber $1/p$ für eine zu $q_1, ..., q_n$ teilerfremde Primzahl p nicht in $\langle x_1, ..., x_n \rangle$ enthalten.

Ein Beispiel einer endlich erzeugten, aber nicht zyklischen Gruppe, an dem auch die Uneindeutigkeit in der Wahl der erzeugenden Teilmenge deutlich wird, ist die Symmetriegruppe des regulären n-Ecks, die sogenannte *Diedergruppe*[1].

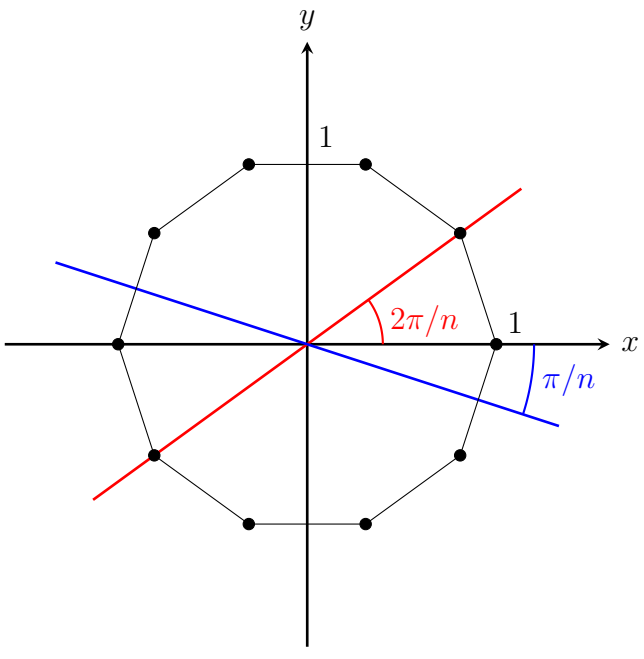
Beispiel 1.2.15.

Für $n \geq 3$ bezeichnen wir mit $P_n \subseteq \mathbb{R}^2$ das reguläre n-Eck mit Zentrum $(0, 0)$ und Ecken $(\cos(2\pi k/n), \sin(2\pi k/n))$ für $k \in \{0, 1, ..., n-1\}$.

Die **Symmetriegruppe** von P_n ist definiert als die Gruppe

$$D_n = \{\varphi \in \mathrm{O}(2, \mathbb{R}) \mid \varphi(P_n) = P_n\} \subseteq O(2, \mathbb{R})$$

der orthogonalen $\mathbb{R}$-linearen Abbildungen $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, die das reguläre n-Eck auf sich selbst abbilden. Sie heißt **Diedergruppe**.



Das reguläre n-Eck P_n für $n = 10$.

[1] Gesprochen „Di-eder“. Die Bezeichnung stammt von Dieder=Zweiflächner.

Jede orthogonale 2×2-Matrix ist entweder eine **Rotation** um einen Winkel φ von der Form

$$R(\varphi) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

oder eine **Spiegelung** $S(\varphi)$ an einer Geraden, die den Winkel $\frac{\varphi}{2}$ mit der x-Achse einschließt

$$S(\varphi) = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}.$$

Die Diedergruppe enthält genau die Rotationen um Vielfache des Winkels $2\pi/n$ und Spiegelungen an Achsen durch die Seitenmittelpunkte und Ecken des n-Ecks:

$$\mathrm{D}_n = \{R(\tfrac{2\pi k}{n}) \mid k = 0, \ldots, n-1\} \dot\cup \{S(\tfrac{2\pi k}{n}) \mid k = 0, \ldots, n-1\}.$$

Dies definiert die Diedergruppe auch für $n = 1$ und $n = 2$. Es gilt $D_1 \cong C_2$ und $D_2 \cong V$ (Kleinsche Vierergruppe).
Insbesondere gilt $|\mathrm{D}_n| = 2n$. Die Diedergruppe wird erzeugt durch die Rotation $r := R(\frac{2\pi}{n})$ und die Spiegelung $s := S(0)$, denn wegen $R(\frac{2\pi k}{n}) = R(\frac{2\pi}{n})^k$ und $S(\frac{2\pi k}{n}) = R(\frac{2\pi}{n})^k S(0)$ lässt sich jedes Element von D_n als Produkt dieser Elemente schreiben.

$$\mathrm{D}_n = \langle r, s \rangle.$$

Die beiden Erzeuger r und s erfüllen die Relationen $r^n = s^2 = e, sr = r^{-1}s$. Eine andere beliebte Wahl von Erzeugern sind die beiden Spiegelungen s und $t := S(\frac{2\pi}{n}) = rs$ mit den Relationen $s^2 = t^2 = (st)^n = e$.

Wir befassen uns nun noch etwas genauer mit den von einzelnen Gruppenelementen $g \in G$ erzeugten zyklischen Untergruppen $\langle g \rangle$, die nach Lemma 1.2.12 genau die Potenzen des Elements g enthalten. Dazu benötigen wir zunächst zwei Rechenregeln für Potenzen.

Lemma 1.2.16: Sei G eine Gruppe und $g \in G$. Dann gilt für alle $m, n \in \mathbb{Z}$

$$g^m g^n = g^{m+n} \qquad (g^m)^n = g^{mn}$$

Beweis:
Nach Bemerkung 1.1.3 sind die Potenzen eines Gruppenelements definiert als

$$g^n = \underbrace{g \cdot g \cdots g}_{n\times} \text{ für } n > 0 \qquad g^0 = e \qquad g^n = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{(-n)\times} \text{ für } n < 0.$$

Wir beweisen die Formeln durch eine Fallunterscheidung. Für die erste Formel ergibt sich:

- $m, n > 0$: $g^n g^m = (g \cdots g)(g \cdots g) = g^{n+m}$.
- $m = 0$: $g^m g^n = g^0 g^n = e \cdot g^n = g^n = g^{m+n}$.
- $n > -m > 0$: $g^m g^n = (g^{-m})^{-1} g^n = (g^{-m})^{-1} g^{-m} g^{m+n} = g^{m+n}$
  Damit ist die Formel für alle m, n mit $|m| < n$ bewiesen.
- m, n beliebig: Wähle ein $N \in \mathbb{N}$ mit $N > |m| + |n|$. Dann gilt $N > |n|$, $N + n > |m|$ und $N > |m + n|$. Dreimalige Anwendung des Falles $|m| < n$ und die Kürzungsregel ergibt

$$g^m g^n g^N = g^m g^{n+N} = g^{m+n+N} = g^{m+n} g^N \quad \Rightarrow \quad g^m g^n = g^{m+n}.$$

2. Für die zweite Formel ergibt sich mit 1.

- $n > 0$: $(g^m)^n = g^m \cdots g^m = g^{m+\ldots+m} = g^{mn}$
- $n = 0$: $(g^m)^n = (g^m)^0 = e = g^0 = g^{mn}$
- $n = -1$: $g^m g^{-m} = g^0 = e \Rightarrow (g^m)^{-1} = g^{-m} = g^{mn}$.
- $n < 0$: $(g^m)^n = ((g^m)^{-n})^{-1} = (g^{m(-n)})^{-1} = g^{-(-mn)} = g^{mn}$.

□

Aus den Rechenregeln für Potenzen folgt direkt, dass jede zyklische Gruppe G abelsch ist. Denn nach Lemma 1.2.12 gilt $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ und nach Lemma 1.2.16 ist $g^n \cdot g^m = g^{n+m} = g^m \cdot g^n$ für alle $n, m \in \mathbb{Z}$.

Korollar 1.2.17: Jede zyklische Gruppe ist abelsch.

Wir können die von einem Gruppenelement $g \in G$ erzeugte zyklische Untergruppe auch mit der abelschen Gruppe $\mathbb{Z}$ in Verbindung bringen, indem wir einer ganzen Zahl n die $n$te Potenz eines festen Gruppenelements $g \in G$ zuordnen. Dies liefert einen Gruppenhomomorphismus, dessen Bild gerade die Potenzen von g enthält.

Korollar 1.2.18: Sei G eine Gruppe und $g \in G$. Dann ist die Abbildung $f_g : \mathbb{Z} \to G : n \mapsto g^n$ ein Gruppenhomomorphismus mit Bild $\langle g \rangle$.

Beweis:
Nach Lemma 1.2.16 gilt $f_g(n+m) = g^{n+m} = g^n \cdot g^m$ und damit ist f_g ein Gruppenhomomorphismus. Sein Bild ist gegeben durch $f_g(\mathbb{Z}) = \{g^n \mid n \in \mathbb{Z}\} = \langle g \rangle$. □

Der Gruppenhomomorphismus f_g aus Korollar 1.2.18 ist offensichtlich surjektiv genau dann, wenn g die Gruppe G erzeugt. Nach Lemma 1.1.9 ist er injektiv, genau dann wenn $\ker(f_g) = \{e\}$, also wenn $g^n \neq e$ für alle $n \neq 0$ gilt. Gibt es ein $n \in \mathbb{N}$ mit $g^n = e$, so folgt daraus sofort auch $g^{-n} = e$. Es ist also sinnvoll, die kleinste positive Zahl n zu betrachten, für die $g^n = e$ gilt, die von g erzeugte Untergruppe dadurch zu charakterisieren.

Definition 1.2.19: Sei G eine Gruppe. Die **Ordnung** $o(g)$ eines Gruppenelements $g \in G$ ist die kleinste positive Zahl n mit $g^n = e$, wenn eine solche Zahl existiert. Ansonsten ist $o(g) = \infty$.

Korollar 1.2.20: Für jeden Erzeuger $g \in G$ einer zyklischen Gruppe G gilt $o(g) = |G|$. Ist $o(g) < \infty$, so gilt

$$G = \{e, g, g^2, \ldots, g^{o(g)-1}\}.$$

Beweis:
Ist $o(g) = \infty$, so gilt $g^n \neq g^m$ für alle $n \neq m \in \mathbb{Z}$. Denn aus $g^n = g^m$ folgt mit der Kürzungsregel $g^{n-m} = e$. Damit enthält $G = \langle g \rangle$ unendlich viele Elemente und $|G| = \infty = o(g)$.

Ist $o(g) = m < \infty$, so können wir mit der Division mit Rest jede ganze Zahl $n \in \mathbb{Z}$ schreiben als $n = km + r$ mit $k \in \mathbb{Z}$ und $r \in \{0, 1, ..., m-1\}$. Daraus folgt $g^n = g^{km+r} = (g^m)^k \cdot g^r = e^k \cdot g^r = g^r$ und $G = \{g^n \mid n \in \mathbb{Z}\} = \{e, g, ..., g^{m-1}\}$. Die Elemente $e, g, ..., g^{m-1}$ sind alle verschieden, denn aus $g^k = g^l$ für $0 \leq k < l \leq m-1$ folgt $g^{l-k} = e$ mit $1 \leq l - k \leq m - 1$, im Widerspruch zur Definition von m. Damit gilt $|G| = m = o(g)$. □

1.3 Faktorgruppen

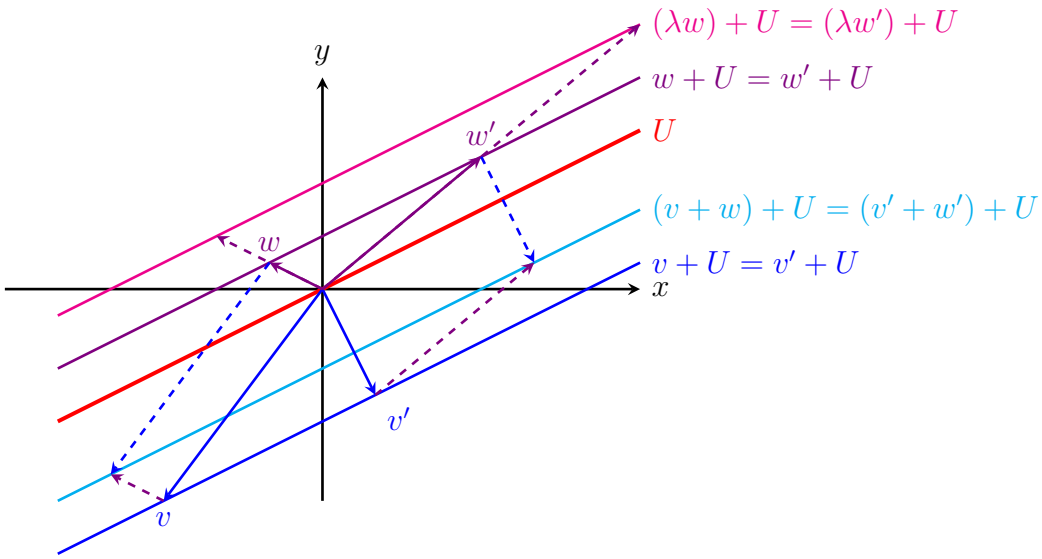
1.3.1 Nebenklassen

Im letzten Abschnitt haben wir gezeigt, dass Untergruppen einige strukturelle Gemeinsamkeiten mit Untervektorräumen aufweisen. Wie auch der Schnitt von Untervektorräumen wieder ein Untervektorraum ist, ist beispielsweise der Schnitt von Untergruppen eine Untergruppe. Ebenso konnten wir die von einer Teilmenge einer Untergruppe erzeugte Untergruppe betrachten, die sich ähnlich verhält wie der von einer Teilmenge eines Vektorraums erzeugte Untervektorraum. In diesem Abschnitt lernen wir eine Konstruktion kennen, die als das Gruppen-Gegenstück von Quotientenräumen aufgefasst werden kann. Wir erinnern an die Konstruktion des Quotientenraums. Sei dazu V ein Vektorraum über einem Körper $\mathbb{K}$ und $U \subseteq V$ ein Untervektorraum.

- Dann erhält man eine Äquivalenzrelation $\sim$ auf V, indem man $v \sim v' \Leftrightarrow v' - v \in U$ setzt.
- Die Äquivalenzklasse eines Vektors $v \in V$ ist der affine Unterraum $v+U = \{v+u \mid u \in U\}$ durch v parallel zu U.
- Die Quotientenmenge V/U ist die Menge der Äquivalenzklassen: $V/U = \{v+U \mid v \in V\}$.
- Sie wird zu einem Vektorraum über $\mathbb{K}$ mit der durch die Repräsentanten definierten Vektoraddition und Skalarmultiplikation

  $$(v+U)+(w+U) = (v+w)+U \qquad \lambda(w+U) = (\lambda w)+U \qquad \forall v, w \in V, \lambda \in \mathbb{K}.$$

  Da die affinen Unterräume auf den rechten Seiten der zwei Ausdrücke nicht von der Wahl der Repräsentanten v, w abhängen, ist die Vektorraumstruktur auf V/U wohldefiniert.



Möchte man eine analoge Konstruktion für eine Gruppe G durchführen, so liegt es nahe statt eines Untervektorraums eine *Untergruppe* $H \subseteq G$ zu betrachten. Anstatt zwei Vektoren als äquivalent zu betrachten, wenn ihre *Differenz* in dem Untervektorraum U enthalten ist, multipliziert man dann ein Gruppenelement mit dem Inversen des anderen und fordert, dass das resultierende Element in H liegt. Dabei hat man nun aber zwei Möglichkeiten: man kann zwei Gruppenelemente $g, g' \in G$ als äquivalent betrachten, wenn $g' \cdot g^{-1} \in H$ gilt oder wenn wenn

$g^{-1} \cdot g' \in H$ gilt. Sie stimmen nur für abelsche Gruppen überein. Für beide Wahlen garantieren aber die Untergruppenaxiome, dass tatsächlich eine Äquivalenzrelation entsteht.

Satz 1.3.1: Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe.

1. Dann sind $g \sim_R g' \Leftrightarrow g'g^{-1} \in H$ und $g \sim_L g' \Leftrightarrow g^{-1}g' \in H$ Äquivalenzrelationen auf G.
2. Die Äquivalenzklassen eines Elements $g \in G$ sind gegeben durch

   $$Hg = \{g' \in G \mid g \sim_R g'\} = \{h \cdot g \mid h \in H\} \qquad gH = \{g' \in G \mid g \sim_L g'\} = \{g \cdot h \mid h \in H\}.$$

   Sie heißen **Rechtsnebenklasse** und **Linksnebenklasse** von H bezüglich g. Die Mengen der Rechts- und Linksnebenklassen werden bezeichnet mit

   $$H\backslash G = \{Hg \mid g \in G\} \qquad G/H = \{gH \mid g \in G\}.$$

Beweis:
Wir beweisen die Aussage für die Äquivalenzrelation $\sim_L$. Der Beweis für $\sim_R$ ist analog (Übung).

• reflexiv: Die Relation $\sim_L$ ist reflexiv, denn nach (UG2) gilt $e = g^{-1}g \in H$ und damit $g \sim_L g$.
• symmetrisch: Ist $g \sim_L g'$, so gilt $g^{-1}g' \in H$. Nach (UG3) ist dann auch $g'^{-1}g = (g^{-1}g')^{-1} \in H$ und damit $g' \sim_L g$.
• transitiv: Ist $g \sim_L g'$ und $g' \sim_L g''$, so gilt $g^{-1}g' \in H$ und $g'^{-1}g'' \in H$. Mit (UG1) folgt $g^{-1}g'' = (g^{-1}g')(g'^{-1}g'') \in H$ und damit $g \sim_L g''$.

Damit ist gezeigt, dass $\sim_L$ eine Äquivalenzrelation ist. Die Äquivalenzklasse eines Elements $g \in G$ ergibt sich direkt aus der Definition

$$\begin{aligned}&\{g' \in G \mid g \sim_L g'\} = \{g' \in G \mid g^{-1}g' \in H\} = \{g' \in G \mid g^{-1}g' = h \text{ für ein } h \in H\} \\ =&\{g' \in G \mid g' = gh \text{ für ein } h \in H\} = \{gh \mid h \in H\} = gH.\end{aligned}$$

□

Bemerkung 1.3.2.

1. Wie jede Äquivalenzrelation definieren die Äquivalenzrelationen $\sim_R$ und $\sim_L$ auf G eine **Partition** von G, also eine Zerlegung von G in paarweise disjunkte, nichtleere Teilmengen. Diese Teilmengen sind gerade die Äquivalenzklassen, also die Nebenklassen. Es gilt:

   $$\begin{array}{lllll} g \sim_R g' & \Leftrightarrow & g' \in Hg & \Leftrightarrow & g \in Hg' \quad \Leftrightarrow \quad Hg = Hg' \\ g \sim_L g' & \Leftrightarrow & g' \in gH & \Leftrightarrow & g \in g'H \quad \Leftrightarrow \quad gH = g'H. \end{array}$$

2. In einer *abelschen* Gruppe G stimmen die Links- und Rechtsnebenklassen überein: $gH = Hg$ für alle $g \in G$ und Untergruppen $H \subseteq G$. Man schreibt dann auch $[g]_H$, $[g]$ oder $g + H$ für die Nebenklasse eines Elements $g \in G$.

Beispiel 1.3.3. Wir betrachten für $n \in \mathbb{N}$ die symmetrische Gruppe $G = S_n$ und die Untergruppe $H = \mathrm{Stab}(k) = \{\pi \in S_n \mid \pi(k) = k\}$ der Permutationen, die ein gegebenes Element und $k \in \{1, ..., n\}$ auf sich selbst abbilden. Dann gilt

$$\begin{aligned}&\pi \sim_L \pi' \Leftrightarrow \pi^{-1} \circ \pi' \in H \Leftrightarrow \pi^{-1} \circ \pi'(k) = k \Leftrightarrow \pi(k) = \pi'(k) \\ &\pi \sim_R \pi' \Leftrightarrow \pi' \circ \pi^{-1} \in H \Leftrightarrow \pi' \circ \pi^{-1}(k) = k \Leftrightarrow \pi^{-1}(k) = \pi'^{-1}(k).\end{aligned}$$

Die Nebenklassen einer Permutation $\pi \in S_n$ sind also gegeben durch

$$\pi H = \{\sigma \in S_n \mid \pi(k) = \sigma(k)\} \qquad H\pi = \{\sigma \in S_n \mid \sigma^{-1}(k) = \pi^{-1}(k)\}.$$

Die Linksnebenklasse enthält also die Permutationen, die das Element k auf dasselbe Element abbilden wie π, und die Rechtsnebenklassen enthält die Permutationen, unter denen das Element k dasselbe Urbild hat wie unter π.

Bevor wir untersuchen können, unter welchen Bedingungen die Mengen $H\backslash G$ und G/H eine Gruppenstruktur tragen, benötigen wir noch ein besseres Verständnis der Nebenklassen. Eine offensichtliche Frage ist, ob und wie sich die Links- und Rechtsnebenklassen einer nicht-abelschen Gruppe zueinander in Beziehung setzen lassen.

In Beispiel 1.3.3 stimmen zwar die Links- und Rechtsnebenklassen nicht überein, aber sie lassen sich ineinander überführen, indem man die Permutation π durch ihr Inverses ersetzt. Da die Inversenbildung die Multiplikationsreihenfolge umdreht und jede Untergruppe in sich selbst überführt, funktioniert dies allgemein, für jede beliebige Gruppe und Untergruppe. Damit wissen wir insbesondere, dass Links- und Rechtsnebenklassen in Bijektion stehen.

Lemma 1.3.4: Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann ist die Abbildung

$$\psi : G/H \to H\backslash G, \quad gH \mapsto Hg^{-1}$$

eine Bijektion zwischen den Mengen G/H und $H\backslash G$.

Beweis:
Zu zeigen ist zunächst, dass ψ wohldefiniert ist, also nicht von der Wahl des Repräsentanten abhängt. Gilt $gH = g'H$, dann ist nach Bemerkung 1.3.2 $g \sim_L g'$, also $g^{-1}g' \in H$. Daraus folgt mit (UG3) auch $(g^{-1}g')^{-1} = g'^{-1}g \in H$, was aber nach Bemerkung 1.3.2 gleichbedeutend ist zu $g^{-1} \sim_R g'^{-1}$, also $Hg^{-1} = Hg'^{-1}$ und $\psi(gH) = \psi(g'H)$. Damit ist ψ wohldefiniert.

Zu zeigen ist noch, dass ψ eine Umkehrabbildung besitzt. Eine offensichtliche Kandidatin ist die Abbildung $\psi' : H\backslash G \to G/H$, $Hg \mapsto g^{-1}H$, deren Wohldefiniertheit man analog zu der von ψ beweist. Tatsächlich ergibt sich für alle $g \in G$

$$\psi' \circ \psi(gH) = \psi'(Hg^{-1}) = (g^{-1})^{-1}H = gH \qquad \psi \circ \psi'(Hg) = \psi(g^{-1}H) = H(g^{-1})^{-1} = Hg.$$

Damit ist ψ bijektiv mit Umkehrabbildung ψ'. □

Definition 1.3.5: Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Die Anzahl der Nebenklassen von H in G heißt **Index** von H in G und wird bezeichnet mit

$$[G : H] := |G/H| = |H\backslash G| \in \mathbb{N} \cup \{\infty\}.$$

Beispiel 1.3.6.

1. Sei $G = S_n$ und $H = \mathrm{Stab}(k) = \{\pi \in S_n \mid \pi(k) = k\}$ die Untergruppe aus Beispiel 1.3.3 mit den Nebenklassen

   $$\pi H = \{\sigma \in S_n \mid \pi(k) = \sigma(k)\} \qquad H\pi = \{\sigma \in S_n \mid \sigma^{-1}(k) = \pi^{-1}(k)\}.$$

   Da eine Permutation $\pi \in S_n$ auf der Zahl k genau n verschiedene Werte annehmen kann und auch genau n Kandidaten für das Urbild $\pi^{-1}(k)$ zur Verfügung stehen, gibt es genau n Linksnebenklassen und genau n Rechtsnebenklassen. Damit ist $[G : H] = n$.

2. Sei $G = \mathbb{Z}$ und $H = n\mathbb{Z} = \langle n \rangle$ die von einer Zahl $n \in \mathbb{N}$ erzeugte Untergruppe. Dann sind die Nebenklassen gegeben durch

$$\bar{z} := z + n\mathbb{Z} = \{w \in \mathbb{Z} \mid w - z \in n\mathbb{Z}\} = \{w \in \mathbb{Z} \mid n \text{ teilt } w - z\}.$$

Es gibt also n Nebenklassen, die den möglichen *Resten* $0, 1, ..., n-1$ einer ganzen Zahl z bei Division durch n entsprechen:

$$\mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}\backslash\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{n-1}\},$$

und damit gilt $[\mathbb{Z} : n\mathbb{Z}] = n$. Da die Nebenklassen in $\mathbb{Z}/n\mathbb{Z}$ den Resten bei der Division durch n entsprechen, nennt man sie auch **Restklassen**. Liegen $w, z \in \mathbb{Z}$ in derselben Restklasse, so nennt man sie **kongruent modulo n** und schreibt $z \equiv w \bmod n$.

Nachdem der Zusammenhang zwischen Links- und Rechtsnebenklassen geklärt ist, ergibt sich auch die Frage nach der Beziehung zwischen den Nebenklassen gH und $g'H$ einer Untergruppe $H \subseteq G$ für verschiedene Elemente in $g, g' \in G$. Man fragt sich beispielsweise, ob die Nebenklassen gH und $g'H$ für $g, g' \in G$ unterschiedlich viele Elemente enthalten können. Wie auch in Beispiel 1.3.6 ist dies generell nicht der Fall. Die Gruppenmultiplikation definiert nämlich Bijektionen zwischen der Untergruppe H und den Linksnebenklassen gH aller Elemente $g \in G$. Eine analoge Aussage gilt für die Rechtsnebenklassen.

Lemma 1.3.7: Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $g \in G$. Dann sind

$$L_g : H \to gH,\ h \mapsto gh \qquad \text{und} \qquad R_g : H \to Hg,\ h \mapsto hg$$

bijektive Abbildungen. Insbesondere gilt $|gH| = |H| = |Hg|$ für alle $g \in G$.

Beweis:
Die Abbildungen L_g und R_g sind surjektiv per Definition der Nebenklassen gH und Hg und injektiv nach der Kürzungsregel, also bijektiv. □

Da jedes Element einer Gruppe G in genau einer (Links-)Nebenklasse der Untergruppe $H \subseteq G$ liegt, können wir mit diesem Lemma eine Beziehung zwischen der Anzahl $[G : H]$ der Nebenklassen, der Gruppenordnung $|G|$ und der Ordnung der Untergruppe $|H|$ herleiten.

Korollar 1.3.8 (Satz von Lagrange): Für jede Gruppe G und Untergruppe $H \subseteq G$ gilt:

$$|G| = [G : H] \cdot |H|.$$

Insbesondere ist für endliche Gruppen G die Ordnung von H ein Teiler der Ordnung von G.

Beweis:
Die Gruppe G ist die disjunkte Vereinigung ihrer $[G : H]$ Linksnebenklassen, und jede Linksnebenklasse hat nach Lemma 1.3.7 die Mächtigkeit $|H|$. Damit gilt $|G| = [G : H] \cdot |H|$. □

Man beachte, dass die Formel im Satz von Lagrange und das Argument in seinem Beweis auch für unendliche Gruppen G Sinn ergeben. In diesem Fall steht auf beiden Seiten ∞, und die Formel besagt, dass die Untergruppe H unendlich ist oder unendlich viele Nebenklassen existieren. Wirklich nützlich ist der Satz von Lagrange jedoch nur für *endliche* Gruppen.

Korollar 1.3.9: Sei G eine endliche Gruppe. Dann teilt die Ordnung jedes Elements $g \in G$ die Gruppenordnung: $\mathrm{ord}(g) \,|\, |G|$.

Beweis:
Wir betrachten die von einem Element $g \in G$ erzeugte Untergruppe $H = \langle g \rangle$. Dann gilt nach Korollar 1.2.20 $o(g) = |\langle g \rangle| = |H|$, und mit dem Satz von Lagrange folgt $|G| = [G : H] \cdot o(g)$. □

Korollar 1.3.10: Sei G eine endliche Gruppe, deren Ordnung eine Primzahl p ist. Dann hat G nur zwei Untergruppen, nämlich $\{e\}$ und G, und jedes Element $g \neq e$ hat Ordnung $o(g) = p$. Insbesondere ist jede Gruppe von Primzahlordnung zyklisch.

Beweis:
Nach dem Satz von Lagrange gilt $p = |G| = |H| \cdot [G : H]$ für jede Untergruppe $H \subseteq G$, und damit muss $|H|$ ein Teiler von p sein. Da p eine Primzahl ist, folgt $|H| = p$ und $H = G$ oder $|H| = 1$ und $H = \{e\}$. Damit gilt auch $\langle g \rangle = \{e\}$ oder $\langle g \rangle = G$ für jedes Element $g \in G$. Im ersten Fall ist $g = e$, im zweiten gilt $o(g) = p$ nach Korollar 1.2.20. □

1.3.2 Normalteiler und Faktorgruppen

Wir versuchen nun in Analogie zur Konstruktion des Quotientenraums, eine Gruppenstruktur auf der Menge der Linksnebenklassen einer Untergruppe $H \subseteq G$ zu definieren. Die einzig sinnvolle Strategie ist es dabei, die Gruppenstruktur über die Repräsentanten zu definieren, also $(g_1 H) \cdot (g_2 H) = (g_1 g_2) H$ für $g_1, g_2 \in G$ zu setzen. Es zeigt sich jedoch schnell, dass dies für nichtabelsche Gruppen nicht ohne Weiteres funktioniert, denn die rechte Seite der Gleichung hängt von der Wahl der Repräsentanten ab. Gilt $g_1' \in g_1 H$ so gibt es zwar ein Element $h \in H$ mit $g_1' = g_1 h$, aber das impliziert nur $g_1' g_2 = g_1 h g_2$ und nicht $g_1' g_2 \in (g_1 g_2) H$. Damit die Multiplikation wohldefiniert ist, muss $h g_2 \in g_2 H$ oder, dazu äquivalent, $g_2^{-1} h g_2 \in H$ für alle $h \in H$ und $g_2 \in G$ gelten. Man erhält also eine Bedingung an die Untergruppe $H \subseteq G$.

Definition 1.3.11: Sei G eine Gruppe. Eine Untergruppe $N \subseteq G$ heißt **Normalteiler** von G oder **normal** in G, falls $gng^{-1} \in N$ für alle $n \in N$ und $g \in G$ gilt. Man schreibt auch $N \trianglelefteq G$.

Beispiel 1.3.12.

1. Die triviale Untergruppe $\{e\}$ und G selbst sind immer Normalteiler in G.
2. Ist G abelsch, so ist jede Untergruppe $N \subseteq G$ ein Normalteiler, denn es gilt $gng^{-1} = n$ für alle $g, n \in G$.
3. Für jede Gruppe G sind das Zentrum $Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$ und jede Untergruppe $H \subseteq Z(G)$ Normalteiler von G, denn es gilt $hgh^{-1} = g \in Z(G)$ für alle $h \in G$, $g \in Z(G)$.
4. Für jede Gruppe G ist die Untergruppe $\mathrm{Inn}(G)$ der inneren Automorphismen aus Beispiel 1.2.5 ein Normalteiler der Automorphismengruppe $\mathrm{Aut}(G)$.

Denn die Gruppe $\mathrm{Inn}(G)$ enthält die Konjugationsabbildungen $C_g : G \to G$, $h \mapsto ghg^{-1}$ für alle Elemente $g \in G$. Für jeden Automorphismus $\psi \in \mathrm{Aut}(G)$ und alle $g, h \in G$ gilt

$$\psi \circ C_g \circ \psi^{-1}(h) = \psi(g \cdot \psi^{-1}(h) \cdot g^{-1}) = \psi(g) \cdot \psi(\psi^{-1}(h)) \cdot \psi(g^{-1}) = \psi(g) \cdot h \cdot \psi(g)^{-1} = C_{\psi(g)}(h).$$

Damit ist $\psi^{-1} \circ C_g \circ \psi^{-1} = C_{\psi(g)} \in \mathrm{Inn}(G)$ für alle $\psi \in \mathrm{Aut}(G)$ und $g \in G$.

5. Die Untergruppe $R = \{R(\frac{2\pi k}{n}) \mid k = 0, 1, ..., n-1\} = \langle R(\frac{2\pi}{n}) \rangle$ der Drehungen ist ein Normalteiler in der Diedergruppe D_n aus Beispiel 1.2.15. Die von der Spiegelung an der x-Achse erzeugte Untergruppe $S = \langle S(0) \rangle$ ist nicht normal in D_n. (Übung).

Es kann natürlich vorkommen, dass eine Gruppe G außer der trivialen Untergruppe und sich selbst keine Normalteiler besitzt. Dies ist beispielsweise für endliche Gruppen von Primzahlordnung der Fall, die ja nach Korollar 1.3.10 nur die triviale Untergruppe und sich selbst als Untergruppen und damit auch keine weiteren Normalteiler haben. Allgemein bezeichnet man eine nichttriviale Gruppe G, die nur die Normalteiler $\{e\}$ und G besitzt, als *einfache Gruppe*, da sie eine einfachere Struktur hat als Gruppen mit weiteren Normalteilern. Für die triviale Gruppe fallen $\{e\}$ und G zusammen, und man fasst sie daher nicht als einfache Gruppe auf.

Definition 1.3.13: Eine Gruppe G heißt **einfach**, wenn $G \neq \{e\}$ gilt und G und $\{e\}$ die einzigen Normalteiler von G sind.

Wir zeigen nun, dass die Bedingung, dass $N \subseteq G$ ein Normalteiler ist, hinreichend ist, um eine Gruppenstruktur auf der Menge G/N der Linksnebenklassen zu erhalten. Dazu definieren wir die Multiplikation über die Repräsentanten und weisen nach, dass sie wohldefiniert ist, also nicht von der Wahl der Repräsentanten abhängt. Dass die Gruppenaxiome erfüllt sind, ergibt sich dann direkt aus den Gruppenaxiomen für G.

Satz 1.3.14: Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler. Dann gilt:

1. Die Menge G/N der Linksnebenklassen mit der Verknüpfung $gN \cdot hN = (gh)N$ ist eine Gruppe mit neutralem Element N, die **Faktorgruppe** von G bezüglich N.
2. Die Abbildung $\pi_N : G \to G/N$, $g \mapsto gN$, die jedem Gruppenelement seine Nebenklasse zuordnet, ist ein surjektiver Gruppenhomomorphismus mit Kern $\ker(\pi_N) = N$. Sie heißt **kanonische Surjektion**.

Beweis:
1. Wir zeigen zunächst, dass die Verknüpfung wohldefiniert ist. Seien dazu $g, g', h, h' \in G$ mit $g'N = gN$ und $h'N = hN$. Dann gibt es Elemente $n, m \in N$ mit $g' = gn$ und $h' = hm$. Da N ein Normalteiler ist und $n \in N$, gilt $h^{-1}nh \in N$. Da N eine Untergruppe ist, folgt

$$g'h' = gnhm = g(hh^{-1})nhm = (gh)(h^{-1}nh)m \in (gh)N \quad \Rightarrow \quad (gh)N = (g'h')N.$$

Damit ist die Verknüpfung wohldefiniert. Ihre Assoziativität folgt direkt aus der Assoziativität der Gruppenmultiplikation in G:

$$(gN \cdot hN) \cdot kN = (gh)N \cdot kN = ((gh)k)N = (g(hk))N = gN \cdot ((hk)N) = gN \cdot (hN \cdot kN)$$

für alle $g, h, k \in G$. Die Nebenklasse $eN = N$ ist das neutrale Element, denn

$$N \cdot gN = eN \cdot gN = (eg)N = gN = (ge)N = gN \cdot eN = gN \cdot N.$$

Die Nebenklasse $g^{-1}N$ ist invers zu gN, denn

$$g^{-1}N \cdot gN = (g^{-1}g)N = eN = N = (gg^{-1})N = gN \cdot g^{-1}N.$$

2. Per Definition der Verknüpfung auf G/N gilt $\pi_N(g) \cdot \pi_N(h) = gN \cdot hN = (gh)N = \pi_N(gh)$ für alle $g, h \in G$, und damit ist π_N ein Gruppenhomomorphismus. Er ist offensichtlich surjektiv, und es gilt $\ker(\pi_N) = \{g \in G \mid \pi_N(g) = N\} = \{g \in G \mid gN = N\} = N$. □

Beispiel 1.3.15.

1. Nach Beispiel 1.3.12 sind die triviale Gruppe $\{e\}$ und G selbst in Normalteiler in G. Die zugehörigen Faktorgruppen sind die Gruppen $G = G/\{e\}$ und $\{e\} = G/G$.

2. Die Untergruppe $n\mathbb{Z} \subseteq \mathbb{Z}$ ist ein Normalteiler, denn $\mathbb{Z}$ ist abelsch. Die Menge der Nebenklassen ist $\mathbb{Z}/n\mathbb{Z} = \{\bar{z} \mid z \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$ mit $\bar{z} := z + n\mathbb{Z}$ (vgl. Beispiel 1.3.6, 2). Die Verknüpfung auf $\mathbb{Z}/n\mathbb{Z}$ ist nach Satz 1.3.14 gegeben durch

   $$\bar{k} + \bar{l} = \overline{k+l} \qquad \forall k, l \in \mathbb{Z}.$$

   Es handelt sich um eine zyklische Gruppe der Ordnung n, die von $\bar{1} \in \mathbb{Z}/n\mathbb{Z}$ erzeugt wird.

Da Normalteiler es uns erlauben, durch Quotientenbildung neue Gruppen zu konstruieren, lohnt es sich, die Eigenschaften von Normalteilern genauer zu untersuchen. Zunächst stellen wir fest, dass die Normalteiler genau die Untergruppen einer Gruppe G sind, für die Links- und Rechtsnebenklassen und die zugehörigen Äquivalenzrelationen übereinstimmen. Wir benötigen also kein zweite Version von Satz 1.3.14 für die Rechtsnebenklassen.

Lemma 1.3.16: Für eine Untergruppe $N \subseteq G$ einer Gruppe G sind äquivalent:

(i) N ist ein Normalteiler in G.
(ii) $N = gNg^{-1} = \{gng^{-1} \mid n \in N\}$ für alle $g \in G$.
(iii) Links- und Rechtsnebenklasse jedes Elements stimmen überein: $gN = Ng \; \forall g \in G$.
(iv) Die Äquivalenzrelationen $\sim_L$ und $\sim_R$ stimmen überein.

Beweis:
(i) ⇔ (ii): Offensichtlich gilt (ii)⇒(i), denn (i) ist gleichbedeutend zu $gNg^{-1} \subseteq N$ für alle $g \in G$. Gilt (i), so gibt es zu jedem Element $n \in N$ und zu jedem $g \in G$ ein Element $n' = g^{-1}ng \in N$ mit $n = gn'g^{-1}$ und damit $gNg^{-1} = N$.
(ii) ⇔ (iii): Für alle $g \in G$ gilt $gNg^{-1} = N$ genau dann wenn $gN = (gNg^{-1})g = Ng$.
(iii) ⇔ (iv): Da die Links- und Rechtsnebenklassen die Äquivalenzklassen der Äquivalenzrelationen $\sim_L$ und $\sim_R$ sind, stimmen die Links- und Rechtsnebenklassen aller Elemente überein genau dann, wenn die Äquivalenzrelationen gleich sind. □

Eine weitere Eigenschaft, die Normalteiler auszeichnet, ist, dass Produkte aus Elementen eines Normalteilers und Elementen einer Untergruppe von G wieder eine Untergruppe bilden. Für zwei *Untergruppen* $H_1, H_2 \subseteq G$ müssen die Mengen $H_1H_2 := \{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$ und $H_2H_1 := \{h_2h_1 \mid h_1 \in H_1, h_2 \in H_2\}$ weder übereinstimmen noch Untergruppen von G sein. Ist aber eine der beteiligten Untergruppen ein *Normalteiler*, so ist dies der Fall.

Lemma 1.3.17: Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler in G. Dann ist $HN = NH$ eine Untergruppe von G.

Beweis:
Nach Lemma 1.3.16 gilt $gN = Ng$ für alle $g \in G$ und damit $HN = NH$. Die Teilmenge $HN = NH$ ist eine Untergruppe von G, denn es gilt $e = ee \in H \cdot N$ (UG2) und für alle $h_1, h_2 \in H$ und $n_1, n_2 \in N$

$$(h_1n_1) \cdot (h_2n_2) = h_1(h_2h_2^{-1})(n_1h_2n_2) = (h_1h_2)(h_2^{-1}n_1h_2)n_2 \in H \cdot N \qquad \text{(UG1)}$$
$$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1} = (h_1^{-1}h_1)(n_1^{-1}h_1^{-1}) = h_1^{-1}(h_1n_1^{-1}h_1^{-1}) \in H \cdot N \qquad \text{(UG3).}$$

Denn da H eine Untergruppe ist, folgt $h_1h_2, h_1^{-1} \in H$ und da N ein Normalteiler ist, gilt $h_1^{-1}n_1h_1 \in N$, $h_2^{-1}n_1h_2 \in N$ und damit auch $(h_2^{-1}n_1h_2)n_2 \in N$. □

In Satz 1.3.14 wurde gezeigt, dass jeder Normalteiler Kern eines Gruppenhomomorphismus ist, nämlich der Kern der zugehörigen kanonischen Surjektion. Wir zeigen, dass auch umgekehrt jeder Kern eines Gruppenhomomorphismus ein Normalteiler ist. Normalteiler sind also genau die Untergruppen, die sich als Kern eines Gruppenhomomorphismus schreiben lassen. Bilder von Normalteilern sind nicht notwendigerweise Normalteiler. Hier benötigt man die zusätzliche Forderung, dass der Gruppenhomomorphismus *surjektiv* ist.

Lemma 1.3.18: Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:

1. Das Urbild $f^{-1}(N)$ eines Normalteilers $N \subseteq H$ ist ein Normalteiler in G.
2. Ist f surjektiv, so ist das Bild $f(M)$ jedes Normalteilers $M \subseteq G$ ein Normalteiler in H.
3. Insbesondere ist $\ker(f) = f^{-1}(\{e_H\})$ ein Normalteiler in G.

Beweis:
1. Sei $N \subseteq H$ ein Normalteiler und $m \in f^{-1}(N) \subseteq G$. Dann ist $f(m) \in N$, und für alle $g \in G$ gilt $f(gmg^{-1}) = f(g)f(m)f(g)^{-1} \in N$, also $gmg^{-1} \in f^{-1}(N)$. Damit ist $f^{-1}(N) \subseteq G$ ein Normalteiler.

2. Sei nun f surjektiv und $M \subseteq G$ ein Normalteiler. Dann gibt es zu jedem $h \in H$ ein $g \in G$ mit $h = f(g)$. Da M ein Normalteiler in G ist, folgt $gmg^{-1} \in M$ für alle $m \in M$ und damit $hf(m)h^{-1} = f(g)f(m)f(g)^{-1} = f(gmg^{-1}) \in f(M)$ für alle $h \in H$, $m \in M$. Damit ist $f(M)$ normal in H.

3. Die Aussage folgt, indem man 1. auf den Normalteiler $\{e_H\} \subseteq H$ anwendet. □

Der Beweis von Lemma 1.3.18, 2. zeigt, dass das Bild $f(N)$ eines Normalteilers $N \subseteq G$ unter einem Gruppenhomomorphismus $f : G \to H$ zwar im allgemeinen kein Normalteiler in H, aber sehr wohl ein Normalteiler in der Untergruppe $f(G) \subseteq H$ ist. Denn für jeden Gruppenhomomorphismus $f : G \to H$ ist die Koeinschränkung $f : G \to f(G)$, $g \mapsto f(g)$ ein surjektiver Gruppenhomomorphismus. Indem wir Lemma 1.3.18 mit den Aussagen für Untergruppen in Lemma 1.2.8 kombinieren, erhalten wir dann den folgenden Satz, der die Ergebnisse zum Verhalten von Untergruppen und Normalteilern unter Gruppenhomomorphismen zusammenfasst.

Satz 1.3.19 (Untergruppenkorrespondenz):
Für jeden Gruppenhomomorphismus $f : G \to H$ ist die Abbildung

$$\varphi_f : \{\text{Untergruppen } U \subseteq G \text{ mit } \ker f \subseteq U\} \to \{\text{Untergruppen von } f(G)\},\ U \mapsto f(U)$$

eine Bijektion mit Inversem

$$\varphi_f^{-1} : \{\text{Untergruppen von } f(G)\} \to \{\text{Untergruppen } U \subseteq G \text{ mit } \ker f \subseteq U\},\ V \mapsto f^{-1}(V).$$

Eine Untergruppe $U \subseteq G$ mit $\ker f \subseteq U$ ist genau dann normal in G, wenn $\varphi_f(U)$ normal in $f(G)$ ist.

Beweis:
Die Abbildungen φ_f und φ_f^{-1} sind wohldefiniert, denn für jede Untergruppe $U \subseteq G$ ist nach Lemma 1.2.8 das Bild $f(U) \subseteq H$ eine Untergruppe von H mit $f(U) \subseteq f(G)$, und für jede Untergruppe $V \subseteq f(G)$ ist das Urbild $f^{-1}(V) \subseteq V$ nach Lemma 1.2.8 eine Untergruppe von G mit $f^{-1}(V) \supseteq f^{-1}(e_H) = \ker f$. Die Abbildungen φ_f und φ_f^{-1} sind zueinander invers, denn es gilt $\varphi_f(\varphi_f^{-1}(V)) = \{f(g) \mid g \in f^{-1}(V)\} = V$ für alle Untergruppen $V \subseteq f(G)$. Ebenso ergibt sich für alle Untergruppen $U \subseteq G$ mit $\ker f \subseteq U$

$$\begin{aligned}
&\varphi_f^{-1}(\varphi_f(U)) = \{g \in G \mid f(g) \in f(U)\} = \{g \in G \mid \exists u \in U : f(g) = f(u)\} \\
&= \{g \in G \mid \exists u \in U : f(u^{-1}g) = f(u)^{-1}f(g) = e_H\} = \{g \in G \mid \exists u \in U : u^{-1}g \in \ker f\} \\
&= \{u \cdot n \mid u \in U, n \in \ker f \subseteq U\} = U.
\end{aligned}$$

Da die Koeinschränkung $f : G \to f(G),\ g \mapsto f(g)$ surjektiv ist, ist nach Lemma 1.3.18 das Bild $f(U)$ jeder normalen Untergruppe $U \subseteq G$ normal in $f(G)$ und das Urbild jeder normalen Untergruppe $V \subseteq f(G)$ normal in G. □

Korollar 1.3.20: Sei N ein Normalteiler der Gruppe G. Dann stehen die Untergruppen (Normalteiler) von G/N in Bijektion mit den Untergruppen (Normalteilern) von G, die N enthalten.

Beweis:
Dies folgt, indem wir Satz 1.3.19 anwenden auf die kanonische Surjektion $f = \pi_N : G \to G/N$ aus Satz 1.3.14. □

Korollar 1.3.20 erlaubt es uns, Untergruppen und Normalteiler einer Faktorgruppe G/N durch Untergruppen und Normalteiler der Gruppe G zu beschreiben. Auf ähnliche Weise lassen sich auch Gruppenhomomorphismen aus der Faktorgruppe G/N in eine beliebige Gruppe H durch Gruppenhomomorphismen von G nach H beschreiben, deren Kern den Normalteiler N enthält.

Satz 1.3.21: Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler. Dann gibt es zu jedem Gruppenhomomorphismus $f : G \to H$ mit $N \subseteq \ker f$ genau einen Gruppenhomomorphismus $f/N : G/N \to H$ mit $f/N \circ \pi_N = f$, nämlich

$$f/N : G/N \to H, \quad gN \mapsto f(g).$$

Dies bezeichnet man als die **charakteristische Eigenschaft** der Faktorgruppe.

Beweis:
Sei $f : G \to H$ ein Gruppenhomomorphismus mit $N \subseteq \ker f$. Ist $f' : G/N \to H$ ein Gruppenhomomorphismus mit $f' \circ \pi_N = f$, so ist f' wegen der Surjektivität von π_N eindeutig bestimmt. Denn $f' \circ \pi_N = f$ impliziert $f'(gN) = f' \circ \pi_N(g) = f(g)$ für alle $g \in G$, also $f' = f/N : G/N \to H$, $gN \mapsto f(g)$. Zu zeigen ist noch, dass $f' = f/N$ wohldefiniert und mit der Gruppenmultiplikation verträglich ist. Gilt $gN = g'N$, so gibt es ein $n \in N$ mit $g' = gn$. Daraus folgt $f'(g'N) = f(g') = f(gn) = f(g)f(n) = f(g)e_H = f(g) = f'(gN)$, denn aus $N \subseteq \ker f$ folgt $f(n) = e_H$ für alle $n \in N$. Per Definition der Verknüpfung auf G/N gilt

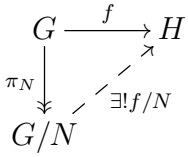
$$f'(gN \cdot hN) = f'(ghN) = f(gh) = f(g)f(h) = f'(gN) \cdot f'(hN),$$

und damit ist f' ein Gruppenhomomorphismus. □

Bemerkung 1.3.22.

1. Fordert man in Satz 1.3.21 nur, dass $N \subseteq G$ eine *Untergruppe* ist, so erhält man immer noch eine surjektive *Abbildung* $\pi_N : G \to G/N$, und zu jedem Gruppenhomomorphismus $f : G \to H$ mit $N \subseteq \ker f$ gibt es genau eine *Abbildung* $f/N : G/N \to H$ mit $f/N \circ \pi_N = f$, nämlich $f/N : G/N \to H$, $gN \mapsto f(g)$.

2. Man sagt, dass der Gruppenhomomorphismus $f : G \to H$ mit $\ker f \supseteq N$ über π_N **faktorisiert** und beschreibt die Situation oft durch ein kommutatives Diagramm, in dem die Surjektivität von π_N durch einen Pfeil mit zwei Spitzen angedeutet wird



Satz 1.3.21 erlaubt es einem, Gruppenhomomorphismen $f' : G/N \to H$ aus einer Faktorgruppe durch Gruppenhomomorphismen $f : G \to H$ zu ersetzen, deren Kern den Normalteiler N enthält. Dies erspart einem viel umständliches Rechnen mit Äquivalenzrelationen und Nebenklassen. Um einen Gruppenhomomorphismus $f' : G/N \to H$ zu konstruieren, muss man nur einen Gruppenhomomorphismus $f : G \to H$ mit $N \subseteq \ker(f)$ finden und kann dann $f' = f/N : G/N \to H$, $gN \mapsto f(g)$ setzen. Satz 1.3.21 erspart es einem also, die Wohldefiniertheit von f' und die Verträglichkeit mit der Gruppenmultiplikation nachzurechnen.

Natürlich kann man Satz 1.3.21 auch auf den Kern eines gegebenen Gruppenhomomorphismus $f : G \to H$ anwenden, der ja nach Lemma 1.3.18 immer ein Normalteiler ist. Dies liefert die Faktorgruppe $G/\ker(f)$ und einen Gruppenhomomorphismus $f/\ker(f) : G/\ker(f) \to H$. Da hier gerade der Kern von f aus der Gruppe G herausgeteilt wurde, ist dieser injektiv. Wir erhalten den berühmten Homomorphiesatz der Erlanger Mathematikerin *Emmy Noether*.

Satz 1.3.23 (Noetherscher Homomorphiesatz):

Für jeden Gruppenhomomorphismus $f : G \to H$ ist die Abbildung

$$f/\ker(f) : G/\ker(f) \to H,\ g\ker f \mapsto f(g)$$

ein injektiver Gruppenhomomorphismus, also ein Isomorphismus auf ihr Bild.

Beweis:
Wir wenden Satz 1.3.21 auf den Normalteiler $\ker(f) \subseteq G$ an. Die liefert einen Gruppenhomomorphismus $f/\ker(f) : G/\ker(f) \to H$. Sein Kern ist

$$\ker(f/\ker(f)) = \{g\ker(f) \mid f(g) = e_H\} = \{g\ker(f) \mid g \in \ker(f)\} = \ker(f).$$

Also ist $f/\ker(f)$ injektiv mit Bild $f(G)$. Man erhält einen Isomorphismus

$$f/\ker(f) : G/\ker(f) \to f(G), \quad g\ker(f) \mapsto f(g).$$

□

Der Noethersche Homomorphiesatz ist sehr nützlich, um zu beweisen, dass eine Faktorgruppe G/N zu einer anderen Gruppe H isomorph ist. Dazu muss man lediglich einen surjektiven Gruppenhomomorphismus $f : G \to H$ mit $\ker(f) = N$ finden.

Beispiel 1.3.24.

1. Aus den Additionsformeln für Sinus und Kosinus folgt, dass die Abbildung

$$R : (\mathbb{R}, +) \to \mathrm{GL}(2, \mathbb{R}), \quad \varphi \mapsto R(\varphi) = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

   ein Gruppenhomomorphismus ist. Ihr Bild ist die Gruppe $\mathrm{SO}(2, \mathbb{R})$ aus Beispiel 1.2.10. Da $R(\varphi) = \mathbb{1}_2$ genau dann, wenn $\varphi \in 2\pi\mathbb{Z}$, ist ihr Kern die Untergruppe $2\pi\mathbb{Z} \subseteq \mathbb{R}$. Der Homomorphiesatz liefert dann einen Isomorphismus

$$R/\ker(R) : \mathbb{R}/2\pi\mathbb{Z} \to \mathrm{SO}(2, \mathbb{R}), \quad \varphi + 2\pi\mathbb{Z} \mapsto R(\varphi).$$

2. Betrachtet man stattdessen den surjektiven Gruppenhomomorphismus

$$R' : (\mathbb{R}, +) \to S^1, \quad \varphi \mapsto e^{\mathrm{i}\varphi}$$

   mit der multiplikativen Gruppe $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ und $\ker(R') = 2\pi\mathbb{Z}$, so erhält man einen Isomorphismus

$$R'/\ker(R') : \mathbb{R}/2\pi\mathbb{Z} \to S^1, \quad \varphi + 2\pi\mathbb{Z} \mapsto e^{2\pi\mathrm{i}z}.$$

3. Wir betrachten die Abbildung

$$\exp : \mathbb{C} \to \mathbb{C}^\times, \quad x + \mathrm{i}y \mapsto e^{x+\mathrm{i}y} = e^x \cdot e^{\mathrm{i}y} = e^x(\cos(y) + \mathrm{i}\sin(y)).$$

   Da die Exponentialabbildung die Bedingung $\exp(z+z') = \exp(z)\cdot\exp(z')$ für alle $z, z' \in \mathbb{C}$ erfüllt, ist sie ein Gruppenhomomorphismus von $(\mathbb{C}, +)$ nach $(\mathbb{C}^\times, \cdot)$. Da sich jedes $z \in \mathbb{C}^\times$ schreiben lässt als $z = e^x(\cos(y) + \mathrm{i}\sin(y))$ mit $x = \log|z|$, $\cos(y) = \mathrm{Re}(z)/|z|$ und $\sin(y) = \mathrm{Im}(z)/|z|$, ist sie surjektiv. Ihr Kern ist $\ker(\exp) = \exp^{-1}(1) = 2\pi\mathrm{i}\mathbb{Z}$. Der Homomorphiesatz liefert dann einen Gruppenisomorphismus

$$\exp/\ker(\exp) : \mathbb{C}/2\pi i\mathbb{Z} \to \mathbb{C}^\times.$$

4. Für $n \in \mathbb{N}$ erhalten wir einen Gruppenhomomorphismus $f : \mathbb{Z} \to S^1$, $z \mapsto e^{2\pi\mathrm{i}z/n}$ mit Bild $f(\mathbb{Z}) = C_n = \{e^{2\pi\mathrm{i}k/n} \mid k \in \mathbb{Z}\}$ und $\ker(f) = n\mathbb{Z}$. Der Isomorphiesatz liefert dann einen Gruppenisomorphismus $f : \mathbb{Z}/n\mathbb{Z} \to C_n$, $\bar{k} \mapsto e^{2\pi\mathrm{i}k/n}$.

Beispiel 1.3.25. Sei G eine Gruppe und $\mathrm{Inn}(G)$ die Gruppe der inneren Automorphismen $C_g : G \to G$, $h \mapsto ghg^{-1}$ aus Beispiel 1.2.5. Die Abbildung

$$C : G \to \mathrm{Inn}(G), \quad g \mapsto C_g$$

ist ein surjektiver Gruppenhomomorphismus, denn es gilt für alle $g, h, k \in G$

$$C_{gh}(k) = (gh)k(gh)^{-1} = g(hkh^{-1})g^{-1} = C_g \circ C_h(k).$$

Der Kern des Gruppenhomomorphismus C ist das Zentrum von G:

$$\ker(C) = \{g \in G \mid C_g = \mathrm{id}_G\} = \{g \in G \mid C_g(h) = ghg^{-1} = h \ \forall h \in G\} = Z(G).$$

Aus Satz 1.3.23 erhält man dann einen Gruppenisomorphismus

$$C/\ker(C) : G/Z(G) \to \mathrm{Inn}(G), \quad gZ(G) \mapsto C_g.$$

Es gibt noch zwei weitere Noethersche Sätze zu Faktorgruppen, die beiden Noetherschen Isomorphiesätze. Sie sind sind im Wesentlichen Spezialfälle oder Iterationen des Noetherschen Homomorphiesatzes und beschreiben Doppelquotienten von Gruppen und Quotienten bezüglich Schnitten von Normalteilern mit Untergruppen.

Satz 1.3.26 (1. Noetherscher Isomorphiesatz):

Sei G eine Gruppe und $K, N \subseteq G$ Normalteiler von G mit $N \subseteq K$. Dann gilt:

1. K/N ist ein Normalteiler der Gruppe G/N.
2. Es gibt einen kanonischen Isomorphismus $\varphi : (G/N)/(K/N) \to G/K$, $(gN)(K/N) \mapsto gK$.

Beweis:
Wir betrachten den surjektiven Gruppenhomomorphismus $\pi_K : G \to G/K$, $g \mapsto gK$ aus Satz 1.3.21. Da $N \subseteq K = \ker(\pi_K)$ gilt, erhalten wir aus Satz 1.3.21 einen Gruppenhomomorphismus $\pi_K/N : G/N \to G/K$, $gN \mapsto gK$. Da $(\pi_K/N)(G/N) = \pi_K(G) = G/K$ ist er surjektiv, und es gilt $\ker(\pi_K/N) = \{gN \mid g \in K\} = K/N$. Nach Lemma 1.3.18 ist K/N damit ein Normalteiler in G/N. Anwendung des Homomorphiesatzes 1.3.23 auf den surjektiven Gruppenhomomorphismus π_K/N liefert nun einen Gruppenisomorphismus

$$\varphi = (\pi_K/N)/(K/N) : (G/N)/(K/N) \to G/K : (gN)(K/N) \mapsto gK.$$

□

Satz 1.3.27 (2. Noetherscher Isomorphiesatz): Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler. Dann ist $H \cap N$ normal in H, N normal in HN, und es gibt einen kanonischen Gruppenisomorphismus

$$\varphi : H/(H \cap N) \to (HN)/N, \quad h(H \cap N) \mapsto hN.$$

Beweis:
Wir wenden den Homomorphiesatz 1.3.23 auf die Einschränkung von π_N auf H an:

$$f := \pi_N|_H : H \to G/N, \ h \mapsto hN.$$

Dies ist ein Gruppenhomomorphismus mit $\ker f = \{h \in H \mid hN = N\} = H \cap \ker \pi_N = H \cap N$, und damit ist $H \cap N$ nach Lemma 1.3.18 normal in H. Die Menge $HN \subseteq G$ ist eine Untergruppe nach Lemma 1.3.17, und da N normal in G ist, ist N auch normal in HN. Das Bild von f ist

$$f(H) = \{hN \mid h \in H\} = HN/N,$$

und der Homomorphiesatz 1.3.23 liefert einen Isomorphismus auf das Bild

$$\varphi = f/\ker(f) : H/(H \cap N) \to (HN)/N, \quad h(H \cap N) \mapsto hN. \qquad \square$$

Eine Gedenktafel für Emmy Noether in Hörsaal H12 enthält den Noetherschen Homomorphiesatz und die zwei Noetherschen Isomorphiesätze, wenn auch in einer anderen Notation. Die Bezeichnung der Isomorphiesätze in diesem Skript folgt der Originalarbeit von Emmy Noether „Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern“ von 1927. Der größte Teil der Literatur hält sich jedoch nicht daran. In gängigen Lehrbüchern findet man die folgenden Bezeichnungen:

Noether	Karpfinger-Meyberg	Fischer
Homomorphiesatz	Homomorphiesatz	1. Isomorphiesatz
1. Isomorphiesatz	2. Isomorphiesatz	3. Isomorphiesatz
2. Isomorphiesatz	1. Isomorphiesatz	2. Isomorphiesatz

1.4 Semidirekte Produkte

Nachdem wir uns im letzten Abschnitt mit Faktorgruppen beschäftigt haben, untersuchen wir nun den Zusammenhang zwischen Faktorgruppen und Produkten von Untergruppen. Ausgangspunkt ist eine Beobachtung aus der linearen Algebra. Betrachtet man einen Quotientenraum V/U für einen Untervektorraum $U \subseteq V$, so gibt es immer ein sogenanntes *Komplement* zu U, also einen Untervektorraum $W \subseteq V$ mit $V = U \oplus W$, und es gilt $V/U \cong W$. Man kann es also vermeiden mit dem Quotienten V/U zu arbeiten, indem man ein Komplement von U wählt. Der Preis dieser Strategie sind willkürliche Wahlen und eine kompliziertere, uneindeutige Beschreibung, denn U besitzt im Allgemeinen viele verschiedene Komplemente.

Versucht man, für Gruppen analog vorzugehen, könnte man ein Komplement eines Normalteilers $N \subseteq G$ definieren als eine Untergruppe $H \subseteq G$ mit $H \cap N = \{e\}$ und $NH = G$, was den Forderungen $U \cap W = \{0\}$ und $U + W = V$ für das Komplement eines Untervektorraums U entspricht. Man könnte dann versuchen die Faktorgruppe G/N durch diese Gruppe H zu ersetzen, also die Gruppe G durch den Normalteiler N und die Gruppe H zu beschreiben. Im Gegensatz zu den Vektorräumen, ist dabei jedoch zunächst unklar, wie die Gruppen H und N interagieren sollen. Wir werden auch sehen, dass Untergruppen $H \subseteq G$ mit $H \cap N = \{e\}$ und $NH = G$ nicht für jeden Normalteiler $N \subseteq G$ existieren. Falls eine solche Untergruppe H existiert, ist G ein sogenanntes *semidirektes Produkt*. Wir definieren das zunächst abstrakt und untersuchen anschließend den Zusammenhang mit Normalteilern und Faktorgruppen.

Satz 1.4.1: Seien G, H Gruppen und $\varphi : G \to \mathrm{Aut}(H)$, $g \mapsto \varphi_g$ ein Gruppenhomomorphismus. Dann ist die Menge $H \times G$ eine Gruppe mit der Verknüpfung

$$(h_1, g_1) \cdot_\varphi (h_2, g_2) := (h_1 \varphi_{g_1}(h_2), g_1 g_2).$$

Sie wird als das **(äußere) semidirekte Produkt** von G und H und mit $H \rtimes_\varphi G$ bezeichnet

Beweis:
1. Wir zeigen, dass $\cdot_\varphi$ assoziativ ist. Da φ ein Gruppenhomomorphismus mit Werten in $\mathrm{Aut}(H)$ ist, gilt $\varphi_{g_1g_2}(h_1) = \varphi_{g_1} \circ \varphi_{g_2}(h_1)$ und $\varphi_{g_1}(h_1h_2) = \varphi_{g_1}(h_1)\varphi_{g_1}(h_2)$ für alle $g_1, g_2 \in G$ und $h_1, h_2 \in H$. Damit erhalten wir für alle $g_1, g_2, g_3 \in G$ und $h_1, h_2, h_3 \in H$

$$\begin{aligned}&(h_1, g_1) \cdot_\varphi ((h_2, g_2) \cdot_\varphi (h_3, g_3)) = (h_1, g_1) \cdot_\varphi (h_2\varphi_{g_2}(h_3), g_2g_3) = (h_1\varphi_{g_1}(h_2\varphi_{g_2}(h_3)), g_1g_2g_3)\\ =&(h_1\varphi_{g_1}(h_2)\varphi_{g_1}(\varphi_{g_2}(h_3))), g_1g_2g_3) = (h_1\varphi_{g_1}(h_2)\varphi_{g_1g_2}(h_3), g_1g_2g_3) = (h_1\varphi_{g_1}(h_2), g_1g_2) \cdot_\varphi (h_3, g_3)\\ =&((h_1, g_1) \cdot_\varphi (h_2, g_2)) \cdot_\varphi (h_3, g_3)\end{aligned}$$

2. Das neutrale Element ist $e = (e_G, e_H)$. Denn da φ ein Gruppenhomomorphismus mit Werten in $\mathrm{Aut}(H)$ ist, gilt $\varphi_{e_G}(h) = \mathrm{id}_H(h) = h$ und $\varphi_g(e_H) = e_H$ für alle $g \in G$, $h \in H$. Es folgt

$$\begin{aligned}(h, g) \cdot_\varphi (e_H, e_G) &= (h\varphi_g(e_H), ge_G) = (he_H, ge_G) = (h, g)\\ (e_H, e_G) \cdot_\varphi (h, g) &= (e_H\varphi_{e_G}(h), e_Gg) = (e_Hh, e_Gg) = (h, g).\end{aligned}$$

3. Das Inverse von (h, g) ist $(\varphi_{g^{-1}}(h^{-1}), g^{-1})$. Da φ ein Gruppenhomomorphismus mit Werten in $\mathrm{Aut}(H)$ ist, gilt $\varphi_g(\varphi_{g^{-1}}(h)) = \varphi_{gg^{-1}}(h) = \varphi_{e_G}(h) = h$ und $\varphi_g(h^{-1}) = \varphi_g(h)^{-1}$, und es folgt

$$\begin{aligned}(h, g) \cdot_\varphi (\varphi_{g^{-1}}(h^{-1}), g^{-1}) &= (h\varphi_g(\varphi_{g^{-1}}(h^{-1})), gg^{-1}) = (hh^{-1}, gg^{-1}) = (e_H, e_G)\\ (\varphi_{g^{-1}}(h^{-1}), g^{-1}) \cdot_\varphi (h, g) &= (\varphi_{g^{-1}}(h^{-1})\varphi_{g^{-1}}(h), g^{-1}g) = (\varphi_{g^{-1}}(h^{-1}h), e_G) = (e_H, e_G).\end{aligned}$$

□

Beispiel 1.4.2.

1. Betrachtet man einen trivialen Gruppenhomomorphismus $\varphi : G \to \mathrm{Aut}(H)$, $g \mapsto \mathrm{id}_H$, so ist $H \rtimes_\varphi G = H \times G$ gerade das direkte Produkt von H und G aus Beispiel 1.1.4, 9.

2. Wählt man $G = \{e\}$ oder $H = \{e\}$, so ist der triviale Gruppenhomomorphismus der einzige Gruppenhomomorphismus $\varphi : G \to \mathrm{Aut}(H)$. Es folgt $H \rtimes_\varphi G \cong H$, falls $G = \{e_G\}$, und $H \rtimes_\varphi G \cong G$, falls $H = \{e_H\}$. Semidirekte Produkte dieser Form werden als **triviale semidirekte Produkte** bezeichnet.

3. Für jede Gruppe G können wir den Gruppenhomomorphismus $\varphi : G \to \mathrm{Aut}(G)$, $g \mapsto C_g$ aus Beispiel 1.1.7, 2. betrachten. Das zugehörige semidirekte Produkt $G \rtimes_\varphi G$ hat dann die Gruppenmultiplikation $(h_1, g_1) \cdot_\varphi (h_2, g_2) = (h_1g_1h_2g_1^{-1}, g_1g_2)$.

4. Für jede Gruppe H können wir $G = \mathrm{Aut}(H)$ und $\varphi = \mathrm{id} : \mathrm{Aut}(H) \to \mathrm{Aut}(H)$ betrachten. Die Gruppenmultiplikation des semidirekten Produkts $H \rtimes_\varphi \mathrm{Aut}(H)$ ist dann gegeben durch $(h_1, f_1) \cdot_\varphi (h_2, f_2) = (h_1f_1(h_2), f_1 \circ f_2)$.

5. Für $H = (\mathbb{K}^n, +)$ und jede Untergruppe $G \subseteq \mathrm{GL}(n, \mathbb{K})$ erhalten wir einen Gruppenhomomorphismus $\varphi : G \to \mathrm{Aut}(\mathbb{K}^n)$, $M \mapsto \varphi_M$ mit $\varphi_M(v) = M \cdot v$ für alle $M \in \mathrm{GL}(n, \mathbb{K})$ und $v \in \mathbb{K}^n$. Das zugehörige semidirekte Produkt $\mathbb{K}^n \rtimes_\varphi G$ hat die Gruppenmultiplikation $(v_1, M_1) \cdot_\varphi (v_2, M_2) = (v_1 + M_1 \cdot v_2, M_1 \cdot M_2)$.

6. Für $\mathbb{K} = \mathbb{R}$ und $G = \mathrm{O}(n, \mathbb{R})$ erhält man aus 5. die **euklidische Gruppe** $\mathbb{R}^n \rtimes_\varphi \mathrm{O}(n, \mathbb{R})$, die Symmetriegruppe des n-dimensionalen euklidischen Raums.

Diese Beispiele zeigen, dass semidirekte Produkte Verallgemeinerungen von direkten Produkten sind, die viele Anwendungen in der Geometrie und in der Algebra besitzen. Insbesondere sind Symmetriegruppen affiner Vektorräume immer semidirekte Produkte. Welche semidirekten Produkte auftreten, hängt von der Dimension ab und davon, mit welchen zusätzlichen Strukturen auf den zugrundeliegenden Vektorräumen sie verträglich sein sollen.

Wir untersuchen nun, wie die Gruppen G und H in einem semidirekten Produkt $H \rtimes_\varphi G$ interagieren. Es zeigt sich, dass sowohl $G \cong \{e_H\} \times G$ und $H \cong H \times \{e_G\}$ Untergruppen von $H \rtimes_\varphi G$ sind, aber im Allgemeinen nur $H \cong H \times \{e_G\}$ ein Normalteiler.

Lemma 1.4.3: Seien G, H Gruppen, $\varphi : G \to \mathrm{Aut}(H)$ ein Gruppenhomomorphismus und $H \rtimes_\varphi G$ das zugehörige semidirekte Produkt. Dann gilt:

1. $H \rtimes_\varphi G$ ist abelsch genau dann, wenn H und G abelsch sind und φ trivial.
2. Die Untergruppe $H \cong H \times \{e_G\}$ ist ein Normalteiler und $(H \rtimes_\varphi G)/H \cong G$.
3. Die Untergruppe $\{e_H\} \times G$ ist ein Normalteiler genau dann, wenn φ trivial ist

Beweis:
1. Sind G, H abelsch und φ trivial, so erhält man nach Beispiel 1.4.2 das direkte Produkt zweier abelscher Gruppen, das wieder abelsch ist. Ist umgekehrt $H \rtimes_\varphi G$ abelsch, so gilt

$$(\varphi_g(h), g) = (e_H, g) \cdot_\varphi (h, e_G) = (h, e_G) \cdot_\varphi (e_H, g) = (h, g) \quad \Rightarrow \quad \varphi_g(h) = h \ \ \forall g \in G, h \in H.$$

Damit ist φ trivial. Außerdem sind dann auch G und H abelsch, denn

$$\begin{aligned}(e_H, g_1 g_2) &= (e_H, g_1) \cdot_\varphi (e_H, g_2) = (e_H, g_2) \cdot_\varphi (e_H, g_1) = (e_H, g_2 g_1) \qquad \forall g_1, g_2 \in G \\ (h_1 h_2, e_G) &= (h_1, e_G) \cdot_\varphi (h_2, e_G) = (h_2, e_G) \cdot_\varphi (h_1, e_G) = (h_2 h_1, e_G) \qquad \forall h_1, h_2 \in H.\end{aligned}$$

2. Die Projektionsabbildung $p_2 : H \rtimes_\varphi G \to G$, $(h, g) \mapsto g$ ist ein surjektiver Gruppenhomomorphismus mit $\ker(p_2) = H \times \{e_G\} \cong H$. Damit ist $H \cong H \times \{e_G\} \subseteq H \rtimes_\varphi G$ ein Normalteiler, und aus dem Homomorphiesatz 1.3.23 folgt $(H \rtimes_\varphi G)/H \cong G$.

3. Ist φ trivial, so ist das semidirekte Produkt $H \rtimes_\varphi G$ das direkte Produkt $G \times H$ und auch die Abbildung $p_1 : H \times G \to H$, $(h, g) \mapsto h$ ist ein Homomorphismus mit $\ker(p_1) = \{e_H\} \times G$. Damit ist $\{e_H\} \times G$ ein Normalteiler. Ist umgekehrt $\{e_H\} \times G$ ein Normalteiler, so folgt

$$(h, e_G)^{-1} \cdot_\varphi (e_H, g) \cdot_\varphi (h, e_G) = (h^{-1}\varphi_g(h), g) \in \{e_H\} \times G \quad \Rightarrow \quad \varphi_g(h) = h \ \ \forall g \in G, h \in H.$$

□

Wir kehren nun zu unserer Ausgangsfrage zurück und untersuchen, unter welchen Umständen eine gegebene Gruppe G isomorph zu einem semidirekten Produkt $N \rtimes_\varphi H$ für geeignete Untergruppen $N, H \subseteq G$ ist. Dafür muss nach Lemma 1.4.3 $N \subseteq G$ zumindest ein Normalteiler sein. Außerdem lässt sich in einem semidirekten Produkt $N \rtimes_\varphi H$ jedes Element eindeutig als Produkt $(n, h) = (n, e_H) \cdot_\varphi (e_N, h)$ eines Elements in $N \times \{e_H\} \cong N$ und eines Elements in $\{e_N\} \times H \cong H$ schreiben. Die Eindeutigkeit ist dabei äquivalent zu der Forderung, dass $H \cap N$ nur das neutrale Element enthält. Wir vermuten also, dass die Bedingungen, $NH = G$ und $N \cap H = \{e\}$ notwendig und hinreichend sind.

Satz 1.4.4: Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler mit $NH = G$ und $H \cap N = \{e\}$. Dann gilt:

1. Die Abbildung $\varphi : H \to \mathrm{Aut}(N)$, $h \mapsto C_h$ mit $C_h(n) = hnh^{-1}$ ist ein Homomorphismus.
2. Sie induziert einen Gruppenisomorphismus $f : N \rtimes_\varphi H \to G$, $(n, h) \mapsto nh$.
3. $H \cong G/N$.

Man nennt dann G das **(innere) semidirekte Produkt** von N und H und schreibt $G = N \rtimes H$.

Beweis:
Da N ein Normalteiler ist, ist die Abbildung $C_h : N \to N$, $n \mapsto hnh^{-1}$ definiert, und man erhält einen Gruppenhomomorphismus $\varphi : H \to \mathrm{Aut}(N)$, $h \mapsto C_h$ (vgl. Beispiel 1.1.7, 2.). Damit ist auch das semidirekte Produkt $N \rtimes_\varphi H$ definiert. Die Abbildung f ist surjektiv, da $NH = G$. Sie ist injektiv, denn aus $f(n_1, h_1) = n_1h_1 = n_2h_2 = f(n_2, h_2)$ folgt $n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H = \{e\}$ und damit $n_1 = n_2$ und $h_1 = h_2$. Sie ist ein Gruppenhomomorphismus, denn

$$\begin{aligned} f\big((n_1, h_1) \cdot_\varphi (n_2, h_2)\big) &= f(n_1\varphi_{h_1}(n_2), h_1h_2) = f(n_1h_1n_2h_1^{-1}, h_1h_2) = n_1h_1n_2h_2 \\ &= f(n_1, h_1) \cdot f(n_2, h_2) \qquad \forall n_1, n_2 \in N, h_1, h_2 \in H. \end{aligned}$$

Aus Lemma 1.4.3.2 ergibt sich damit $G/N \cong (N \rtimes_\varphi H)/N \cong H$. □

Beispiel 1.4.5. Wir betrachten die Diedergruppe D_n aus Beispiel 1.2.15

$$\mathrm{D}_n = \{r^k \mid k = 0, \ldots, n-1\} \dot\cup \{sr^k \mid k = 0, \ldots, n-1\},$$

wobei r die Drehung um den Winkel $\frac{2\pi}{n}$ bezeichnet und s die Spiegelung an der x-Achse. Nach Beispiel 1.2.15 gelten die Relationen $r^n = s^2 = e, sr = r^{-1}s$.

Aus den Relationen folgt $sr^ks^{-1} = r^{-k}$ für alle $k \in \mathbb{Z}$. Damit ist $N = \langle r\rangle \cong \mathbb{Z}/n\mathbb{Z} \subseteq D_n$ ein Normalteiler. Die Untergruppe $H = \langle s\rangle = \{e, s\} \cong \mathbb{Z}/2\mathbb{Z}$ erfüllt $H \cap N = \{e\}$ und $NH = D_n$. Nach Satz 1.4.4 ist die Diedergruppe damit ein semidirektes Produkt $D_n = N \rtimes_\varphi H$ mit dem Gruppenhomomorphismus $\varphi : H \to \mathrm{Aut}(N)$, $\varphi_s(r^k) = sr^ks^{-1} = r^{-k}$. Schreibt man die abelschen Gruppen $N \cong \mathbb{Z}/n\mathbb{Z}$ und $H \cong \mathbb{Z}/2\mathbb{Z}$ additiv, so ergibt sich

$$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \qquad \text{mit} \quad \varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \varphi_{\bar 1}(\bar k) = -\bar k.$$

Die Unterscheidung zwischen *inneren* und *äußeren* semidirekten Produkten ist eine künstliche. Sie beschreibt einen Unterschied in der Ausgangssituation, nämlich ob man ein semidirektes Produkt aus einem Gruppenhomomorphismus in eine Automorphismengruppe oder aus einem Normalteiler einer gegebenen Gruppe konstruiert. Die resultierenden Gruppen sind jedoch isomorph, und deswegen spielt das eigentlich keine Rolle.

Satz 1.4.4 erlaubt es uns, statt der Faktorgruppe G/N auch die dazu isomorphe Untergruppe $H \subseteq G$ zu betrachten. Sie spielt also dieselbe Rolle wie das Komplement eines Untervektorraums $U \subseteq V$ für die Quotientenräume. Der entscheidende Unterschied zu Komplementen von Untervektorräumen ist aber, dass eine Untergruppe $H \subseteq G$, die die Bedingungen aus Satz 1.4.4 erfüllt, nicht zu jedem Normalteiler $N \subseteq G$ existieren muss. Die Tatsache, dass $N \subseteq G$ ein Normalteiler ist, garantiert also nicht, dass sich G als semidirektes Produkt der Form $G = N \rtimes G/N$ schreiben lässt. Ein einfaches Kriterium dafür, dass dies möglich ist, ist das folgende.

Satz 1.4.6: Sei G eine Gruppe, $N \subseteq G$ ein Normalteiler und $\pi_N : G \to G/N$ die kanonische Surjektion. Dann gilt $G \cong N \rtimes (G/N)$ genau dann, wenn es einen Gruppenhomomorphismus $f : G/N \to G$ gibt mit $\pi_N \circ f = \mathrm{id}_{G/N}$. Man sagt f **spaltet** π_N.

Beweis:
Ist $G \cong N \rtimes_\varphi (G/N)$, so können wir die kanonische Surjektion identifizieren mit der Abbildung $\pi_N = p_2 : N \rtimes_\varphi (G/N) \to (G/N)$, $(n, gN) \mapsto gN$ und erhalten den Gruppenhomomorphismus $f : G/N \to N \rtimes_\varphi (G/N)$, $gN \mapsto (e_H, gN)$ mit $\pi_N \circ f = \mathrm{id}_{G/N}$.

Gibt es umgekehrt einen Gruppenhomomorphismus $f : G/N \to G$ mit $\pi_N \circ f = \mathrm{id}_{G/N}$, so betrachten wir die Untergruppe $H = f(G/N) \subseteq G$ und zeigen, dass N und H die Bedingungen in Satz 1.4.4 erfüllen. Ist $g \in H \cap N$, so gibt es ein $g' \in G$ mit $g = f(g'N)$ und $\pi_N(g) = N$. Daraus folgt $g'N = \pi_N \circ f(g'N) = \pi_N(g) = N$. Da f ein Gruppenhomomorphismus ist, ergibt sich $g = f(g'N) = f(N) = e$ und damit $H \cap N = \{e\}$. Um zu zeigen, dass $NH = G$, schreiben wir ein Element $g \in G$ als Produkt $g = (g \cdot f(\pi_N(g))^{-1}) \cdot f(\pi_N(g))$ mit $f(\pi_N(g)) \in H$. Da

$$\pi_N(g \cdot f(\pi_N(g))^{-1}) = \pi_N(g) \cdot (\pi_N \circ f \circ \pi_N(g)))^{-1} = \pi_N(g) \cdot \pi_N(g)^{-1} = \pi_N(gg^{-1}) = \pi_N(e) = N,$$

gilt $gf(\pi_N(g))^{-1} \in \ker(\pi_N) = N$ und damit $NH = G$. Mit Satz 1.4.4 folgt die Behauptung. □

Beispiel 1.4.7.

1. Die Gruppe $\mathbb{Z}/4\mathbb{Z}$ ist kein nichttriviales semidirektes Produkt. Denn ihre einzige nichttriviale echte Untergruppe ist $\{\bar{0}, \bar{2}\} \cong \mathbb{Z}/2\mathbb{Z}$. Da $\mathbb{Z}/4\mathbb{Z}$ abelsch ist, wäre sie als semidirektes Produkt nach Lemma 1.4.3 ein direktes Produkt. Also käme dafür nur die Kleinsche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in Frage, aber diese Gruppe ist nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$.

2. Analog kann man zeigen, dass die abelschen Gruppen $\mathbb{Z}/p^n\mathbb{Z}$ für $n \in \mathbb{N}$ und $p \in \mathbb{N}$ prim keine nichttrivialen semidirekten Produkte sind, obwohl sie zu jedem $d \in \{0, 1, ..., n-1\}$ eine zu $\mathbb{Z}/p^d\mathbb{Z}$ isomorphe Untergruppe besitzen.

3. Die **Quaternionengruppe** Q_8 ist die Gruppe $Q_8 = \{\pm e, \pm i, \pm j, \pm k\} \subseteq \mathrm{GL}(2, \mathbb{C})$ mit

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad j = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \qquad k = \begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix}$$

   und den Relationen

$$i \cdot j = k = -j \cdot i \qquad k \cdot i = j = -i \cdot k \qquad j \cdot k = i = -k \cdot j \qquad i^2 = j^2 = k^2 = -e.$$

   Die Elemente $\pm i, \pm j, \pm k$ haben Ordnung 4, das Element $-e$ hat Ordnung 2, und e ist das neutrale Element. Die Untergruppe $N = \{e, -e\} \cong \mathbb{Z}/2\mathbb{Z}$ ist ein Normalteiler. Die Faktorgruppe $Q_8/N = \{N, iN, jN, kN\}$ ist nach Bemerkung 1.1.5 isomorph zur Kleinschen Vierergruppe $Q_8/N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, denn $xN \cdot xN = x^2N = -eN = N$ für $x = i, j, k$.

   Die Quaternionengruppe Q_8 ist aber kein semidirektes Produkt $\mathbb{Z}/2\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Denn jeder Gruppenhomomorphismus $f : Q_8/N \to Q_8$ muss die Elemente iN, jN, kN der Ordnung 2 in Q_8/N auf Elemente der Ordnung 1 oder 2 in Q_8 abbilden. Daraus folgt $f(iN), f(jN), f(kN) \in N$ und damit ist $\pi_N \circ f \neq \mathrm{id}_{Q_8/N}$. Also ist nach Satz 1.4.6 Q_8 nicht isomorph zu einem semidirekten Produkt $\mathbb{Z}/2\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Beispiel 1.4.7 zeigt, dass der Versuch die Betrachtung von Faktorgruppen durch die Betrachtung von Untergruppen zu ersetzen, schon für sehr simple Gruppen scheitern muss. Ist eine gegebene Gruppe H isomorph zu einer Faktorgruppe G/N, so muss es keine Untergruppe von G geben, die zu H isomorph ist und zusammen mit dem Normalteiler N die Gruppe G aufspannt. Faktorgruppen lassen sich im Allgemeinen also nicht durch Untergruppen ersetzen. Dies ist der Grund, warum Faktorgruppen in der Gruppentheorie unverzichtbar sind unf eine viel wichtigere Rolle spielen als Quotientenräume in der linearen Algebra.

1.5 Gruppenoperationen

Wir nehmen nun den Standpunkt ein, aus dem am Anfang des Kapitels die Gruppen motiviert wurden und betrachten Gruppen als *Bewegungen* oder *Symmetrien* von algebraischen oder geometrischen Objekten. Dabei fassen wir Gruppenelemente insbesondere als Abbildungen von Mengen in sich selbst auf, die verschiedene Elemente ineinander überführen. Ein schon bekanntes Beispiel dafür ist die Permutationsgruppe S_X einer Menge X. Mit Hilfe von Gruppenhomomorphismen $\varphi : G \to S_X$ können wir aber auch jeder andere Gruppe G Abbildungen der Menge X in sich selbst zuordnen. Dies führt auf den Begriff der *Gruppenoperation* oder *Gruppenwirkung*. Gleichzeitig betrachten wir natürlich auch Abbildungen zwischen Mengen mit Gruppenoperationen, die mit den Gruppenoperationen veträglich sind.

Definition 1.5.1: Sei G eine Gruppe mit neutralem Element $e \in G$ und X eine Menge.

1. Eine **(Links)wirkung** oder **(Links)operation** von G auf X ist eine Abbildung

   $$\triangleright : G \times X \to X,\ (g, x) \mapsto g \triangleright x$$

   mit

   (O1) $e \triangleright x = x$ für alle $x \in X$,

   (O2) $(gh) \triangleright x = g \triangleright (h \triangleright x)$ für alle $g, h \in G$ und $x \in X$.

   Eine Menge X zusammen mit einer Linksoperation von G auf X heißt eine **G-Menge**.

2. Sind $\triangleright_X : G \times X \to X$ und $\triangleright_Y : G \times Y \to Y$ Linksoperationen, so heißt eine Abbildung $f : X \to Y$ **G-äquivariant** oder **Homomorphismus von G-Mengen** wenn

   $$f(g \triangleright_X x) = g \triangleright_Y f(x) \qquad \forall g \in G, x \in X.$$

   Ist f zusätzlich bijektiv, so nennt man f einen **G-Isomorphismus** oder **Isomorphismus von G-Mengen**.

Bemerkung 1.5.2.

1. Analog definiert man eine **Rechtswirkung** oder **Rechtsoperation** einer Gruppe G auf einer Menge X als eine Abbildung $\triangleleft : X \times G \to X$, $(x, g) \mapsto x \triangleleft g$ mit $x \triangleleft e = x$ und $x \triangleleft (gh) = (x \triangleleft g) \triangleleft h$ für alle $x \in X$ und $g, h \in G$.

   Wir können uns aber auf Linksoperationen beschränken, weil für jede Rechtsoperation $\triangleleft$ die Abbildung $\triangleright : G \times X \to X$, $(g, x) \mapsto x \triangleleft g^{-1}$ eine Linksoperation ist und für jede Linksoperation $\triangleright$ die Abbildung $\triangleleft : X \times G \to X$, $(x, g) \mapsto g^{-1} \triangleright x$ eine Rechtsoperation.

2. Alternativ kann man eine Linksoperation von G auf X auch definieren als einen Gruppenhomomorphismus $\sigma : G \to S_X$ von G in die Gruppe S_X der Permutationen von X.

   Ist nämlich $\triangleright : G \times X \to X$ eine Linksoperation, so ist für alle $g \in G$ die Abbildung $\sigma_g : X \to X$, $x \mapsto g \triangleright x$ eine Bijektion mit Inversem $\sigma_g^{-1} = \sigma_{g^{-1}}$, also eine Permutation. Da nach (O2) $\sigma_g \circ \sigma_h = \sigma_{gh}$, erhält man einen Homomorphismus $\sigma : G \to S_X$, $g \mapsto \sigma_g$. Ist umgekehrt $\sigma : G \to S_X$, $g \mapsto \sigma_g$ ein Gruppenhomomorphismus, so erhalten wir eine Abbildung $\triangleright : G \times X \to X$, $(g, x) \mapsto \sigma_g(x)$, die (O1) und (O2) erfüllt (Übung).

Beispiel 1.5.3.

1. Jede Gruppe G operiert auf jede Menge X durch die **triviale Gruppenoperation** $\triangleright : G \times X \to X$, $(g, x) \mapsto x$. Dies entspricht dem Homomorphismus $\sigma : G \to S_X$, $g \mapsto \mathrm{id}_X$.

2. Jede Gruppe G operiert auf sich selbst durch Links- und Rechtsmultiplikation:

   $$\triangleright_L : G \times G \to G,\ (g, h) \mapsto g \triangleright_L h = gh \qquad \triangleright_R : G \times G \to G,\ (g, h) \mapsto g \triangleright_R h = hg^{-1}.$$

   Die **Inversion** $f : G \to G$, $g \mapsto g^{-1}$ ist G-Isomorphismus von $(G, \triangleright_L)$ nach $(G, \triangleright_R)$.
   Für $g \in G$ ist die **Rechtstranslation** $R_g : G \to G$, $h \mapsto hg$ ein G-Automorphismus von $(G, \triangleright_L)$, die **Linkstranslation** $L_g : G \to G$, $h \mapsto gh$ ein G-Automorphismus von $(G, \triangleright_R)$.

3. Jede Gruppe operiert auf sich selbst durch Konjugation

   $$\triangleright_C : G \times G \to G,\ (g, h) \mapsto g \triangleright_C h = ghg^{-1}.$$

4. Für jede Untergruppe $H \subseteq G$ operiert G auf den Nebenklassen G/H und $H\backslash G$ durch

   $$\triangleright'_L : G \times G/H \to G/H,\ (g, kH) \mapsto gkH \qquad \triangleright'_R : G \times H\backslash G \to H\backslash G,\ (g, Hk) \mapsto Hkg^{-1}.$$

   Die kanonischen Surjektionen $\pi_L : G \to G/H$, $g \mapsto gH$ und $\pi_R : G \to H\backslash G$, $g \mapsto Hg$ sind G-äquivariant bezüglich $\triangleright_L$ und $\triangleright'_L$ und bezüglich $\triangleright_R$ und $\triangleright'_R$.

5. Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so definiert jede Gruppenoperation $\triangleright : H \times X \to X$ eine Gruppenoperation von G auf X, den **Pullback** von $\triangleright$ entlang φ

   $$\triangleright_\varphi : G \times X \to X,\ (g, x) \mapsto g \triangleright_\varphi x = \varphi(g) \triangleright x.$$

   Denn $\triangleright$ entspricht einem Gruppenhomomorphismus $\sigma : H \to S_X$, und durch Verkettung erhält man einen Gruppenhomomorphismus $\sigma \circ \varphi : G \to S_X$.

6. Insbesondere ist für jede Untergruppe $U \subseteq H$ die Inklusionsabbildung $\iota : U \to H$, $u \mapsto u$ ein Gruppenhomomorphismus, und damit liefert jede Operation $\triangleright : H \times X \to X$ eine Operation $\triangleright_\iota : U \times X \to X$, $(u, x) \mapsto u \triangleright x$ von U auf X, die **Einschränkung** von $\triangleright$ auf U.

7. Eine Teilmenge $Y \subseteq X$ heißt **invariant** oder **stabil** unter der Operation $\triangleright : G \times X \to X$, wenn $g \triangleright y \in Y$ für alle $g \in G$ und $y \in Y$ gilt. In diesem Fall erhält man eine Operation $\triangleright : G \times Y \to Y$, $(g, y) \mapsto g \triangleright y$, die **Einschränkung** von $\triangleright$ auf Y.

8. Jede Gruppe G operiert durch $\triangleright : G \times U_G \to U_G$, $(g, H) \mapsto gHg^{-1}$ auf der Menge U_G ihrer Untergruppen.

   Die Abbildung $\triangleright$ ist wohldefiniert, denn für jede Untergruppe $H \subseteq G$ und jedes $g \in G$ ist auch gHg^{-1} eine Untergruppe von G. Sie ist eine Operation, da $e \triangleright H = eHe^{-1} = H$ und $(g_1 g_2) \triangleright H = (g_1 g_2) H (g_1 g_2)^{-1} = g_1 (g_2 H g_2^{-1}) g_1^{-1} = g_1 \triangleright (g_2 \triangleright H)$ für alle $g_1, g_2 \in G$.

9. Ist V ein Vektorraum über dem Körper $\mathbb{K}$, so operiert jede Untergruppe $G \subseteq \mathrm{GL}_{\mathbb{K}}(V)$ auf V durch $\triangleright : G \times V \to V$, $(\varphi, v) \mapsto \varphi(v)$. Die Abbildungen $f_\lambda : V \to V$, $v \mapsto \lambda v$ für $\lambda \in \mathbb{K}$ sind G-äquivariant.

10. Insbesondere operiert jede Untergruppe $G \subseteq \mathrm{GL}(n, \mathbb{K})$ auf $\mathbb{K}^n$ durch $\triangleright : G \times \mathbb{K}^n \to \mathbb{K}^n$, $(M, v) \mapsto M \cdot v$. Die Abbildungen $f_\lambda : \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto \lambda v$ für $\lambda \in \mathbb{K}$ sind G-äquivariant.

Um die Struktur von G-Mengen besser zu verstehen, bietet es sich an, die Mengen der Punkte in einer G-Menge X zu untersuchen, die durch die Operation von G aufeinander abgebildet werden. Dies sind die minimalen G-stabilen Mengen, auf die wir eine Operation nach Beispiel 1.5.3, 8. einschränken können. Es stellt sich heraus, dass diese Mengen eine Partition der Menge X und damit eine Äquivalenzrelation auf X definieren.

Satz 1.5.4: Sei $\triangleright : G \times X \to X$ eine Gruppenoperation von G auf X. Dann ist

$$x \sim y \quad \Leftrightarrow \quad \exists g \in G : \, y = g \triangleright x$$

eine Äquivalenzrelation auf X. Die Äquivalenzklasse eines Elements $x \in X$ ist die Menge

$$G \triangleright x \; := \; \{g \triangleright x \mid g \in G\}.$$

Sie heißt **Bahn** oder **Orbit** von x. Die **Länge** einer Bahn $G \triangleright x$ ist definiert als ihre Mächtigkeit. Gibt es nur eine einzige Bahn, so nennt man die Gruppenoperation **transitiv**.

Beweis:
• Reflexivität: Es gilt $x = e \triangleright x$ und damit $x \sim x$.
• Symmetrie: Aus $x \sim y$ folgt $y = g \triangleright x$ für ein $g \in G$ und damit

$$g^{-1} \triangleright y = g^{-1} \triangleright (g \triangleright x) \overset{(O1)}{=} (g^{-1} g) \triangleright x = e \triangleright x \overset{(O2)}{=} x \quad \Rightarrow \quad y \sim x.$$

• Transitivität: Ist $x \sim y$ und $y \sim z$, so gibt es $g, h \in G$ mit $y = g \triangleright x$ und $z = h \triangleright y$. Daraus folgt $z = h \triangleright y = h \triangleright (g \triangleright x) = (hg) \triangleright x$ und damit $x \sim z$. □

Beispiel 1.5.5.

1. Die Bahnen der trivialen Gruppenwirkung $\triangleright : G \times X \to X$, $(g, x) \mapsto x$ sind einelementig: $G \triangleright x = \{x\}$ für alle $x \in X$.

2. Für jede symmetrische Bilinearform η auf dem $\mathbb{R}^n$ ist die **orthogonale Gruppe**

   $$O_\eta = \{M \in \mathrm{GL}(n, \mathbb{R}) \mid \eta(M \cdot v, M \cdot w) = \eta(v, w) \; \forall v, w \in \mathbb{R}^n\}$$

   eine Untergruppe von $\mathrm{GL}(n, \mathbb{R})$. Sie operiert durch $\triangleright : \mathrm{O}_\eta \times \mathbb{R}^n \to \mathbb{R}^n$, $(M, v) \mapsto M \cdot v$ auf dem $\mathbb{R}^n$ (vgl. Beispiel 1.5.3, 9). Da $\eta(M \triangleright v, M \triangleright v) = \eta(Mv, Mv) = \eta(v, v)$ für alle $M \in \mathrm{O}_\eta$ und $v \in \mathbb{R}^n$, ist die Bahn $\mathrm{O}_\eta \triangleright v$ jedes Vektors $v \in \mathbb{R}^n$ in einer **Quadrik** $Q^c_\eta = \{w \in \mathbb{R}^n \mid \eta(w, w) = c\}$ für $c \in \mathbb{R}$ enthalten .

3. Wählt man für η in 2. das euklidische Skalarprodukt auf dem $\mathbb{R}^n$, so ist $O_\eta = \mathrm{O}(n, \mathbb{R})$. Die Bahnen sind die **Sphären** $S^{n-1}_r = \{x \in \mathbb{R}^n \mid x_1^2 + \ldots + x_n^2 = r^2\}$ vom Radius $r > 0$ sowie die Menge $\{0\}$.

4. Nach Beispiel 1.5.3, 2. und 6. operiert jede Untergruppe $H \subseteq G$ auf G durch Links- und Rechtsmultiplikation. Die zugehörigen Bahnen sind die Rechts - und Linksnebenklassen:

$$H \triangleright_L g = \{h \cdot g \mid h \in H\} = Hg \qquad H \triangleright_R g = \{gh^{-1} \mid h \in H\} = \{gh \mid h \in H\} = gH.$$

5. Nach Beispiel 1.5.3, 3. operiert jede Gruppe G auf sich selbst durch Konjugation. Die Bahnen sind die **Konjugationsklassen** $G \triangleright h = C^h = \{ghg^{-1} \mid g \in G\}$. Liegen zwei Elemente von G in derselben Bahn, so nennt man sie **zueinander konjugiert**.

6. Die Operationen $\triangleright_L$ und $\triangleright_R$ einer Gruppe G auf sich selbst durch Links- und Rechtsmultiplikation (Beispiel 1.5.3, 2.) und die zugehörigen Operationen $\triangleright'_L$ und $\triangleright'_R$ auf G/H und $H\backslash G$ für eine Untergruppe $H \subseteq G$ (Beispiel 1.5.3, 6.) sind transitiv.

7. Nach Beispiel 1.5.3, 8. operiert jede Gruppe G durch $\triangleright : G \times U_G \to U_G$, $(g, H) \mapsto gHg^{-1}$ auf der Menge U_G ihrer Untergruppen. Zwei Untergruppen $H, H' \subseteq G$ liegen genau dann in derselben Bahn von $\triangleright$, wenn es ein $g \in G$ gibt mit $H' = gHg^{-1}$. In diesem Fall nennt man die Untergruppen $H, H' \subseteq G$ **zueinander konjugiert**.

Da es sich bei *in der gleichen Bahn liegen* um eine Äquivalenzrelation handelt, bilden die Bahnen einer Operation $\triangleright : G \times X \to X$ eine Partition von X. Die G-Menge X ist also die disjunkte Vereinigung ihrer Bahnen: jeder Punkt $x \in X$ liegt in genau einer Bahn. Da die Bahnen stabil unter G sind, lässt sich die Operation $\triangleright$ nach Beispiel 1.5.3, 7. zu einer transitiven Operation von G auf jeder Bahn einschränken. Damit können wir jede G-Menge in G-Mengen mit *transitiven* G-Operationen zerlegen. Wir werden zeigen, dass sich jede transitive Operation von G durch die Operation von G auf die Nebenklassen geeigneter Untergruppen beschreiben lässt. Diese Untergruppen sind die sogenannten *Stabilisatoren*.

Definition 1.5.6: Sei $\triangleright : G \times X \to X$ ein Gruppenoperation. Die Menge

$$G_x := \{g \in G \mid g \triangleright x = x\}$$

heißt **Stabilisator**, **Standgruppe** oder **Isotropiegruppe** von x. Ein Element $x \in X$ mit $G_x = G$ heißt **Fixpunkt** von $\triangleright$.

Beispiel 1.5.7.

1. Die Operationen $\triangleright_L : G \times G \to G$, $(g, h) \mapsto gh$ und $\triangleright_R : G \times G \to G$, $(g, h) \mapsto hg^{-1}$ haben triviale Stabilisatoren: $G_h = \{e\}$ für alle $h \in G$ und damit keine Fixpunkte, falls $G \neq \{e\}$.

2. Für die Operation $\triangleright : \mathrm{O}(3, \mathbb{R}) \times \mathbb{R}^3 \to \mathbb{R}^3$, $(M, v) \mapsto M \cdot v$ ist 0 ein Fixpunkt und $G_v \cong \mathrm{O}(2, \mathbb{R})$ für alle $v \in \mathbb{R}^3 \setminus \{0\}$. Denn es gilt $G \cdot 0 = 0$ für alle $G \in \mathrm{O}(3, \mathbb{R})$ und

$$G_{e_1} = \{M \in \mathrm{O}(3, \mathbb{R}) \mid Me_1 = e_1\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \;\middle|\; A \in \mathrm{O}(2, \mathbb{R}) \right\} \cong \mathrm{O}(2, \mathbb{R}).$$

   Jeder Vektor $w \in \mathbb{R}^3 \setminus \{0\}$ ist von der Form $w = \lambda Be_1$ mit geeigneten $B \in \mathrm{O}(3, \mathbb{R})$ und $\lambda \in \mathbb{R}^\times$. Daraus folgt

$$\begin{aligned} G_w &= \{M \in \mathrm{O}(3, \mathbb{R}) \mid Mw = w\} = \{M \in \mathrm{O}(3, \mathbb{R}) \mid \lambda MBe_1 = \lambda Be_1\} \\ &= \{M \in \mathrm{O}(3, \mathbb{R}) \mid MBe_1 = Be_1\} = \{M \in \mathrm{O}(3, \mathbb{R}) \mid B^{-1}MB \cdot e_1 = e_1\} = BG_{e_1}B^{-1} \\ &\cong \mathrm{O}(2, \mathbb{R}) \end{aligned}$$

3. Für die Operation $\triangleright_C : G \times G \to G$, $(g,h) \mapsto ghg^{-1}$ von G auf sich selbst durch Konjugation sind die Bahnen gerade die Konjugationsklassen und die Stabilisatoren die Zentralisatoren von Elementen aus G

$$G \triangleright h = C^h = \{ghg^{-1} \mid g \in G\} \qquad G_h = Z_h = \{g \in G \mid ghg^{-1} = h\}.$$

Die Menge der Fixpunkte ist das Zentrum (vgl. Beispiel 1.5.5, 5. und Beispiel 1.2.4, 6.)

$$Z(G) = \{h \in G \mid g \triangleright h = ghg^{-1} = h \ \forall g \in G\} = \{h \in G \mid gh = hg \ \forall g \in G\}.$$

4. Nach Beispiel 1.5.3, 9. operiert jede Gruppe G auf der Menge U_G ihrer Untergruppen durch $\triangleright : G \times U_G \to U_G$, $H \mapsto gHg^{-1}$. Die Fixpunkte dieser Operation sind gerade die Normalteiler in G. Der Stabilisator einer Untergruppe $H \in U_G$ ist

$$G_H = N(H) = \{g \in G \mid gHg^{-1} = H\}$$

Er heißt **Normalisator** von H und ist die größte Untergruppe von G, in der H normal ist.

Wir zeigen nun, dass die Stabilisatoren eine Gruppenoperation $\triangleright : G \times X \to X$ vollständig beschreiben. Dazu stellen wir fest, dass der Stabilisator G_x jedes Punkts $x \in X$ eine Untergruppe ist und betrachten die transitive G-Operation $\triangleright'_L : G \times G/G_x \to G/G_x$, $(g, hG_x) \mapsto (gh)G_x$ auf seinen Nebenklassen aus Beispiel 1.5.3, 4. Es stellt sich heraus, dass die resultierende G-Menge G-isomorph zu der Bahn von x unter der Operation $\triangleright$ ist.

Satz 1.5.8: Sei $\triangleright : G \times X \to X$ eine Operation von G auf X. Dann gilt für alle $x \in X$:

1. Der Stabilisator G_x ist eine Untergruppe von G.
2. Die Abbildung $\pi_x : G/G_x \to G \triangleright x$, $gG_x \mapsto g \triangleright x$ ist ein G-Isomorphismus.

Beweis:
1. Sind $h_1, h_2 \in G_x$, so gilt $h_1 \triangleright x = x$ und $h_2 \triangleright x = x$. Mit (O1) folgt $(h_1h_2) \triangleright x = h_1 \triangleright (h_2 \triangleright x) = h_1 \triangleright x = x$ und damit $h_1h_2 \in G_x$ (UG1). Wegen $e \triangleright x = x$ gilt $e \in G_x$ (UG2). Aus $h \in G_x$ folgt $x = e \triangleright x = (h^{-1}h) \triangleright x = h^{-1} \triangleright (h \triangleright x) = h^{-1} \triangleright x$, also $h^{-1} \in G_x$ (UG3).

2. Die Abbildung π_x ist wohldefiniert, denn aus $g_1G_x = g_2G_x$ folgt $g_1 = g_2h$ mit $h \in G_x$ und

$$\pi_x(g_1G_x) = g_1 \triangleright x = (g_2h) \triangleright x = g_2 \triangleright (h \triangleright x) = g_2 \triangleright x = \pi_x(g_2G_x).$$

Sie ist G-äquivariant, denn für alle $x \in X$ und $g, k \in G$ gilt

$$\pi_x(g \triangleright kG_x) = \pi_x((gk)G_x) = (gk) \triangleright x = g \triangleright (k \triangleright x) = g \triangleright \pi_x(kG_x).$$

Das Bild von π_x ist die Bahn $G \triangleright x$, und damit ist π_x surjektiv. Außerdem ist π_x injektiv, denn aus $\pi_x(g_1G_x) = \pi_x(g_2G_x)$ folgt

$$(g_2^{-1}g_1) \triangleright x = \pi_x(g_2^{-1}g_1G_x) = g_2^{-1} \triangleright \pi_x(g_1G_x) = g_2^{-1} \triangleright \pi_x(g_2G_x) = \pi_x(g_2^{-1}g_2G_x) = \pi_x(eG_x) = x,$$

also $g_2^{-1}g_1 \in G_x$ und $g_1G_x = g_2G_x$. □

Der Satz zeigt insbesondere, dass jede G-Menge mit einer *transitiven* G-Operation G-isomorph ist zu einer G-Menge G/H für eine geeignete Untergruppe $H \subseteq G$. Damit haben wir gezeigt, dass sich jede G-Menge bis auf G-Isomorphie durch die G-Mengen G/H aus Beispiel 1.5.3, 4. für geeignete Untergruppen $H \subseteq G$ beschreiben lässt. Um damit die G-Mengen bis auf G-Isomorphie zu bestimmen, müssen wir nur noch klären, welche Untergruppen $H \subseteq G$ isomorphe G-Mengen definieren.

Satz 1.5.9:

1. Für zwei Untergruppen $H_1, H_2 \subseteq G$ sind die G-Mengen G/H_1 und G/H_2 genau dann G-isomorph, wenn H_1 und H_2 zueinander konjugiert sind.
2. Für jede Gruppe G stehen G-Isomorphieklassen von transitiven G-Mengen in Bijektion mit Konjugationsklassen von Untergruppen von G.

Beweis:
1. Ist $H_2 = gH_1g^{-1}$ für ein $g \in G$, so ist H_2 der Stabilisator von $gH_1 \in G/H_1$, denn es gilt

$$k \in G_{gH_1} \quad \Leftrightarrow \quad (kg)H_1 = gH_1 \quad \Leftrightarrow \quad g^{-1}kg \in H_1 \quad \Leftrightarrow \quad k \in gH_1g^{-1}. \tag{1.1}$$

Nach Satz 1.5.8 ist $\pi'_{gH} : G/H_2 \to G/H_1$, $gH_2 \mapsto gH_1$ damit ein G-Isomorphismus.

Um zu zeigen, dass H_1 und H_2 zueinander konjugiert sind, wenn die G-Mengen G/H_1 und G/H_2 isomorph sind, stellen wir zunächst fest, dass jeder G-Isomorphismus $f : X \to Y$ von einer G-Menge $(X, \triangleright_X)$ in eine G-Menge $(Y, \triangleright_Y)$ Stabilisatoren auf Stabilisatoren abbildet:

$$g \in G_x \Leftrightarrow g \triangleright_X x = x \overset{f \text{ bijektiv}}{\Leftrightarrow} f(g \triangleright_X x) = f(x) \overset{f\ G\text{-äquiv.}}{\Leftrightarrow} g \triangleright_Y f(x) = f(x) \Leftrightarrow g \in G_{f(x)}.$$

Damit ist gezeigt, dass $G_x = G_{f(x)}$ für alle $x \in X$. Ist also $f : G/H_2 \to G/H_1$ ein G-Isomorphismus, so gibt es ein $g \in G$ mit $f(H_2) = gH_1$, und mit (1.1) folgt daraus für die Stabilisatoren $H_2 = G_{H_2} = G_{f(H_2)} = G_{gH_1} = gH_1g^{-1}$.

2. Nach Satz 1.5.8 ist jede transitive G-Menge G-isomorph zu einer G-Menge G/H für eine Untergruppe $H \subseteq G$, und nach 1. sind zwei G-Mengen G/H_1 und G/H_2 isomorph genau dann, wenn H_1 und H_2 zueinander konjugiert sind. □

Da wir die Bahnen in G-Mengen auf die Nebenklassen von Untergruppen zurückführen konnten, können wir sie nun auch mit bekannten Größen beschreiben, die die Nebenklassen charakterisieren, beispielsweise dem Index der Stabilisatoren. Dies erlaubt es uns die Anzahl der Fixpunkte einer endlichen G-Menge durch die Indizes von Untergruppen von G zu beschreiben und Aussagen über die Anzahl der Fixpunkte zu treffen. Besonders interessant werden diese Ergebnisse, wenn man sie auf die Operation von G auf sich selbst durch Konjugation anwendet, wo die Fixpunkte gerade die Elemente des Zentrums sind.

Korollar 1.5.10 (Bahnengleichung):
Sei $\triangleright : G \times X \to X$ eine Operation von G auf eine endliche Menge X mit Fixpunktmenge X^G und R ein **Repräsentantensystem** der Bahnen, also eine Teilmenge $R \subseteq X$, die genau ein Element aus jeder Bahn von $\triangleright$ enthält. Dann gilt

$$|X| = \sum_{x \in R} [G : G_x] = |X^G| + \sum_{x \in R \setminus X^G} [G : G_x] \tag{1.2}$$

Beweis:
Jedes Element von X ist in genau einer Bahn von $\triangleright$ enthalten. Damit ist die Anzahl der Elemente in X die Summe der Anzahlen der Elemente in den Bahnen. Nach Satz 1.5.8 hat die Bahn $G \triangleright x$ genau $|G \triangleright x| = |G/G_x| = [G : G_x]$ Elemente, und da R ein Repräsentantensystem ist, folgt die Behauptung. □

Korollar 1.5.11 (Klassengleichung):
Für jede endliche Gruppe G und jedes Element $h \in G$ gilt $|G/Z_h| = [G : Z_h] = |C^h|$. Ist R ein Repräsentantensystem der Konjugationsklassen, so gilt die **Klassengleichung**

$$|G| = \sum_{h \in R} [G : Z_h] = |Z(G)| + \sum_{h \in R \setminus Z(G)} [G : Z_h]. \tag{1.3}$$

Beweis:
Ist G eine endliche Gruppe, so sind die Bahnen der Operation $\triangleright : G \times G \to G$, $(g, h) \mapsto ghg^{-1}$ Konjugationsklassen und die Stabilisatoren Zentralisatoren (vgl. Beispiel 1.5.5, 5. und 1.2.4, 6)

$$G \triangleright h = C^h = \{ghg^{-1} \mid g \in G\} \qquad G_h = Z_h = \{g \in G \mid ghg^{-1} = h\}.$$

Ist R ein Repräsentantensystem der Konjugationsklassen, so ist die zugehörige Bahnengleichung (1.2) gerade die Klassengleichung (1.3). □

Die Klassengleichung liefert Einschränkungen an die Struktur einer endlichen Gruppe. Sie ist besonders nützlich für Gruppen von Primpotenzordnung, die sogenannten p-Gruppen. Für Gruppen von Primzahlordnung wurde in Korollar 1.3.10 bereits gezeigt, dass sie zyklisch sind und damit abelsch nach Korollar 1.2.17. Hier besteht also kein weiterer Klärungsbedarf. Ist die Gruppenordnung zwar keine Primzahl, aber eine Primpotenz, so lässt sich aus der Klassengleichung zumindest folgern, dass die Gruppe ein nichttriviales Zentrum hat.

Definition 1.5.12: Eine Gruppe der Ordnung p^n mit $p \in \mathbb{N}$ prim, $n \in \mathbb{N}_0$ heißt **p-Gruppe**.

Korollar 1.5.13: Jede nichttriviale p-Gruppe hat ein nichttriviales Zentrum.

Beweis:
Sei $|G| = p^n$ für ein $n \in \mathbb{N}$ und R ein Repräsentantensystem der Konjugationsklassen von G. Dann gilt $|C^h| = [G : Z_h]$ für alle $h \in G$ nach Korollar 1.5.11, und nach dem Satz von Lagrange ist $[G : Z_h]$ ein Teiler der Gruppenordnung p^n. Ist $h \notin Z(G)$, so folgt $[G : Z_h] > 1$ und damit ist p ein Teiler von $[G : Z_h]$. Aus der Klassengleichung ergibt sich

$$|Z(G)| = |G| - \sum_{h \in R \setminus Z(G)} [G : Z_h] = p^n - \sum_{h \in R \setminus Z(G)} [G : Z_h]$$

Da die rechte Seite durch p teilbar ist, gilt das auch für $|Z(G)|$, und es folgt $|Z(G)| > 1$. □

Beispiel 1.5.14. Die Diedergruppe D_4 aus Beispiel 1.2.15 hat Ordnung $8 = 2^3$, ist also eine nichttriviale 2-Gruppe. Ihr Zentrum ist gegeben durch $Z(D_4) = \{e, r^2\}$, wobei r^2 die Punktspiegelung am Ursprung ist.

Auf ähnliche Weise lassen sich aus der Bahnengleichung Aussagen über die Anzahl der Fixpunkte von Operationen von p-Gruppen gewinnen.

Korollar 1.5.15: Sei G eine nichttriviale p-Gruppe und $\triangleright : G \times X \to X$ eine Operation von G auf einer endlichen Menge X mit Fixpunktmenge $X^G = \{x \in X \mid g \triangleright x = x\}$. Dann gilt

$$|X^G| \equiv |X| \bmod p.$$

Ist $|X|$ nicht durch p teilbar, so hat X mindestens einen Fixpunkt.

Beweis:
Nach dem Satz von Lagrange ist ist $[G : G_x]$ ein Teiler von $|G|$ für jedes $x \in X$. Da G eine p-Gruppe ist, ist $[G : G_x]$ damit entweder durch p teilbar oder $[G : G_x] = 1$. Letzteres ist genau dann der Fall, wenn x ein Fixpunkt ist. Für jedes Repräsentantensystem R der Bahnen ergibt sich aus der Bahnengleichung

$$|X^G| = |X| - \sum_{x \in R \setminus X^G} [G : G_x] \equiv |X| \bmod p.$$

□

1.6 Die symmetrischen Gruppen

Die symmetrischen Gruppen S_n sind in einem gewissen Sinn die Mütter aller endlichen Gruppen: Jede endliche Gruppe ist in einer symmetrischen Gruppe als Untergruppe enthalten. Diese auf den ersten Blick überraschende Aussage ergibt sich daraus, dass jede Gruppe durch Linksmultiplikation auf sich selbst operiert. Dies liefert einen Gruppenhomomorphismus in ihre Permutationsgruppe.

Satz 1.6.1 (**Satz von Cayley**)**:** Jede Gruppe G ist isomorph zu einer Untergruppe ihrer Permutationsgruppe S_G. Insbesondere ist jede endliche Gruppe G isomorph zu einer Untergruppe einer Permutationsgruppe S_n.

Beweis:
Für jedes Gruppenelement $g \in G$ betrachten wir die Abbildung $L_g \colon G \to G$, $h \mapsto gh$ mit Inversem $L_g^{-1} = L_{g^{-1}} : G \to G$, $h \mapsto g^{-1}h$. Die Abbildung $L : G \to S_G$, $g \mapsto L_g$ ist ein Gruppenhomomorphismus, denn für alle $g, h, k \in G$ gilt

$$L_{gh}(k) = (gh)k = g(hk) = L_g \circ L_h(k).$$

Sie ist injektiv, denn aus $L_g = L_h$ folgt $g = L_g(e) = L_h(e) = h$. Damit ist G isomorph zu dem Bild $L(G) \subseteq S_G$. Ist G endlich, so ist S_G damit isomorph zu S_n für $n = |G|$, denn jede Bijektion $f : X \to Y$ zwischen zwei Mengen X und Y induziert einen Gruppenisomorphismus $\varphi_f : S_X \to S_Y$, $\sigma \mapsto f \circ \sigma \circ f^{-1}$. □

Der Satz von Cayley ist in der Praxis nicht sehr hilfreich, um die Struktur von endlichen Gruppen zu verstehen. Das liegt daran, dass die Gruppen S_n mit wachsendem n immer mehr und kompliziertere Untergruppen besitzen, die sich nur schwer bilanzieren lassen. Dennoch lohnt es sich, die Struktur der symmetrischen Gruppen genauer zu untersuchen. Eines der wichtigsten Hilfsmittel dabei sind die sogenannten *Zykel* oder *zyklischen Permutationen.*

Definition 1.6.2: Seien $1 \leq k \leq n \in \mathbb{N}$.

1. Eine Permutation $\sigma \in S_n$ heißt k-**Zykel** oder **Zykel der Länge** k, wenn es paarweise verschiedene $i_1, ..., i_k \in \{1, ..., n\}$ gibt mit $\sigma(i_j) = i_{j+1}$ für $1 \leq i < k$, $\sigma(i_k) = i_1$ und $\sigma(i) = i$ für alle $i \notin \{i_1, ..., i_k\}$. Man schreibt $\sigma = (i_1, ..., i_k)$.

2. Ein 2-Zykel heißt auch **Vertauschung** oder **Transposition** und ein 2-Zykel $(i, i+1)$ für ein $i \in \{1, ..., n-1\}$ **elementare Vertauschung** oder **elementare Transposition**.

Die Schreibweise $\sigma = (i_1, ..., i_k)$ für einen k-Zykel ist offensichtlich uneindeutig, denn alle zyklischen Permutationen des Tupels $(i_1, ..., i_k)$ bezeichnen die gleiche Permutation

$$\sigma = (i_1, i_2, ..., i_k) = (i_2, ..., i_k, i_1) = (i_3, ..., i_k, i_1, i_2) = ... = (i_k, i_1, ..., i_{k-1}).$$

Dennoch bewährt sich diese Schreibweise, weil bestimmte Aussagen in ihr eine sehr eingängige Form annehmen. Insbesondere erhält man die folgenden Rechenregeln für k-Zykel, die sich durch direktes Nachrechnen beweisen lassen (Übung).

Lemma 1.6.3: Es gilt für alle k-Zykel $(i_1, ..., i_k)$ und Permutationen $\pi \in S_n$:

1. $(i_1, ..., i_k)^{-1} = (i_k, ..., i_1)$
2. $(i_1, i_2, ..., i_k) = (i_1, i_2) \circ (i_2, i_3) \circ \ldots \circ (i_{k-1}, i_k)$.
3. $\pi \circ (i_1, .., i_k) \circ \pi^{-1} = (\pi(i_1), ..., \pi(i_k))$ für alle $\pi \in S_n$.
4. $(i_1, ..., i_k)^k = \mathrm{id}$.

Da Zykel Permutationen von besonders einfacher Form sind, bietet es sich an komplexere Permutationen in Zykel zu zerlegen, also sie als Verkettung von geeigneten Zykeln zu schreiben. Die erste Frage ist, ob man dabei mit Zykeln der Länge zwei, also mit Vertauschungen, oder sogar mit elementaren Vertauschungen auskommt. Da jede elementare Vertauschung die Reihenfolge zweier benachbarter Zahlen verändert, ist es naheliegend, diese Frage zu klären, indem wir Zahlenpaare bilanzieren, deren Reihenfolge von einer Permutation verändert werden.

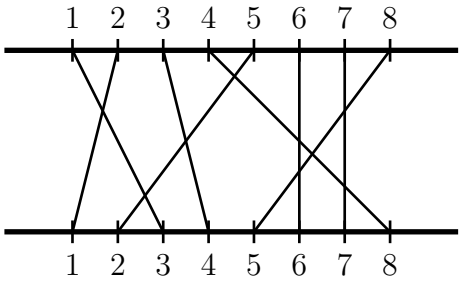
Definition 1.6.4: Sei $\sigma \in S_n$ eine Permutation.

1. Ein **Fehlstandspaar** von σ ist ein Paar (i, j) mit $1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)$.
2. Die Anzahl der Fehlstandspaare heißt die **Länge** von σ und wird mit $\ell(\sigma)$ bezeichnet.
3. Das **Signum** von σ ist $\mathrm{sgn}(\sigma) = (-1)^{\ell(\sigma)}$. Gilt $\mathrm{sgn}(\sigma) = 1$, so nennt man σ **gerade**, gilt $\mathrm{sgn}(\sigma) = -1$ so nennt man σ **ungerade**.

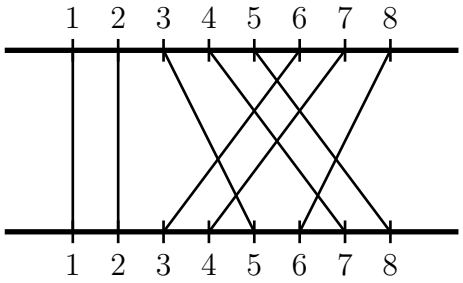
Beispiel 1.6.5.

1. Die Permutation $\mathrm{id} \in S_n$ ist die einzige Permutation mit $\ell(\sigma) = 0$ und somit gerade.
2. Jede elementare Transposition $(i, i+1)$ hat genau ein Fehlstandspaar, nämlich $(i, i+1)$.
3. Eine Vertauschung $\sigma = (i, j)$ mit $i < j$ hat genau $\ell(\sigma) = 2(j - i) - 1$ Fehlstandspaare, nämlich $(i, i+1)$, $(i, i+2)$,...,$(i, j-1)$, (i, j), $(i+1, j)$, $(i+2, j)$,...,$(j-1, j)$. Also gilt $\mathrm{sgn}(\sigma) = -1$.

Man kann die Fehlstandspaare leicht durch eine diagrammatische Beschreibung von Permutationen visualisieren. Dazu zeichnet man für eine Permutation $\sigma \in S_n$ zwei parallele horizontale Linien mit n Punkten, die von links nach rechts mit den Zahlen $1, ..., n$ nummeriert sind. Anschließend verbindet man den Punkt i auf der oberen Gerade durch ein Geradensegment mit dem Punkt $\sigma(i)$ auf der unteren Gerade, so dass sich in jedem Punkt maximal zwei Geradensegmente kreuzen. Letzteres kann man durch ein Verschieben der Punkte auf der oberen und unteren Gerade immer erreichen. Die Länge von σ ist dann die Anzahl der Kreuzungspunkte im Diagramm, denn jeder Kreuzungspunkt entspricht einem Paar (i, j) mit $i < j$ und $\sigma(i) > \sigma(j)$.



Die Permutation
$\sigma = [3, 1, 4, 8, 2, 6, 7, 5] \in S_8$ mit $\ell(\sigma) = 9$



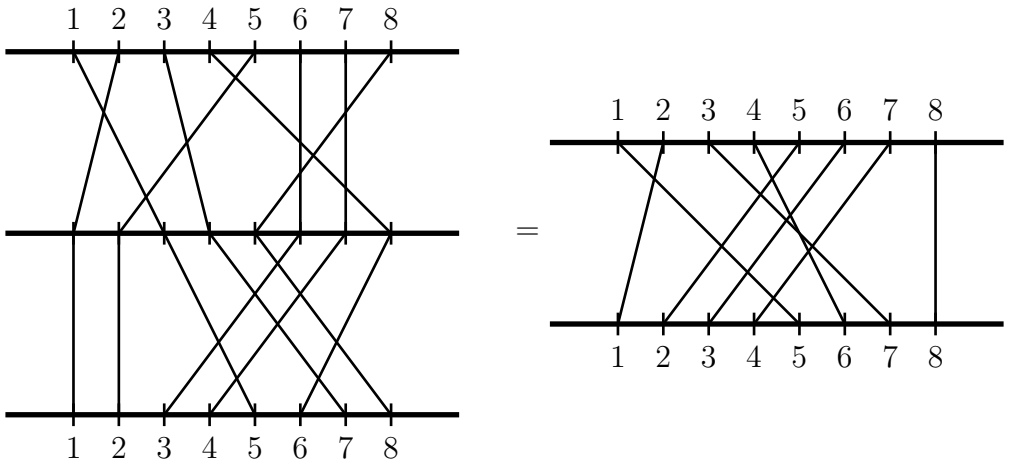
Die Permutation
$\tau = [1, 2, 6, 7, 8, 3, 4, 5] \in S_8$ mit $\ell(\tau) = 8$.

Durch Verketten mit geeigneten elementaren Transpositionen können wir nach und nach die Länge einer Permutation reduzieren, indem wir in jedem Schritt ein Fehlstandspaar eliminieren. Das Verfahren bricht ab, wenn wir eine Permutation der Länge Null erreichen, also die Identitätsabbildung. Damit haben wir die betrachtete Permutation dann als Verkettung elementarer Transpositionen ausgedrückt.

Satz 1.6.6: Jede Permutation $\sigma \in S_n$ lässt sich als Produkt von $l(\sigma)$ elementaren Vertauschungen schreiben.

Beweis:
Induktion über $\ell(\sigma)$. Ist $\ell(\sigma) = 0$, so gilt $\sigma = \mathrm{id}$, und damit ist σ das leere Produkt von elementaren Vertauschungen. Sei die Aussage bewiesen für alle $\tau \in S_n$ mit $l(\tau) < m$ und $\sigma \in S_n$ eine Permutation der Länge $l(\sigma) = m$. Dann gibt es ein ein $i \in \{1, \ldots, n-1\}$ mit $\sigma(i) > \sigma(i+1)$, denn ansonsten wäre $\sigma(1) < \sigma(2) < \ldots < \sigma(n)$ und damit $\sigma = \mathrm{id}$. Die Permutation $\tau = \sigma \circ (i, i+1)$ hat dann ein Fehlstandspaar weniger als σ und damit Länge $\ell(\tau) = \ell(\sigma) - 1 = m - 1$. Nach Induktionsvoraussetzung ist sie damit das Produkt von $\ell(\sigma) - 1$ Vertauschungen. Damit ist $\sigma = (i, i+1) \circ \tau$ ein Produkt von $\ell(\sigma)$ Vertauschungen. □

Das Verhalten der Fehlstandspaare unter der Verkettung von Permutationen lässt sich leicht visualisieren. Das Verketten von Permutationen entspricht nämlich dem Untereinanderstellen der zugehörigen Diagrammen mit anschließendem Glätten der Geradensegmente.



Die Verkettung $\tau \circ \sigma = [1, 2, 5, 7, 8, 3, 4, 6] \circ [3, 1, 4, 8, 2, 6, 7, 5] = [5, 1, 7, 6, 2, 3, 4, 8]$
mit $\ell(\tau \circ \sigma) = 11$.

Während sich beim Untereinanderstellen die Anzahlen der Kreuzungspunkte addieren, vernichtet oder erzeugt das anschließende Glätten *gerade* Anzahlen von Kreuzungspunkten (Warum?). Man kann also nicht erwarten, dass sich die Längen der Permutationen beim Verketten addieren. Da sich die Anzahl durch das Glätten aber nur um *geradzahlig* viele Kreuzungspunkte ändert, multiplizieren sich unter der Verkettung ihre Signa.

Satz 1.6.7: Die Abbildung $\operatorname{sgn} : S_n \to C_2$ ist ein Gruppenhomomorphismus. Ihr Kern

$$A_n = \{\sigma \in S_n \mid \operatorname{sign}(\sigma) = 1\} \subseteq S_n$$

ist ein Normalteiler in S_n mit $\frac{1}{2}n!$ Elementen, falls $n > 1$. Er heißt **alternierende Gruppe**.

Beweis:
Ist σ ein Produkt von k elementaren Vertauschungen, so gilt $\operatorname{sgn}(\sigma) = (-1)^k$, denn jede elementare Vertauschung erzeugt oder vernichtet ein Fehlstandspaar. Ist τ Produkt von l elementaren Vertauschungen ist, so ist $\sigma \circ \tau$ Produkt von $k + l$ elementaren Vertauschungen, und es folgt

$$\operatorname{sgn}(\sigma \circ \tau) = (-1)^{k+l} = (-1)^k \cdot (-1)^l = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau).$$

Da sich jede Permutation nach Satz 1.6.6 als Produkt von elementaren Vertauschungen schreiben lässt, ist sgn damit ein Gruppenhomomorphismus. Wie jeder Kern eines Gruppenhomomorphismus ist A_n ein Normalteiler. Ist $\sigma \in S_n$ eine Vertauschung, so gilt $\sigma \circ \pi \in A_n$ ($\pi \in A_n$) genau dann, wenn $\pi \in S_n \setminus A_n$ ($\sigma \circ \pi \in A_n$). Damit ist $|A_n| = |S_n \setminus A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$. □

Die Zerlegung einer Permutation in elementare Vertauschungen ist zwar nützlich, um das Verhalten des Signums zu untersuchen, hat aber mehrere Nachteile. Der wichtigste ist die mangelnde Eindeutigkeit. Je nachdem, in welcher Reihenfolge einzelne Fehlstandspaare eliminiert werden, entstehen verschiedene Produkte elementarer Vertauschungen, die alle die gleiche Permutation beschreiben. Dies liegt daran, dass die beteiligten elementaren Vertauschungen in der Regel nicht kommutieren. Ein hinreichendes Kriterium dafür, dass zwei Permutationen $\sigma, \tau \in S_n$ kommutieren lässt sich sehr leicht finden. Es reicht aus, dass jede Zahl $i \in \{1, ..., n\}$ ein Fixpunkt von mindestens einer dieser Permutationen ist, also dass die Mengen ihrer nicht-Fixpunkte disjunkt sind. Ist dies der Fall, so nennt man die beiden Permutationen disjunkt.

Definition 1.6.8: Der **Träger** $\operatorname{spt}(\sigma)$ einer Permutation $\sigma \in S_n$ ist die Menge

$$\operatorname{spt}(\sigma) = \{i \in \{1, ..., n\} \mid \sigma(i) \neq i\}.$$

Zwei Permutationen $\sigma, \tau \in S_n$ heißen **disjunkt**, wenn $\operatorname{spt}(\sigma) \cap \operatorname{spt}(\tau) = \emptyset$.

Indem wir bei der Zerlegung der Permutation auch Zykel der Länge > 2 zulassen, können wir erreichen, dass alle beteiligten Zykel in der Zerlegung disjunkt sind und damit kommutieren. Dies liefert eine eindeutigere Zerlegung der Permutation, die sogenannte Zykelzerlegung.

Satz 1.6.9: Jede Permutation $\sigma \in S_n$ ist ein Produkt $\sigma = \tau_1 \circ ... \circ \tau_m$ paarweise disjunkter Zykel τ_j der Länge ≥ 2 für ein $m \in \mathbb{N}_0$. Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Zykel und heißt **Zykelzerlegung** von σ.

Beweis:
Wir betrachten die von σ erzeugte Untergruppe $\langle\sigma\rangle = \{\sigma^k \mid k \in \mathbb{Z}\} \subseteq S_n$ und die Operation $\triangleright : \langle\sigma\rangle \times \{1,...,n\} \to \{1,...,n\}$, $(\sigma^k, i) \mapsto \sigma^k(i)$. Die Bahnen dieser Operation sind gegeben durch $\langle\sigma\rangle \triangleright i = \{\sigma^k(i) \mid k \in \mathbb{Z}\} = \{i, \sigma(i), ..., \sigma^{k_i-1}(i)\}$ mit $k_i = |\langle\sigma\rangle \triangleright i| \in \mathbb{N}$. Sie bilden eine Partition von $\{1,...,n\}$. Ist $R = \{i_1,...,i_m\}$ ein Repräsentantensystem der Bahnen, so erhält man damit m Zykel $\tau_1,...,\tau_m$ mit $\tau_j = (i_j, \sigma(i_j), ..., \sigma^{k_{i_j}-1}(i_j))$ und $\sigma = \tau_1 \circ ... \circ \tau_m$. Da $\tau_j(i) = i$ für alle i, die nicht in der Bahn von i_j liegen, sind diese Zykel paarweise disjunkt, und es folgt $\tau_i \circ \tau_j = \tau_j \circ \tau_i$ für alle $i, j \in \{1,...,m\}$. □

Bemerkung 1.6.10. Die Zykelzerlegung einer Permutation σ kann man auch als die Zerlegung der Menge $\{1,...,n\}$ in die Bahnen der Gruppenoperation

$$\triangleright : \mathbb{Z} \times \{1,...,n\} \to \{1,...,n\}, \quad (k,i) \mapsto \sigma^k(i)$$

sehen. Diese Operation entspricht nach Bemerkung 1.5.2, 2. einem Gruppenhomomorphismus, nämlich dem Gruppenhomomorphismus $f_\sigma : \mathbb{Z} \to S_n$, $k \mapsto \sigma^k$ aus Korollar 1.2.18.

Beispiel 1.6.11. Die Permutationen

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 4 & 3 & 2 & 7 & 5 & 1 & 6 & 10 & 9 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 9 & 6 & 10 & 5 & 1 & 7 & 8 & 2 & 4 \end{pmatrix}$$

haben die Zykelzerlegungen $\sigma = (1,8,6,5,7)(2,4)(9,10)$ und $\tau = (1,3,6)(2,9)(4,10)$. Die Fixpunktmenge σ ist $\{3\}$ und die Fixpunktmenge von τ ist $\{5,7,8\}$.

Der Nachteil der Zykelzerlegung ist, dass sie ein kompliziertes Verhalten unter der Verkettung von Permutationen zeigt. Zerlegt man zwei Permutationen in ihre Zykel so sind die Zykel der zwei Permutationen in der Regel nicht disjunkt und können daher nicht einfach multipliziert werden. Die Zykelzerlegung des Produkts ist also im Allgemeinen nicht das Produkt der Zykelzerlegungen. Die entscheidenden Vorteile der Zykelzerlegung sind ihre Eindeutigkeit und die Tatsache, dass sie sehr gut zur Untersuchung der Konjugationsklassen geeignet ist.

Satz 1.6.12: Zwei Permutationen $\pi, \sigma \in S_n$ sind zueinander konjugiert genau dann, wenn in ihrer Zykelzerlegung jeweils gleich viele Zykel jeder Länge auftreten.

Beweis:
Sind $\pi, \sigma \in S_n$ zueinander konjugiert, so gibt es eine Permutation $\tau \in S_n$ mit $\sigma = \tau \circ \pi \circ \tau^{-1}$. Ist $\pi = \pi_1 \circ ... \circ \pi_m$ die Zykelzerlegung von π, so folgt

$$\sigma = \tau \circ \pi \circ \tau^{-1} = \tau \circ (\pi_1 \circ ... \circ \pi_m) \circ \tau^{-1} = (\tau \circ \pi_1 \circ \tau^{-1}) \circ ... \circ (\tau \circ \pi_m \circ \tau^{-1}) = \sigma_1 \circ ... \circ \sigma_m,$$

und nach Lemma 1.6.3 ist [2] σ_j ein Zykel gleicher Länge wie π_j. Sind umgekehrt $\pi, \sigma \in S_n$ Permutationen in deren Zykelzerlegung jeweils gleich viele Zykel jeder Länge auftreten, so gibt es Zykel $\pi_j = (i_1^j, ..., i_{k_j}^j)$ und $\sigma_j = (l_1^j, ..., l_{k_j}^j)$ mit $\pi = \pi_1 \circ ... \circ \pi_m$ und $\sigma = \sigma_1 \circ ... \circ \sigma_m$. Definieren wir $\tau : \{1,...,n\} \to \{1,...,n\}$ durch $\tau(i_r^j) = l_r^j$ und $\tau(i) = i$ für $i \notin \{i_1^1, ..., i_{k_1}^1, ..., i_1^m, ..., i_{k_m}^m\}$, so ist τ eine Permutation mit $\tau \circ \pi_j \circ \tau^{-1} = \sigma_j$ für alle $j \in \{1,...,m\}$ und daraus folgt $\tau \circ \pi \circ \tau^{-1} = \sigma$. □

[2] nach geeigneter Anordnung der Zykelzerlegung von τ

Beispiel 1.6.13. Die Permutationen $\sigma_1 = (1,2,3) \circ (4,5)$ und $\sigma_2 = (1,2) \circ (3,4,5)$ in S_5 sind zueinander konjugiert. Es gilt $\sigma_2 = \tau\sigma_1\tau^{-1}$ mit $\tau = [3,4,5,1,2]$.

Die Konjugationsklasse einer Permutation ist also durch die Zykelzerlegung eindeutig bestimmt, und letztere ist nach Satz 1.6.9 eindeutig bis auf die Reihenfolge der Zykel. Ordnet man die Zykel so, dass ihre Längen schwach monoton fallen, erhalten wir eine *eindeutige* Charakterisierung der Konjugationsklassen. Da jede Zahl $i \in \{1, ..., n\}$ in genau einem Zykel einer Permutation $\sigma \in S_n$ enthalten ist, addieren sich die Zykellängen zu n, wenn man *auch die Zykel der Länge 1* berücksichtigt, also die Fixpunkte. Damit entsprechen die Konjugationsklassen in der Gruppe S_n genau den *Partitionen* der Zahl n.

Korollar 1.6.14: Konjugationsklassen in der symmetrischen Gruppe S_n stehen in Bijektion mit **Partitionen** von n: Tupeln $(\lambda_1, ..., \lambda_k)$ mit $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_k \geq 1$ und $n = \lambda_1 + ... + \lambda_k$.

Für eine Permutation $\sigma \in S_n$, deren Zykellängen durch die Partition $(\lambda_1, \lambda_2, ..., \lambda_k)$ gegeben sind, gilt $\text{sgn}(\sigma) = (-1)^{n-k}$ und $o(\sigma) = \text{kgV}(\lambda_1, ..., \lambda_k)$.

Beweis:
Nach Lemma 1.6.3 gilt $(i_1, ..., i_k) = (i_1, i_2) \circ (i_2, i_3) \circ \ldots \circ (i_{k-1}, i_k)$. Da $\text{sgn}(i,j) = -1$ und sgn ein Gruppenhomomorphismus ist, folgt $\text{sgn}(i_1, ..., i_\lambda) = (-1)^{\lambda-1}$. Daraus ergibt sich für eine Permutation σ mit Zykellängen $\lambda_1, \lambda_2, ..., \lambda_k$

$$\text{sgn}(\sigma) = (-1)^{\lambda_1-1} \cdot (-1)^{\lambda_2-1} \cdots (-1)^{\lambda_k-1} = (-1)^{\lambda_1+...+\lambda_k-k} = (-1)^{n-k}.$$

Ist $\sigma = \sigma_1 \circ ... \circ \sigma_k$ das Produkt disjunkter λ_i-Zykel σ_i, so gilt $\sigma^n = \sigma_1^n \circ ... \circ \sigma_k^n$ für alle $n \in \mathbb{N}$ und damit $\sigma^n = \text{id}$ genau dann, wenn $\sigma_i^n = \text{id}$ für alle $i = 1, ..., k$. Da σ_i ein Element der Ordnung $o(\sigma_i) = \lambda_i$ ist, ist das kleinste Element $n \in \mathbb{N}$ mit $\sigma_i^n = 1$ für alle $i = 1, ..., k$ das kleinste gemeinsame Vielfache von $\lambda_1, ..., \lambda_k$. □

Beispiel 1.6.15. Wir untersuchen die Konjugationsklassen der symmetrischen Gruppen S_n.

- Die Gruppe $S_1 = \{\text{id}\}$ ist die triviale Gruppe.
- Die Gruppe $S_2 = C_2 = \{\text{id}, (1,2)\}$ ist abelsch und besitzt daher zwei Konjugationsklassen mit je einem Element $C_{\text{id}} = \{\text{id}\}$ und $C_{(1,2)} = \{(1,2)\}$.
- Für die Gruppe S_3 mit $3! = 6$ Elementen erhält man

Partition	Repräsentant	Kardinalität	Signum	Ordnung
3	$(1,2,3)$	2	$+1$	3
$2+1$	$(1,2)$	3	-1	2
$1+1+1$	id	1	$+1$	1

- Für die Gruppe S_4 mit $4! = 24$ Elementen erhält man

Partition	Repräsentant	Kardinalität	Signum	Ordnung
4	$(1,2,3,4)$	6	-1	4
$3+1$	$(1,2,3)$	8	$+1$	3
$2+2$	$(1,2)(3,4)$	3	$+1$	2
$2+1+1$	$(1,2)$	6	-1	2
$1+1+1+1$	id	1	$+1$	1

- Für die Gruppe S_5 mit $5! = 120$ Elementen erhält man

Partition	Repräsentant	Kardinalität	Signum	Ordnung
5	$(1,2,3,4,5)$	24	$+1$	5
$4+1$	$(1,2,3,4)$	30	-1	4
$3+2$	$(1,2,3)(4,5)$	20	-1	6
$3+1+1$	$(1,2,3)$	20	$+1$	3
$2+2+1$	$(1,2)(3,4)$	15	$+1$	2
$2+1+1+1$	$(1,2)$	10	-1	2
$1+1+1+1+1$	id	1	$+1$	1

Konjugationsklassen einer Gruppe G sind insbesondere dann wichtig, wenn man versucht ihre Normalteiler zu bestimmen. Denn per Definition eines Normalteilers $N \subseteq G$ gilt $gng^{-1} \in N$ für alle $g \in G$ und $n \in N$, und damit ist jede Konjugationsklasse eines Elements in N wieder in N enthalten. Jeder Normalteiler N ist also die disjunkte Vereinigung von Konjugationsklassen. Nutzt man aus, dass die Ordnung $|N|$ nach dem Satz von Lagrange ein Teiler der Gruppenordnung ist, so kann man die Normalteiler der Gruppen S_n für kleine n bestimmen.

Beispiel 1.6.16.

- In S_3 gibt es neben der trivialen Untergruppe und S_3 selbst nur Untergruppen der Ordnung 2 oder 3. Da jeder Normalteiler eine disjunkte Vereinigung von Konjugationsklassen ist und das neutrale Element enthalten muss, ergibt sich als einzige Möglichkeit $N = \{\mathrm{id}\} \cup C_{(1,2,3)} = A_3$. Da $|A_3| = \frac{1}{2}|S_3| = 3$ gilt $A_3 \cong C_3$.
- In S_4 kann es neben der trivialen Untergruppe und S_4 selbst nur Normalteiler der Ordnung 2, 3, 4, 6, 12 geben. Die alternierende Gruppe $A_4 = \{\mathrm{id}\} \cup C_{(1,2,3)} \cup C_{(1,2)(3,4)}$ ist nach Satz 1.6.7 ein Normalteiler der Ordnung 12. Da jeder Normalteiler eine disjunkte Vereinigung von Konjugationsklassen ist, die id enthält, ergibt sich aus den Kardinalitäten der Konjugationsklassen als einzige weitere Möglichkeit $N = \{\mathrm{id}\} \cup C_{(1,2)(3,4)}$ mit $|N| = 4$. Man kann nachrechnen, dass dies tatsächlich ein zu $C_2 \times C_2$ isomorpher Normalteiler ist.

Aus Satz 1.6.7 und Beispiel 1.6.16 folgt, dass die alternierende Gruppe $A_3 \cong C_3$ eine zyklische Gruppe der Ordnung 3 und damit nach dem Satz von Lagrange einfach ist. Dagegen enthält die alternierende Gruppe A_4 die Gruppe $C_2 \times C_2$ als Normalteiler, ist also keine einfache Gruppe. Für $n \geq 5$ wird die Untersuchung der Normalteiler der Gruppen A_n und S_n über die Konjugationsklassen schnell sehr kompliziert. Man kann aber mit strukturellen Argumenten zeigen, dass jede alternierende Gruppe A_n für $n \geq 5$ einfach ist. Dazu benötigen wir das folgende Lemma.

Lemma 1.6.17:

1. Für $n \geq 3$ wird die alternierende Gruppe A_n von den 3-Zykeln in S_n erzeugt.
2. Für $n \geq 5$ liegen alle 3-Zykel in A_n in derselben Konjugationsklasse.

Beweis:
1. Jeder 3-Zykel (i,j,k) liegt in A_n, denn nach Lemma 1.6.3 gilt $(i,j,k) = (i,j)(j,k)$ und damit $\mathrm{sgn}(i,j,k) = \mathrm{sgn}(i,j) \cdot \mathrm{sgn}(j,k) = (-1) \cdot (-1) = 1$. Da nach Satz 1.6.6 jede Permutation ein Produkt elementarer Vertauschungen ist und A_n die Untergruppe der geraden Permutationen ist, wird A_n von Permutationen der Form $(i,j)(k,l)$ mit $i,j,k,l \in \{1,..,n\}$ erzeugt. Es reicht also, zu zeigen, dass jede solche Permutation ein Produkt von 3-Zykeln ist. Sind i,j,k,l paarweise verschieden, so gilt $(i,j)(k,l) = (i,k,j)(i,k,l)$. Ansonsten gilt entweder $(i,j) = (k,l)$ und

$(i,j)(k,l) = \mathrm{id}$ ist das leere Produkt von 3-Zykeln, oder wir können ohne Beschränkung der Allgemeinheit annehmen, dass $l = i$. Dann ergibt sich $(i,j)(k,i) = (k,j,i)$.

2. Sei $n \geq 5$ und $\tau = (i,j,k)$ mit $i,j,k \in \{1,...,n\}$ ein 3-Zykel. Wir wählen eine Permutation $\pi' \in S_n$ mit $\pi'(1) = i$, $\pi'(2) = j$ und $\pi'(3) = k$. Ist $\mathrm{sgn}(\pi') = 1$, so setzen wir $\pi = \pi'$. Ist $\mathrm{sgn}(\pi') = -1$, so setzen wir $\pi = \pi' \circ (4,5)$ und erhalten $\pi(1) = i$, $\pi(2) = j$ und $\pi(3) = k$ sowie $\mathrm{sgn}(\pi) = -\mathrm{sgn}(\pi') = 1$. Damit gibt es eine Permutation $\pi \in A_n$ mit $\pi(1) = i$, $\pi(2) = j$ und $\pi(3) = k$, und nach Lemma 1.6.3 gilt $\tau = \pi \circ (1,2,3) \circ \pi^{-1}$. Also liegen alle 3-Zykel in A_n in derselben Konjugationsklasse. □

Können wir zeigen, dass jeder nichttriviale Normalteiler in der Gruppe A_n mindestens einen 3-Zykel enthält, so folgt mit Lemma 1.6.17 direkt, dass die Gruppen A_n für $n \geq 5$ einfach sind. Denn da für $n \geq 5$ alle 3-Zykel nach Lemma 1.6.17 in A_n zueinander konjugiert sind, enthält N dann alle 3-Zykel. Da diese nach Lemma 1.6.17 die ganze Gruppe A_n erzeugen, liegt dann ganz A_n in N. Dies ist in der Tat für alle $n \geq 5$ der Fall.

Satz 1.6.18: Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.

Beweis:
Wir zeigen, dass jeder nichttriviale Normalteiler N in A_n einen 3-Zykel enthält. Da $\{\mathrm{id}\} \neq N$ gibt es eine Permutation $\sigma \in N \setminus \{\mathrm{id}\}$. Da N ein Normalteiler in A_n ist, gilt $\sigma \circ (\tau \circ \sigma^{-1} \circ \tau^{-1}) \in N$ für alle $\tau \in A_n$. Sei nun $\sigma = \sigma_1 \circ ... \circ \sigma_m$ eine Zerlegung von σ in disjunkte Zykel der Länge ≥ 2 wie in Satz 1.6.9, so dass σ_1 ein Zykel maximaler Länge ist.

- **Fall 1:** Ist $\sigma_1 = (i,j,k,l,...)$ ein Zykel der Länge ≥ 4, so können wir $\tau = (i,j,k)$ betrachten, der nach Lemma 1.6.17 in A_n liegt. Da $\mathrm{spt}(\tau) = \{i,j,k\} \subseteq \mathrm{spt}(\sigma_1)$ erhalten wir mit Lemma 1.6.3

$$\begin{aligned}\sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1} &= (\sigma \circ \tau \circ \sigma^{-1}) \circ \tau^{-1} = (\sigma(i), \sigma(j), \sigma(k)) \circ (i,j,k)^{-1} \\ &= (j,k,l) \circ (k,j,i) = (i,l,j) \in N.\end{aligned}$$

- **Fall 2:** Ist $\sigma_1 = (i,j,k)$ ein Zykel der Länge 3, so ist entweder $\sigma = \sigma_1$, und die Aussage ist bewiesen, oder $m \geq 2$ und σ_2 ist von der Form $\sigma_2 = (r,s,t)$ oder $\sigma_2 = (r,s)$. In diesem Fall können wir den 3-Zykel $\tau = (i,j,r) \in A_n$ mit $\mathrm{spt}(\tau) \subseteq \mathrm{spt}(\sigma_1) \cup \mathrm{spt}(\sigma_2)$ betrachten und erhalten mit Lemma 1.6.3

$$\begin{aligned}\sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1} &= (\sigma \circ \tau \circ \sigma^{-1}) \circ \tau^{-1} = (\sigma(i), \sigma(j), \sigma(r)) \circ (i,j,r)^{-1} \\ &= (j,k,s) \circ (r,j,i) = (i,r,k,s,j) \in N.\end{aligned}$$

  Indem wir Fall 1 auf $(i,r,k,s,j) \in N$ anwenden, folgt die Behauptung.

- **Fall 3:** Ist $\sigma_1 = (i,j)$ ein 2-Zykel, so sind auch $\sigma_1, ..., \sigma_m$ 2-Zykel. Da $\mathrm{sgn}(\sigma) = 1 = (-1)^m$, muss dann $m \geq 2$ gelten. Dann ist σ_2 von der Form $\sigma_2 = (k,l)$ mit $\{i,j\} \cap \{k,l\} = \emptyset$, und wegen $n \geq 5$ gibt es ein $r \in \{1,...,n\} \setminus \{i,j,k,l\}$. Wir betrachten den 3-Zykel $\tau = (i,k,r) \in A_n$ und erhalten mit Lemma 1.6.3

$$\begin{aligned}\sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1} &= (\sigma \circ \tau \circ \sigma^{-1}) \circ \tau^{-1} = (\sigma(i), \sigma(k), \sigma(r)) \circ (i,k,r)^{-1} \\ &= (j,l,\sigma(r)) \circ (r,k,i) \in N.\end{aligned}$$

  Falls $\sigma(r) = r$, folgt $(j,l,\sigma(r)) \circ (r,k,i) = (r,k,i,j,l) \in N$ und mit Fall 1 die Behauptung. Ansonsten sind $(j,l,\sigma(r))$ und (r,k,i) disjunkt, und mit Fall 2 folgt die Behauptung.

Damit ist gezeigt, dass jeder Normalteiler $N \subseteq A_n$ einen 3-Zykel σ enthält. Da nach Lemma 1.6.17 alle 3-Zykel in A_n zu σ konjugiert sind und N ein Normalteiler ist, liegen alle 3-Zykel in N. Da die 3-Zykel nach Lemma 1.6.17 die alternierende Gruppe A_n erzeugen, folgt $N = A_n$. □

Bemerkung 1.6.19. Man kann zeigen, dass A_5 die kleinste nicht-abelsche einfache Gruppe ist. Die nächstgrößere hat 168 Elemente.

1.7 Endlich erzeugte abelsche Gruppen

1.7.1 Zyklische Gruppen

In diesem Abschnitt befassen wir uns mit endlich erzeugten abelschen Gruppen und werden schließlich alle endlich erzeugten abelschen Gruppen bis auf Isomorphie klassifizieren. Das Ziel ist also eine Liste von endlich erzeugten abelschen Gruppen, so dass jede endlich erzeugte abelsche Gruppe isomorph zu genau einer endlich erzeugten abelschen Gruppe in der Liste ist. Wir beginnen unsere Untersuchung mit den zyklischen Gruppen. Wir haben bereits gezeigt, dass alle zyklischen Gruppen abelsch sind (Korollar 1.2.17) und jede Gruppe von Primzahlordnung zyklisch ist (Korollar 1.3.10). Indem wir die Ergebnisse zu Faktorgruppen ausnutzen, können wir alle zyklischen Gruppen als Faktorgruppen von $\mathbb{Z}$ beschreiben.

Satz 1.7.1: Sei G eine zyklische Gruppe. Dann gilt

$$G \cong \begin{cases} \mathbb{Z} & |G| = \infty \\ \mathbb{Z}/n\mathbb{Z} & |G| = n. \end{cases}$$

Beweis:
Wir betrachten $G = \langle g \rangle$ und den surjektiven Gruppenhomomorphismus $f_g : \mathbb{Z} \to G$, $k \mapsto g^k$ aus Korollar 1.2.18. Sein Kern ist eine Untergruppe von $\mathbb{Z}$ und damit nach Beispiel 1.2.6 von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$. Ist $n = 0$, so erhält man $\ker f_g = 0$, und damit ist f_g ein Isomorphismus. Ist $n > 0$, so erhält man mit dem Homomorphiesatz 1.3.23 einen Isomorphismus $f_g/\ker f_g : \mathbb{Z}/n\mathbb{Z} \to G$, $\bar{k} \mapsto g^k$. □

Beispiel 1.7.2. Die Gruppe $C_n = \{e^{2\pi ik/n} \mid k = 0, 1, ..., n-1\}$ der $n$ten Einheitswurzeln aus Beispiel 1.2.4 ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$. Denn die Abbildung $f_n : \mathbb{Z} \to C_n$, $k \mapsto e^{2\pi ik/n}$ ist wegen der Identität $e^{ix} \cdot e^{iy} = e^{i(x+y)}$ für alle $x, y \in \mathbb{R}$ ein surjektiver Gruppenhomomorphismus. Ihr Kern ist $\ker f_n = n\mathbb{Z} \subset \mathbb{Z}$, und mit dem Homomorphiesatz folgt $C_n \cong \mathbb{Z}/n\mathbb{Z}$.

Korollar 1.7.3: Jede Gruppe G von Primzahlordnung $|G| = p$ ist isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Beweis:
Nach Korollar 1.3.10 ist jede Gruppe G mit $|G| = p$ prim zyklisch, und mit Satz 1.7.1 folgt $G \cong \mathbb{Z}/p\mathbb{Z}$. □

Wir untersuchen nun noch systematisch die Unter- und Faktorgruppen zyklischer Gruppen. Für Gruppen von Primzahlordnung ist bereits bekannt, dass sie außer sich selbst und der trivialen Untergruppe keine weiteren Untergruppen haben. Für die zyklische Gruppe $\mathbb{Z}$ ist aus Beispiel 1.2.6 bekannt dass jede Untergruppe entweder wieder isomorph zu $\mathbb{Z}$ oder die triviale Gruppe ist. Im Allgemeinen können zyklische Gruppen aber durchaus auch andere Untergruppen haben. Beispielsweise hat die Gruppe $\mathbb{Z}/6\mathbb{Z}$ die Untergruppen $\{\bar{0}, \bar{3}\} \cong \mathbb{Z}/2\mathbb{Z}$ und $\{\bar{0}, \bar{2}, \bar{4}\} \cong \mathbb{Z}/3\mathbb{Z}$. Um der Frage auf den Grund zu gehen, welche Gruppen auftreten können, stellen wir zunächst fest, dass Untergruppen und Faktorgruppen zyklischer Gruppen wieder zyklisch sind.

Korollar 1.7.4: Jede Untergruppe und jeder Quotient einer zyklischen Gruppe ist zyklisch.

Beweis:
1. Sei $G = \langle g \rangle$ zyklisch und $H \subseteq G$ eine Untergruppe. Dann wird der Quotient G/H von der Nebenklasse gH erzeugt, ist also wieder zyklisch.

2. Um zu sehen, dass H zyklisch ist, betrachten wir den Homomorphismus $f_g : \mathbb{Z} \to G$, $k \mapsto g^k$. Dann ist $K := f_g^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$ und nach Beispiel 1.2.6 von der Form $K = n\mathbb{Z}$ mit $n \in \mathbb{N}_0$. Ist $n = 0$ so ist K die triviale Gruppe und damit zyklisch. Für $n > 0$ gilt $n\mathbb{Z} \cong \mathbb{Z}$ nach Beispiel 1.2.6, und damit ist K zyklisch. Da f_g surjektiv ist, gilt $H = f_g(K) \cong K/\ker f_g$ und damit ist H nach 1. zyklisch. □

Für die Ordnung von Untergruppen endlicher zyklischer Gruppen kommen nach dem Satz von Lagrange nur Teiler der Gruppenordnung in Frage. Die Frage ist, ob auch zu allen Teilern der Gruppenordnung Untergruppen existieren, und wie viele davon auftreten können. Es stellt sich heraus, dass für zyklische Gruppen die bestmögliche Umkehrung des Satzes von Lagrange gilt.

Satz 1.7.5: Sei G eine zyklische Gruppe mit $|G| = n < \infty$. Dann hat G zu jedem positiven Teiler d von n genau eine Untergruppe der Ordnung d.

Beweis:
Da G endlich und zyklisch ist, können wir mit Satz 1.7.1 annehmen, dass $G = \mathbb{Z}/n\mathbb{Z}$. Wir betrachten die kanonische Surjektion $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \bar{k}$. Nach der Untergruppenkorrespondenz 1.3.19 entsprechen Untergruppen $H' \subseteq G$ genau den Untergruppen $H \subseteq \mathbb{Z}$, die die Untergruppe $\ker \pi = n\mathbb{Z}$ enthalten. Letztere sind nach Beispiel 1.2.6 von der Form $H = m\mathbb{Z}$ für ein $m \geq 0$, und es gilt $n\mathbb{Z} \subseteq m\mathbb{Z}$ genau dann, wenn $n \in m\mathbb{Z}$, also wenn m ein Teiler von n ist. Also entsprechen die Untergruppen von G genau den Teilern von n.

Für jeden Teiler m von n ist $H' = \pi(H) = m\mathbb{Z}/n\mathbb{Z}$, und die Division durch m definiert einen Gruppenisomorphismus $f : H' \to \mathbb{Z}/\frac{n}{m}\mathbb{Z}$, $\overline{mk} \mapsto \bar{k}$. Also gilt $H' \cong \mathbb{Z}/\frac{n}{m}\mathbb{Z}$ und $|H| = \frac{n}{m}$. Da mit m auch $\frac{n}{m}$ alle Teiler von n durchläuft, ist die Behauptung bewiesen. □

Noch expliziter können wir die endlichen zyklischen Gruppen mit Hilfe des sogenannten chinesischen Restsatzes beschreiben. Er erlaubt es uns, die endlichen zyklischen Gruppen $\mathbb{Z}/n\mathbb{Z}$ als Produkte von zyklischen Gruppen von Primpotenzordnung zu beschreiben, indem wir die Zahl n in teilerfremde Primpotenzen zerlegen.

Satz 1.7.6 (Chinesischer Restsatz):
Sind $m, n \in \mathbb{N}$ teilerfremd, so erhält man einen Gruppenisomorphismus

$$\varrho : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$$

Beweis:
Die Abbildung $\varrho' : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $z \mapsto (z + m\mathbb{Z}, z + n\mathbb{Z})$ ist ein Homomorphismus mit

$$\ker(\varrho') = n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{kgV}(m, n)\mathbb{Z} = mn\mathbb{Z}.$$

Nach dem Homomorphiesatz induziert sie einen injektiven Gruppenhomomorphismus

$$\varrho = \varrho'/\ker\varrho' : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ z + mn\mathbb{Z} \mapsto (z + m\mathbb{Z}, z + n\mathbb{Z}).$$

Da $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ beides endliche Mengen mit mn Elementen sind, ist ϱ als injektive Abbildung auch bijektiv, und damit ein Gruppenisomorphismus. □

Korollar 1.7.7: Jede endliche zyklische Gruppe ist isomorph zu einer Gruppe der Form

$$\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

mit paarweise teilerfremden Primzahlen $p_1, ..., p_k \in \mathbb{N}$, $k \in \mathbb{N}_0$ und $n_1, ..., n_k \in \mathbb{N}$.

1.7.2 Klassifikation der endlich erzeugten abelschen Gruppen

Nachdem im letzten Abschnitt gezeigt wurde, dass jede zyklische Gruppe isomorph ist zu $\mathbb{Z}$ oder zu einer Gruppe $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}$, zeigen wir nun, dass jede *endlich erzeugte* abelsche Gruppe isomorph ist zu einem Produkt solcher Gruppen. Anschließend untersuchen wir, welche solchen Produkte zueinander isomorph sind. Sind beide Fragen beantwortet, so haben wir die abelschen Gruppen bis auf Isomorphie vollständig klassifiziert. Da wir isomorphe Gruppen nicht unterscheiden, kennen wir damit alle endlich erzeugten abelschen Gruppen. Da wir nun auch mehrere Erzeuger zulassen, arbeiten wir statt mit $\mathbb{Z}$ mit den Gruppen

$$\mathbb{Z}^m = \mathbb{Z} \times \ldots \times \mathbb{Z} = \{(z_1, \ldots, z_m) \mid z_1, \ldots, z_m \in \mathbb{Z}\},$$

wobei jede Kopie von $\mathbb{Z}$ einem Erzeuger entspricht. Diese Gruppen sind offensichtlich endlich erzeugt, denn sie werden von den m Elementen $e_i = (0, ..., 0, 1, 0, ..., 0)$ erzeugt, den sogenannten **kanonischen Erzeugern**, die im $i$ten Eintrag eine Eins und ansonsten nur Nullen enthalten. Wir benutzen im Folgenden die additive Notation für abelsche Gruppen.

Zunächst klären wir, wie sich die Eigenschaft *endlich erzeugt zu sein* unter Gruppenhomomorphismen verhält. Es stellt sich heraus, dass sie unter surjektiven Gruppenhomomorphismen erhalten bleibt und sich damit auf Faktorgruppen überträgt.

Lemma 1.7.8:

1. Bilder endlich erzeugter Gruppen unter Gruppenhomomorphismen sind endlich erzeugt.
2. Faktorgruppen endlich erzeugter Gruppen sind endlich erzeugt.
3. Sind der Kern und das Bild eines Gruppenhomomorphismus $f : G \to H$ endlich erzeugt, so ist auch G endlich erzeugt.

Beweis:
1. Sei $G = \langle g_1, ..., g_m \rangle$ endlich erzeugt und $f : G \to H$ ein Gruppenhomomorphismus. Dann ist $K := f^{-1}(\langle f(g_1), ..., f(g_m) \rangle)$ eine Untergruppe von G mit $g_1, ..., g_m \in K$. Daraus ergibt sich $G = \langle g_1, ..., g_m \rangle = K$ und $f(G) = f(K) = \langle f(g_1), ..., f(g_m) \rangle$.

2. Ist G endlich erzeugt und $N \subseteq G$ ein Normalteiler, so ist $\pi : G \to G/N$, $g \mapsto gN$ ein surjektiver Gruppenhomomorphismus, und nach 1. ist G/N damit endlich erzeugt.

3. Sei $f : G \to H$ ein Gruppenhomomorphismus, $f(G) = \langle h_1, ..., h_m \rangle$, $\ker f = \langle k_1, \ldots, k_n \rangle$ und $g_i \in f^{-1}(h_i)$ für $i = 1, ..., m$. Wegen $\ker f = \langle k_1, \ldots, k_n \rangle \subseteq \langle g_1, \ldots, g_m, k_1, \ldots, k_n \rangle$ entspricht $\langle g_1, \ldots, g_m, k_1, \ldots, k_n \rangle$ nach der Untergruppenkorrespondenz 1.3.19 der Untergruppe $f(\langle g_1, ..., g_n \rangle) = \langle h_1, ..., h_n \rangle = f(G)$. Damit gilt $\langle g_1, \ldots, g_m, k_1, \ldots, k_n \rangle = G$. □

Obwohl es auf den ersten Blick plausibel erscheint, dass auch Untergruppen endlich erzeugter Gruppen endlich erzeugt sein könnten, ist dies im Allgemeinen nicht der Fall. Dies liegt daran, dass die Erzeuger der Gruppe nicht in der Untergruppe enthalten sein müssen. Untergruppe einer endlich erzeugten Gruppe zu sein sagt sehr wenig über die Struktur einer Gruppe aus.

Beispiel 1.7.9. Die von den Matrizen

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \tag{1.4}$$

erzeugte Untergruppe $G = \langle A, B \rangle \subseteq \mathrm{GL}(2, \mathbb{Q})$ ist per Definition endlich erzeugt, aber ihre Untergruppe $H = \{C \in G \mid c_{11} = c_{22} = 1\}$ ist nicht endlich erzeugt. Sie ist isomorph zu einer nicht endlich erzeugten Untergruppe von $(\mathbb{Q}, +)$ (Übung).

Wir werden nun zeigen, dass Untergruppen endlich erzeugter *abelscher* Gruppen immer endlich erzeugt sind. Als ersten Schritt untersuchen wir dafür die Gruppen $\mathbb{Z}^m$, aus denen wir später alle endlich erzeugten abelschen Gruppen als Faktorgruppen konstruieren werden.

Lemma 1.7.10: Jede Untergruppe der Gruppe $\mathbb{Z}^m$ wird von maximal m Elementen erzeugt.

Beweis:
Induktion über m. Der Fall $m = 0$ ist trivial. Sei die Aussage bewiesen für alle $m \leq k - 1$ und $H \subseteq \mathbb{Z}^k$ eine Untergruppe. Wir betrachten den Gruppenhomomorphismus

$$p_k : \mathbb{Z}^k \to \mathbb{Z},\ (a_1, \ldots, a_k)^T \mapsto a_k$$

mit Kern $\ker p_k = \{(a_1, \ldots, a_{k-1}, 0) \mid a_1, \ldots, a_{k-1} \in \mathbb{Z}\} \cong \mathbb{Z}^{k-1}$ und seine Einschränkung $p_k|_H : H \to \mathbb{Z}$. Ihr Kern $\ker(p_k|_H) = \ker p_k \cap H$ ist isomorph zu einer Untergruppe von $\mathbb{Z}^{k-1}$ und damit nach Induktionsvoraussetzung durch maximal $k - 1$ Elemente erzeugt. Das Bild $p_k(H) \subseteq \mathbb{Z}$ ist nach Beispiel 1.2.6 als Untergruppe von $\mathbb{Z}$ von maximal einem Element erzeugt. Aus dem Beweis von Lemma 1.7.8, 3. folgt, dass H von maximal k Elementen erzeugt wird. □

Um nun andere endlich erzeugte abelsche Gruppen zu untersuchen, konstruieren wir Gruppenhomomorphismen $f : \mathbb{Z}^m \to G$. Genauso wie es nach Korollar 1.2.18 zu jedem Element $g \in G$ einer beliebigen Gruppe G immer genau einen Gruppenhomomorphismus $f_g : \mathbb{Z} \to \langle g \rangle$, $k \mapsto g^k$

mit $f(1) = g$ gibt, können wir für eine *abelsche* Gruppe G beliebig viele Elemente $g_1, ..., g_m \in G$ vorgeben und erhalten dann genau einen Gruppenhomomorphismen $f : \mathbb{Z}^m \to G$ mit $f(e_i) = g_i$. Können wir einen surjektiven Gruppenhomomorphismus dieser Form finden, so ist die abelsche Gruppe nach dem Homomorphiesatz dann isomorph zu einer Faktorgruppe von $\mathbb{Z}^m$.

Satz 1.7.11: Sei G eine abelsche Gruppe. Dann gilt:

1. Zu beliebigen Elementen $g_1, ..., g_m \in G$ gibt es genau einen Gruppenhomomorphismus $f : \mathbb{Z}^m \to G$ mit $f(e_i) = g_i$ für $i = 1, \ldots, m$, nämlich
$$f : \mathbb{Z}^m \to G,\ (z_1, \ldots, z_m) \mapsto z_1 g_1 + \ldots + z_m g_m. \tag{1.5}$$
2. Die Gruppe G ist endlich erzeugt genau dann, wenn es einen surjektiven Gruppenhomomorphismus $f : \mathbb{Z}^m \to G$ gibt für ein $m \in \mathbb{N}_0$.
3. Jede endlich erzeugte abelsche Gruppe ist isomorph zu einer Faktorgruppe $\mathbb{Z}^m/U$ mit einer Untergruppe $U \subseteq \mathbb{Z}^m$.

Beweis:
1. Die Abbildung f erfüllt die Bedingungen $f(e_i) = g_i$ für $i = 1, ..., m$ und ist ein Gruppenhomomorphismus, denn es gilt

$$\begin{aligned} &f((z_1, ..., z_m) + (z'_1, ..., z'_m)) = f(z_1 + z'_1, ..., z_m + z'_m) = (z_1 + z'_1)g_1 + ... + (z_m + z'_m)g_m \\ &= z_1 g_1 + z'_1 g_1 + ... + z_m g_m + z'_m g_m = f(z_1, ..., z_m) + f(z'_1, ..., z'_m). \end{aligned}$$

Ist umgekehrt $f' : \mathbb{Z}^m \to G$ ein Gruppenhomomorphismus mit $f'(e_i) = g_i$, so folgt

$$\begin{aligned} f'(z_1, ..., z_m) &= f'(z_1 e_1 + ... + z_m e_m) = z_1 f'(e_1) + \ldots + z_m f'(e_m) = z_1 g_1 + \ldots + z_m g_m \\ &= f(z_1, ..., z_m) \quad \forall z_1, ..., z_m \in \mathbb{Z}. \end{aligned}$$

2. Ist $G = \langle g_1, ..., g_m \rangle$ endlich erzeugt, so gibt es nach 1. einen Gruppenhomomorphismus $f : \mathbb{Z}^m \to G$ mit $f(e_i) = g_i$. Daraus folgt $G = \langle g_1, ..., g_m \rangle \subseteq f(\mathbb{Z}^m)$ und damit ist f surjektiv. Gibt es umgekehrt einen surjektiven Gruppenhomomorphismus $f : \mathbb{Z}^m \to G$, dann gilt nach Lemma 1.7.8 wegen $\mathbb{Z}^m = \langle e_1, ..., e_m \rangle$ auch $G = \langle f(e_1), \ldots, f(e_m) \rangle$, und G ist endlich erzeugt.

3. Nach 2. gibt es zu jeder endlich erzeugten abelschen Gruppe einen surjektiven Gruppenhomomorphismus $f : \mathbb{Z}^m \to G$. Mit dem Homomorphiesatz folgt daraus $G \cong \mathbb{Z}^m / \ker f$. □

Korollar 1.7.12: Untergruppen endlich erzeugter abelscher Gruppen sind endlich erzeugt

Beweis:
Ist G endlich erzeugt, so gibt es nach Satz 1.7.11 einen surjektiven Gruppenhomomorphismus $f : \mathbb{Z}^m \to G$. Für jede Untergruppe $U \subseteq G$ ist $f^{-1}(U) \subseteq \mathbb{Z}^m$ eine Untergruppe und damit endlich erzeugt nach Lemma 1.7.10 . Die Einschränkung $f' : f^{-1}(U) \to U$, $x \mapsto f(x)$ ist ein surjektiver Gruppenhomomorphismus, und mit dem Homomorphiesatz folgt $U \cong f^{-1}(U)/\ker f'$. Da $f^{-1}(U)$ endlich erzeugt ist, gilt das nach Lemma 1.7.8, 2. auch für $U \cong f^{-1}(U)/\ker f'$. □

Wir werden nun die endlich erzeugten abelschen Gruppen genauer untersuchen, indem wir sie wie in Satz 1.7.11 als Faktorgruppen einer Gruppe $\mathbb{Z}^m$ bezüglich einer geeigneten Untergruppe $U \subseteq \mathbb{Z}^m$ beschreiben. Entscheidende Vereinfachungen ergeben sich dadurch, dass wir die Erzeuger dieser Untergruppe durch eine ganzzahlige Matrix beschreiben. Nach Satz 1.7.10 wird

nämlich jede Untergruppe $U \subseteq \mathbb{Z}^m$ von maximal m Erzeugern erzeugt, ist also von der Form $U = \langle k_1, ..., k_n \rangle$ mit $n \leq m$ und $k_i \in \mathbb{Z}^m$. Indem wir die Erzeuger $k_1, ..., k_n \in \mathbb{Z}^m$ als Spaltenvektoren schreiben und nebeneinanderstellen, erhalten wir eine Matrix $A \in \mathrm{Mat}(m \times n, \mathbb{Z})$. Dies ist nichts anderes als eine Präsentation der Gruppe $\mathbb{Z}^m/U$, die aufgrund der Abelizität eine einfachere Form annimmt.

Definition 1.7.13: Für $n \leq m$ und $A = (k_1, ..., k_n) \in \mathrm{Mat}(m \times n, \mathbb{Z})$ schreiben wir $\mathbb{Z}^m/A\mathbb{Z}^n$ für die Faktorgruppe $\mathbb{Z}^m/U$ mit $U = \langle k_1, ..., k_n \rangle \subseteq \mathbb{Z}^m$. Einen Isomorphismus $f : \mathbb{Z}^m/A\mathbb{Z}^n \to G$ in eine abelsche Gruppe G bezeichnet man als eine **Präsentation** von G.

Beispiel 1.7.14. Ist $A = (a_{ij}) \in \mathrm{Mat}(m \times n, \mathbb{Z})$ mit $n \leq m$ eine Diagonalmatrix, also eine Matrix mit $a_{ij} = 0$ für $i \neq j$, so ist die Untergruppe $U = A\mathbb{Z}^n = \langle a_{11}e_1, ..., a_{nn}e_n \rangle$, und es folgt

$$\mathbb{Z}^m/A\mathbb{Z}^n \cong \mathbb{Z}/a_{11}\mathbb{Z} \times \ldots \times \mathbb{Z}/a_{nn}\mathbb{Z} \times \mathbb{Z}^{m-n}.$$

Der Fall einer Diagonalmatrix ist offensichtlich besonders einfach, da wir die Gruppe $\mathbb{Z}^m/A\mathbb{Z}^n$ dann direkt als Produkt von zyklischen Gruppen schreiben können. Allgemein ist die Präsentation einer abelschen Gruppe durch eine Matrix alles andere als eindeutig. Wir können etwa die Erzeuger der Untergruppe A$\mathbb{Z}^n$ permutieren, sie mit -1 multiplizieren oder ganzzahlige Vielfache eines Erzeugers zu einem anderen dazuaddieren, ohne die Untergruppe zu ändern. Die entspricht genau den elementaren Spaltenoperationen auf der Matrix A aus dem Gauß-Verfahren. Die gleichen Umformungen können wir auf die Erzeuger der Gruppe $\mathbb{Z}^n$ anwenden, was entsprechenden Zeilenoperationen entspricht. Die einzigen Unterschiede zum Gauß-Verfahren für Matrizen mit Einträgen in einem Körper ist, dass nur *ganzzahlige* Vielfache von Zeilen und Spalten zu anderen Zeilen oder Spalten addiert werden werden und dass nur Multiplikation einer Zeile oder Spalte mit -1 erlaubt ist.

Definition 1.7.15: Sei $A \in \mathrm{Mat}(m \times n, \mathbb{Z})$ eine ganzzahlige Matrix. Die folgenden Transformationen heißen **elementare Operationen** auf A:

(E1) Addieren eines ganzzahligen Vielfachen einer Zeile (Spalte) zu einer anderen Zeile (Spalte).

(E2) Vertauschen zweier Zeilen (Spalten).

(E3) Multiplikation einer Zeile (Spalte) mit -1.

Zwei Matrizen $A, B \in \mathrm{Mat}(m \times n, \mathbb{Z})$ heißen **äquivalent**, wenn es eine endliche Folge von elementaren Operationen gibt, die die Matrix A in B überführt.

Da sich jede elementare Operation offensichtlich durch eine andere elementare Operation umkehren lässt, ist die Äquivalenz von ganzzahligen Matrizen tatsächlich eine Äquivalenzrelation. Dieses Umkehren garantiert die Symmetrie, während Reflexivität und Transitivität trivialerweise erfüllt sind. Wie auch im Gauß-Verfahren lassen sich die elementaren Operationen durch Links- und Rechtsmultiplikation der Matrix mit Elementarmatrizen beschreiben.

Bemerkung 1.7.16. Die Matrizen

$$M^j = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & & \vdots \\ \vdots & & \ddots & -1 & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 & 1 \end{pmatrix} \qquad M^j_{li} = \begin{cases} 1 & l = i \neq j \\ -1 & l = i = j \\ 0 & \text{sonst} \end{cases}$$

$$V^{jk} = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 0 & \dots & 1 & & \vdots \\ \vdots & & \vdots & 1 & \vdots & & \vdots \\ \vdots & & 1 & \dots & 0 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 & 1 \end{pmatrix} \qquad V^{jk}_{li} = \begin{cases} 1 & l = i \notin \{j,k\} \\ 1 & \{l,i\} = \{j,k\} \\ 0 & \text{sonst} \end{cases}$$

$$A^{jk}(z) = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & z & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 & 1 \end{pmatrix} \qquad A^{jk}(z)_{li} = \begin{cases} 1 & i = l \\ z & l = j, i = k\,, \\ 0 & \text{sonst,} \end{cases} \qquad z \in \mathbb{Z}$$

heißen **Elementarmatrizen**. Sie sind invertierbar mit Inversen $(M^j)^{-1} = M^j$, $(V^{jk})^{-1} = V^{jk}$, $A^{jk}(z)^{-1} = A^{jk}(-z)$. Für jede Matrix A $\in \mathrm{Mat}(m \times n, \mathbb{Z})$ entspricht

- die Linksmultiplikation $A \mapsto M^j \cdot A$ (Rechtsmultiplikation $A \mapsto A \cdot M^j$) der Multiplikation der $j$ten Zeile (Spalte) von A mit -1,
- die Linksmultiplikation $A \mapsto V^{jk} \cdot A$ (Rechtsmultiplikation $A \mapsto A \cdot V^{jk}$) dem Vertauschen der $j$ten und $k$ten Zeile (Spalte) von A,
- die Linksmultiplikation $A \mapsto A^{jk}(z) \cdot A$ (Rechtsmultiplikation $A \mapsto A \cdot A^{jk}(z)$) dem Addieren der mit $z \in \mathbb{Z}$ multiplizierten $k$ten Zeile (Spalte) zur $j$ten Zeile (Spalte) von A.

Eine kleinere Schwierigkeit ist, dass für invertierbare Matrizen mit ganzzahligen Einträgen die Inverse nicht unbedingt ganzzahlige, sondern nur rationale Einträge haben müssen. Dies ist jedoch kein ernsthaftes Problem, da ganzzahlige Matrizen mit ganzzahligen Inversen eine Untergruppe von $\mathrm{GL}(n, \mathbb{Q})$ bilden, die die Elementarmatrizen enthält.

Lemma 1.7.17: Die invertierbaren ganzzahligen $(n \times n)$-Matrizen mit ganzzahligen Inversen bilden eine Untergruppe $\mathrm{GL}(n, \mathbb{Z}) \subseteq \mathrm{GL}(n, \mathbb{Q})$.

Beweis:
Offensichtlich gilt $\mathbb{1}_n \in \mathrm{GL}(n, \mathbb{Z})$ (UG2). Sind $A, B \in \mathrm{GL}(n, \mathbb{Z})$, so sind A, B ganzzahlig mit ganzzahligen Inversen A^{-1}, B^{-1}. Damit ist per Definition der Matrixmultiplikation auch AB ganzzahlig mit ganzzahligem Inversen $(AB)^{-1} = B^{-1}A^{-1}$ und damit $AB \in \mathrm{GL}(n, \mathbb{Z})$ (UG1). Da A^{-1} ganzzahlig mit ganzzahligem Inversen A ist, ist auch $A^{-1} \in \mathrm{GL}(n, \mathbb{Z})$ (UG3). □

Können wir nun zeigen, dass Matrizen in $\mathrm{Mat}(m \times n, \mathbb{Z})$, die durch Linksmultiplikation mit Elementen von $\mathrm{GL}(m, \mathbb{Z})$ und Rechtsmultiplikation mit Elementen von $\mathrm{GL}(n, \mathbb{Z})$ auseinander hervorgehen, isomorphe Faktorgruppen von $\mathbb{Z}^m$ definieren, so ergibt sich aus Bemerkung 1.7.16 direkt, dass elementare Operationen die Isomorphieklasse die zugehörige Faktorgruppe nicht ändern. Wir können dann diese ganzzahlige Variante des Gauß-Verfahrens benutzen, um die zugehörigen Matrizen zu vereinfachen.

Lemma 1.7.18: Sind $A, B \in \mathrm{Mat}(m \times n, \mathbb{Z})$ und $S \in \mathrm{GL}(m, \mathbb{Z})$, $T \in \mathrm{GL}(n, \mathbb{Z})$ mit $B = SAT$, so sind die Gruppen $\mathbb{Z}^m / A\mathbb{Z}^n$ und $\mathbb{Z}^m / B\mathbb{Z}^n$ zueinander isomorph.

Beweis:
Die Abbildungen $f_S : \mathbb{Z}^m \to \mathbb{Z}^m$, $v \mapsto S \cdot v$ und $f_T : \mathbb{Z}^n \to \mathbb{Z}^n$, $w \mapsto T \cdot w$ sind Gruppenhomomorphismen mit Inversen $f_S^{-1} = f_{S^{-1}}$ und $f_T^{-1} = f_{T^{-1}}$, also Gruppenautomorphismen. Damit gilt $T\mathbb{Z}^n = f_T(\mathbb{Z}^n) = \mathbb{Z}^n$, und $f : \mathbb{Z}^m \to \mathbb{Z}^m / B\mathbb{Z}^n$, $v \mapsto Sv + B\mathbb{Z}^n$ ist ein surjektiver Gruppenhomomorphismus mit $\ker f = \{v \in \mathbb{Z}^m \mid Sv \in B\mathbb{Z}^n\} = \{v \in \mathbb{Z}^m \mid Sv \in SAT\mathbb{Z}^n\} = AT\mathbb{Z}^n = A\mathbb{Z}^n$. Nach dem Isomorphiesatz induziert er einen Gruppenisomorphismus

$$f/\ker f : \mathbb{Z}^m / A\mathbb{Z}^n \to \mathbb{Z}^m / B\mathbb{Z}^n,\ v + A\mathbb{Z}^n \mapsto Sv + B\mathbb{Z}^n.$$

□

Korollar 1.7.19: Sind $A, B \in \mathrm{Mat}(m \times n, \mathbb{Z})$ mit $n \leq m$ äquivalent, so sind die Gruppen $\mathbb{Z}^m / A\mathbb{Z}^n$ und $\mathbb{Z}^m / B\mathbb{Z}^n$ isomorph.

Beweis:
$A, B \in \mathrm{Mat}(m \times n, \mathbb{Z})$ äquivalent, so lassen sie sich durch endlich viele elementare Zeilen- und Spaltenoperationen ineinander überführen. Diese entsprechen nach Bemerkung 1.7.16 respektive der Linksmultiplikation mit Matrizen in $\mathrm{GL}(m, \mathbb{Z})$ und der Rechtsmultiplikation mit Matrizen in $\mathrm{GL}(n, \mathbb{Z})$. Also gibt es Matrizen $S_1, ..., S_s \in \mathrm{GL}(m, \mathbb{Z})$ und $T_1, ..., T_t \in \mathrm{GL}(n, \mathbb{Z})$ mit $B = S_1 \cdots S_s A T_1 \cdots T_t$, und da $\mathrm{GL}(m, \mathbb{Z}) \subseteq \mathrm{GL}(m, \mathbb{Q})$ und $\mathrm{GL}(n, \mathbb{Z}) \subseteq \mathrm{GL}(n, \mathbb{Q})$ Untergruppen sind, gilt $S = S_1 \cdots S_s \in \mathrm{GL}(m, \mathbb{Z})$ und $T = T_1 \cdots T_t \in \mathrm{GL}(n, \mathbb{Z})$. Mit Lemma 1.7.18 folgt dann die Behauptung. □

Wir können nun das ganzzahlige Gauß-Verfahren benutzen, um die Matrizen, die die Faktorgruppen von $\mathbb{Z}^m$ beschreiben, in eine möglichst einfache Form zu bringen. Diese ist jedoch weniger einfach als das Ergebnis des Gauß-Verfahrens für Matrizen über Körpern, da hier auf Teilbarkeit geachtet werden muss. Wir zeigen zunächst, dass wir die Matrix in Blockdiagonalform bringen können und iterieren dann diesen Schritt, um eine Diagonalmatrix zu erhalten.

Lemma 1.7.20: Jede Matrix $A = (a_{ij}) \in M(m \times n, \mathbb{Z})$ mit $a_{11} > 0$ ist äquivalent zu einer Matrix $B = (b_{ij}) \in M(m \times n, \mathbb{Z})$ der Form

$$B = \begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{m2} & \dots & b_{mn} \end{pmatrix} \quad \text{mit} \quad b_{11} > 0. \tag{1.6}$$

Beweis:
Induktion über a_{11}. Gilt $a_{11} = 1$, so erreicht man durch Addieren von Vielfachen der ersten Zeile von A zu den anderen Zeilen, dass $a_{21} = ... = a_{m1} = 0$ gilt und durch Addieren von Vielfachen der ersten Spalte von A zu den anderen Spalten, dass $a_{12} = ... = a_{1n} = 0$ gilt.

Sei nun $A = (a_{ij}) \in M(m \times n, \mathbb{Z})$ mit $a_{11} > 0$ und die Behauptung bewiesen für alle Matrizen $A' = (a'_{ij})$ mit $0 < a'_{11} < a_{11}$. Wir unterscheiden nun drei Fälle:

Fall 1: Alle Einträge $a_{12}, \dots, a_{1n}, a_{21}, \dots, a_{m1}$ sind durch a_{11} teilbar.

Dann kann man durch Addieren von Vielfachen der ersten Zeile von A zu den anderen Zeilen erreichen, dass $a_{21} = ... = a_{m1} = 0$ und dann durch Addieren von Vielfachen der ersten Spalte von A zu den anderen Spalten, dass $a_{12} = ... = a_{1n} = 0$. Damit ist die Behauptung bewiesen.

Fall 2: Es gibt ein $i \in \{2, \dots m\}$ mit $a_{11} \nmid a_{i1}$. Dann teilen wir mit Rest:

$$a_{i1} = c\, a_{11} + r \text{ mit } c, r \in \mathbb{Z} \text{ und } 0 < r < a_{11}.$$

Nun ziehen wir das c-fache der ersten Zeile von A von der i-ten Zeile ab und vertauschen dann die beiden Zeilen. Dadurch erhalten wir eine zu A äquivalente Matrix A' mit $0 < a'_{11} = r < a_{11}$. Die Behauptung folgt nun aus der Induktionsvoraussetzung.

Fall 3: Es gibt ein $j \in \{2, \dots n\}$ mit $a_{11} \nmid a_{1j}$. In diesem Fall argumentieren wir wie im 2. Fall, aber mit Spalten- statt Zeilentransformationen. □

Lemma 1.7.21: Jede Matrix $A \in \mathrm{Mat}(m \times n, \mathbb{Z})$ ist äquivalent zu einer **positiven Diagonalmatrix**, also einer Matrix $D = (d_{ij})$ mit $d_{ij} = 0$ für $i \neq j$ und $d_{ii} \geq 0$ für alle $i = 1, ..., \min(m, n)$.

Beweis:
Induktion über $k := \min(m, n)$. Für $k = 0$ ist $m = 0$ oder $n = 0$, und es ist nichts zu zeigen. Sei die Aussage bewiesen für $\min(n, m) \leq t - 1$ und $A \in \mathrm{Mat}(m \times n, \mathbb{Z})$ mit $\min(n, m) = t$. Ist $A = 0$, so ist nichts mehr zu zeigen. Ansonsten können wir durch Vertauschen von Zeilen und Spalten erreichen, dass $a_{11} \neq 0$. Ist $a_{11} < 0$, so können wir durch Multiplizieren der ersten Zeile mit -1 erreichen, dass $a_{11} > 0$ gilt. Nach Lemma 1.7.20 ist A dann zu einer Matrix B der Form (1.6) äquivalent. Nun können wir die Induktionsvoraussetzung auf die Submatrix $B' = (b_{ij})_{i,j \geq 2}$ anwenden und erhalten die Behauptung. □

Mit diesen Ergebnissen erhalten wir eine Grobklassifikation der endlich erzeugten abelschen Gruppen. Indem wir die Matrix in der Präsentation einer endlich erzeugten abelschen Gruppe diagonalisieren, können wir zeigen, dass jede endlich erzeugte abelsche Gruppe ein Produkt zyklischer Gruppen ist.

Satz 1.7.22: Jede endlich erzeugte abelsche Gruppe G ist isomorph zu einem Produkt endlich vieler zyklischer Gruppen: es gibt $r, k \in \mathbb{N}_0$ und $n_1, \ldots, n_k \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}. \tag{1.7}$$

Ist $k = 0$, so nennt man G **frei** oder **freie abelsche Gruppe**.

Beweis:
Sei $G \cong \mathbb{Z}^m/A\mathbb{Z}^n$ mit $n \leq m$ eine Präsentation von G. Nach Lemma 1.7.21 ist A äquivalent zu einer positiven Diagonalmatrix $D = (d_{ij})$, und mit Korollar 1.7.19 folgt $G \cong \mathbb{Z}^m/D\mathbb{Z}^n$, also

$$G \cong \mathbb{Z}^m/D\mathbb{Z}^n \cong \mathbb{Z}^{m-n} \times \mathbb{Z}/d_{11}\mathbb{Z} \times \mathbb{Z}/d_{22}\mathbb{Z} \times \ldots \times \mathbb{Z}/d_{nn}\mathbb{Z}. \qquad \square$$

Die Zerlegung (1.7) ist offensichtlich nicht eindeutig. Einerseits können die einzelnen Faktoren im Produkt permutiert werden. Andererseits lassen sich ja bereits die zyklischen Gruppen mit Hilfe des chinesischen Restsatzes weiter aufspalten in zyklische Gruppen von Primpotenzordnung. Damit kann auch die Beschreibung der endlich erzeugten abelschen Gruppen in (1.7) nicht eindeutig sein. Zumindest besteht aber für die Zahl $r \in \mathbb{N}$ Hoffnung auf Eindeutigkeit. Um dies zu beweisen, benutzen wir die sogenannte Torsionsuntergruppe.

Lemma 1.7.23: Sei G eine abelsche Gruppe. Dann ist

$$\mathrm{tors}(G) := \{g \in G \mid o(g) < \infty\}$$

eine Untergruppe von G, die sogenannte **Torsionsuntergruppe**.

Beweis:
Offensichtlich gilt $o(0) = 1$ und damit $0 \in \mathrm{tors}(G)$ (UG2). Da aus $ng = 0$ mit $n \in \mathbb{N}$ auch $-ng = n(-g) = 0$ folgt, ist $-g \in \mathrm{tors}(G)$ für alle $g \in \mathrm{tors}(G)$ (UG3). Sind $g_1, g_2 \in \mathrm{tors}(G)$, so gibt es $n_1, n_1 \in \mathbb{N}$ mit $n_1 g_1 = n_2 g_2 = 0$. Also ist $n_1 n_2 (g_1 + g_2) = n_2(n_1 g_1) + n_1(n_2 g_2) = 0$ und damit $g_1 + g_2 \in \mathrm{tors}(G)$ (UG1). $\square$

Beispiel 1.7.24. Ist $G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ wie in (1.7), so ist

$$\mathrm{tors}(G) \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \qquad G/\mathrm{tors}(G) \cong \mathbb{Z}^r.$$

Denn aus $n(z_0, \bar{z}_1, ..., \bar{z}_k) = (nz_0, \overline{nz_1}, \ldots, \overline{nz_k}) = (0, ..., 0)$ für ein $n \in \mathbb{N}$ folgt $z_0 = 0$, und damit $\mathrm{tors}(G) \subseteq \{0\} \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$. Umgekehrt gibt es für $n = \mathrm{kgV}(n_1, ..., n_k)$ ganze Zahlen $r_k \in \mathbb{Z}$ mit $n = r_k n_k$, und es folgt $n(0, \bar{z}_1, ..., \bar{z}_k) = (0, r_1\overline{n_1 z_1}, ..., r_k\overline{n_k z_k}) = (0, \ldots, 0)$ für alle $(0, \bar{z}_1, ..., \bar{z}_k) \in \{0\} \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$. Also gilt $\{0\} \times \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} = \mathrm{tors}(G)$ und damit $G/\mathrm{tors}(G) \cong \mathbb{Z}^r$.

Indem wir den chinesischen Restsatz 1.7.6 auf die Faktoren $\mathbb{Z}/n_i\mathbb{Z}$ in (1.7) anwenden, können wir jede endlich erzeugte abelsche Gruppe als ein Produkt einer freien abelschen Gruppe $\mathbb{Z}^r$ und von zyklischen Gruppen von Primpotenzordnung schreiben wie in Korollar 1.7.7. Mit Hilfe der Torsionsuntergruppe können wir dann die Eindeutigkeit der Zahl r beweisen. Eine ähnliche, aber etwas kompliziertere Betrachtung ergibt die Eindeutigkeit der darin auftretenden Primpotenzen. Damit haben wir die endlich erzeugten abelschen Gruppen vollständig klassifiziert.

Satz 1.7.25: Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte $r, m \in \mathbb{N}_0$, Primzahlen $p_1, ..., p_m \in \mathbb{N}$ und $k_1, ..., k_m \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{k_1} \times \ldots \times \mathbb{Z}/p_m^{k_m} \tag{1.8}$$

Die Primpotenzen $p_i^{k_i}$ sind eindeutig bis auf die Reihenfolge. Die eindeutig bestimmte Zahl $r \in \mathbb{N}_0$ heißt **Rang** von G

Beweis:
1. Die Existenz einer solchen Zerlegung ergibt sich, indem man den chinesischen Restsatz 1.7.6 auf die Faktoren $\mathbb{Z}/n_i\mathbb{Z}$ in Satz 1.7.22 anwendet, wobei man die Zahl n_i als Produkt von teilerfremden Primpotenzen schreibt.

2. Wir zeigen die Eindeutigkeit von r. Nach Beispiel 1.7.24 gilt $G/\operatorname{tors}(G) = \mathbb{Z}^r$, und dies charakterisiert $\mathbb{Z}^r$ durch die Gruppe G. Um die Eindeutigkeit von r zu beweisen, reicht es, zu zeigen, dass aus $\mathbb{Z}^r \cong \mathbb{Z}^s$ mit $r, s \in \mathbb{N}_0$ auch $r = s$ folgt. Ist $\mathbb{Z}^r \cong \mathbb{Z}^s$, so gilt offensichtlich auch $2\mathbb{Z}^r \cong 2\mathbb{Z}^s$ und wegen $\mathbb{Z}^m/2\mathbb{Z}^m \cong (\mathbb{Z}/2\mathbb{Z})^m$ für alle $m \in \mathbb{N}_0$ ergibt sich

$$(\mathbb{Z}/2\mathbb{Z})^r \cong \mathbb{Z}^r/2\mathbb{Z}^r \cong \mathbb{Z}^s/2\mathbb{Z}^s \cong (\mathbb{Z}/2\mathbb{Z})^s.$$

Daraus folgt $2^r = |(\mathbb{Z}/2\mathbb{Z})^r| = |(\mathbb{Z}/2\mathbb{Z})^s| = 2^s$ und damit $r = s$.

3. Zu zeigen ist noch die Eindeutigkeit der Primzahlen p_i und Zahlen k_i. Dazu charakterisieren wir sie auf eine Weise, die nur noch von der abelschen Gruppe G abhängt. Wir betrachten für endlich erzeugte abelsche Gruppen G, $s \in \mathbb{N}_0$ und Primzahlen $p \in \mathbb{N}$ die Untergruppen

$$G_{p,s} = \{g \in G \mid p^s g = 0\}.$$

Ist $G = U \times V$ ein direktes Produkt, so folgt $p^s(u, v) = (p^s u, p^s v) = (0, 0)$ genau dann, wenn $p^s u = 0$ und $p^s v = 0$, und damit gilt $(U \times V)_{p,s} = U_{p,s} \times V_{p,s}$. Um $G_{p,s}$ für eine abelsche Gruppe der Form (1.8) zu bestimmen, müssen wir also nur noch die zyklischen Gruppen betrachten. Offensichtlich gilt $(\mathbb{Z}^r)_{p,s} = \{0\}$, und für eine zyklische Gruppe der Form $G = \mathbb{Z}/q^n\mathbb{Z}$ mit $n \in \mathbb{N}$ und $q \in \mathbb{N}$ prim, erhalten wir

$$G_{p,s} \cong \begin{cases} \{0\} & q \neq p \\ \mathbb{Z}/p^n\mathbb{Z} & q = p \text{ und } n \leq s \\ \mathbb{Z}/p^s\mathbb{Z} & q = p \text{ und } n \geq s. \end{cases} \tag{1.9}$$

Denn ist $p^s z = 0$ für ein $z \in G$, so ist $o(g)$ ein Teiler von p^s. Da $o(g)$ auch ein Teiler der Gruppenordnung ist, folgt $o(g) = 1$ oder $q = p$. Damit ergibt sich $G_{p,s} = \{0\}$ für $q \neq p$. Ist $p = q$ und $n \leq s$, so ist $p^s g = 0$ für alle $g \in G = \mathbb{Z}/p^n\mathbb{Z}$ und damit $G_{p,s} = G = \mathbb{Z}/p^n\mathbb{Z}$. Ist $p = q$ und $n \geq s$, so ist $p^s g = 0$ für ein $g \in G = \mathbb{Z}/p^n\mathbb{Z}$ genau dann, wenn $\bar{p}^n$ ein Teiler von $\bar{p}^s g$ ist, also genau dann, wenn $\bar{p}^{n-s}$ ein Teiler von g ist. Da die Vielfachen von $\bar{p}^{n-s}$ in $\mathbb{Z}/p^n\mathbb{Z}$ eine Untergruppe bilden, die isomorph zu $\mathbb{Z}/p^s\mathbb{Z}$ ist folgt (1.9). Damit gilt insbesondere $|(\mathbb{Z}/q^n\mathbb{Z})_{p,s}| = \operatorname{ggT}(q^n, p^s)$.

4. Kombinieren wir diese Ergebnisse, so finden wir für eine abelsche Gruppe der Form (1.8)

$$\begin{aligned} |G_{p,s}| &= |(\mathbb{Z}^r)_{p,s} \times (\mathbb{Z}/p_1^{k_1})_{p,s} \times \ldots \times (\mathbb{Z}/p_m^{k_m})_{p,s}| = |(\mathbb{Z}/p_1^{k_1})_{p,s}| \cdots |(\mathbb{Z}/p_m^{k_m})_{p,s}| \\ &= \operatorname{ggT}(p_1^{k_1}, p^s) \cdots \operatorname{ggT}(p_m^{k_m}, p^s) \end{aligned}$$

für alle $s \in \mathbb{N}_0$ und Primzahlen $p \in \mathbb{N}$. Die linke Seite der Gleichung hängt nur von G, p und s ab, die rechte enthält p^s und die Primpotenzen $p_i^{k_i}$. Indem wir p und s variieren, ergibt sich, dass alle Primpotenzen $p_i^{k_i}$ in (1.8) eindeutig bis auf die Reihenfolge sind. □

Korollar 1.7.26: Sei p eine Primzahl und $n \in \mathbb{N}_0$. Dann stehen die abelschen Gruppen der Ordnung p^n in Bijektion mit den Partitionen von n. Die Gruppe $\mathbb{Z}/p^{\lambda_1} \times \ldots \times \mathbb{Z}/p^{\lambda_m}$ entspricht dabei der Partition $(\lambda_1, ..., \lambda_m)$.

Beweis:
Ist G eine abelsche Gruppe der Ordnung p^n, so ist nach dem Satz von Lagrange die Ordnung jeder Untergruppe ein Teiler von p^n und damit von der Ordnung p^k mit $0 \leq k \leq n$. Nach Satz 1.7.25 ist G damit von der Form $G \cong \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\lambda_m}\mathbb{Z}$ mit $1 \leq \lambda_i \leq n$. Da daraus $|G| = p^{\lambda_1} \cdots p^{\lambda_m} = p^{\lambda_1 + ... + \lambda_m} = p^n$ folgt, muss $\lambda_1 + ... + \lambda_m = n$ gelten. Fordern wir $\lambda_1 \geq \ldots \geq \lambda_m$, so wird die Beschreibung eindeutig und $(\lambda_1, ..., \lambda_m)$ ist eine Partition von n. □

Beispiel 1.7.27. Wir untersuchen die abelschen Gruppen von Zweierpotenz-Ordnung:

- Bis auf Isomorphie gibt es zwei Gruppen der Ordnung $2^2 = 4$ und beide sind abelsch, nämlich $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sie entsprechen den Partitionen 2 und $2 = 1+1$. Die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ heißt **Kleinsche Vierergruppe**. Sie ist die kleinste nicht-zyklische Gruppe.
- Bis auf Isomorphie sind die abelschen Gruppen der Ordnung $8 = 2^3$ die Gruppen $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sie entsprechen den Partitionen 3, $3 = 2 + 1$, $3 = 1 + 1 + 1$.
- Für die Gruppenordnung $16 = 2^4$ erhält man die abelschen Gruppen $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sie entsprechen den Partitionen 4, $4 = 3 + 1$, $4 = 2 + 2$, $4 = 2 + 1 + 1$, $4 = 1 + 1 + 1 + 1$.

Korollar 1.7.28: Sei G eine endliche abelsche Gruppe und p eine Primzahl, die die Ordnung von G teilt. Dann enthält G ein Element der Ordnung p.

Beweis:
Ist G von der Form (1.8) $G \cong \mathbb{Z}/p_1^{k_1} \times \ldots \times \mathbb{Z}/p_m^{k_m}$, so gilt $|G| = p_1^{n_1} \cdots p_m^{n_m}$. Es gilt also $p = p_i$ für mindestens eine der Primzahlen p_i. Das Element $g = \bar{p}_i^{n_i - 1}$ in $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$ hat dann die Ordnung p. □

1.8 Auflösbare Gruppen

Im letzten Abschnitt wurden die endlich erzeugten abelschen Gruppen klassifiziert, indem wir sie als direkte Produkte freier abelscher Gruppen und zyklischer Gruppen von Primpotenz-Ordnung zerlegt haben. In diesem Abschnitt untersuchen wir die Zerlegung allgemeinerer endlicher Gruppen, einerseits in *abelsche* Gruppen, andererseits in *einfache* Gruppen, also Gruppen ohne nichttriviale echte Normalteiler. Wir werden dabei kein Klassifikationsresultat erhalten - diese Frage ist zu schwierig - aber ein besseres Verständnis der Struktur endlicher Gruppen.

Zunächst sollte dabei geklärt werden, was man unter einer Zerlegung versteht. Anders als bei der Klassifikation abelscher Gruppen können wir nicht davon ausgehen, dass jede Gruppe eine Zerlegung als direktes Produkt abelscher oder einfacher Gruppen besitzt. Nichtabelsche Gruppen lassen sich offensichtlich nie als direkte Produkte, sondern höchstens als *semidirekte Produkte* abelscher Gruppen schreiben, wie beispielsweise die Diedergruppe in Beispiel 1.4.5. Außerdem muß auch eine Beschreibung als semidirektes Produkt abelscher Gruppen nicht existieren. Nach

Satz 1.4.6 und Beispiel 1.4.7 garantiert die Existenz eines Normalteilers $N \subseteq G$ nämlich *nicht*, dass sich die Gruppe G als semidirektes Produkt $G = N \rtimes G/N$ schreiben lässt.

Daher ist es vielversprechender, statt semidirekten Produkten Zerlegungen als multiple Quotienten zu betrachten. Dazu sucht man einen echten Normalteiler N in G, dann einen echten Normalteiler N' in N, einen echten Normalteiler N'' in $N', \ldots$ und fordert, dass die Faktorgruppen G/N, N/N', $N'/N'', \ldots$ abelsch oder einfach sind. Wir konzentrieren uns dabei auf Zerlegungen mit abelschen Faktorgruppen, die nur für die sogenannten *auflösbare Gruppen* existieren. Die Zerlegung in einfache Faktorgruppen ist aufgrund der komplizierteren Struktur der einfachen Gruppen deutlich schwieriger, aber wichtig, da sie für *jede* endliche Gruppe existiert und die einfachen endlichen Gruppen seit 2002 vollständig klassifiziert sind.

Definition 1.8.1: Sei G eine Gruppe.

1. Eine **Subnormalreihe** von G ist eine endliche aufsteigende Folge von Untergruppen

   $$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_{n-1} \subseteq G_n = G \qquad \text{mit } G_{i-1} \text{ normal in } G_i \text{ für } i = 1, ..., n.$$

   Die Faktorgruppen G_i/G_{i-1} heißen **Faktoren** der Subnormalreihe.

2. Eine Subnormalreihe, in der alle Faktoren einfach sind, heißt **Kompositionsreihe** und die Faktoren darin heißen **Kompositionsfaktoren**.

3. Die Gruppe G heißt **auflösbar**, wenn sie eine Subnormalreihe besitzt, in der alle Faktoren abelsch sind.

Die Bezeichnung *Subnormalreihe* bezieht sich darauf, dass nur Normalität von G_{i-1} in G_i und nicht Normalität von G_{i-1} in ganzen Gruppe G gefordert wird. Die Bezeichnung *auflösbar* bezieht sich auf gewisse Gleichungen, die sich für auflösbare Gruppen auflösen lassen. Es lässt sich zeigen, dass jede endliche Gruppe eine Kompositionsreihe, also eine Subnormalreihe mit *einfachen* Faktoren besitzt. Eine Subnormalreihe mit abelschen Faktoren muss dagegen nicht unbedingt existieren.

Satz 1.8.2: Jede endliche Gruppe G besitzt eine Kompositionreihe.

Beweis:
Induktion über $|G|$. Der Fall $|G| = 1$ ist trivial. Sei nun G eine Gruppe der Ordnung $|G| = k \geq 2$. Dann besitzt G einen echten Normalteiler, beispielsweise die triviale Untergruppe $\{e\} \subseteq G$. Da G endlich ist können wir einen maximalen echten Normalteiler wählen, also einen Normalteiler $N \subsetneq G$, so dass aus $N' \subsetneq G$ normal in G mit $N \subseteq N'$ folgt $N = N'$. Nach der Untergruppenkorrespondenz 1.3.19 für die kanonische Surjektion $\pi_N : G \to G/N$ entsprechen die Normalteiler von G/N dann den Normalteilern von G mit $N \subseteq G$. Wegen der Maximalität von N hat damit G/N keine nichttrivialen echten Normalteiler, ist also einfach. Da $|N| < |G|$ liefert die Induktionsvoraussetzung eine Subnormalreihe $\{e\} = N_0 \subseteq N_1 ... \subseteq N_n = N$ von N mit einfachen Faktoren. Damit ist $\{e\} \subseteq N_1 \subseteq ... \subseteq N_n = N \subseteq G$ eine Subnormalreihe von G mit einfachen Faktoren. □

Der **Satz von Jordan-Hölder**, der in dieser Vorlesung nicht bewiesen wird, besagt, dass die Kompositionsfaktoren in einer Kompositionsreihe einer Gruppe G eindeutig bis auf die Reihenfolge sind. Offensichtlich gilt dies nicht für die Faktoren von Subnormalreihen (Warum?).

Ist eine endliche Gruppe G auflösbar, so besitzt G eine Subnormalreihe, in der jeder Faktor eine endliche abelsche Gruppe ist. Mit Hilfe des chinesischen Restsatzes 1.7.6 können wir dann jeden Faktor in zyklische Gruppen von Primpotenzordnung aufspalten und jede Gruppe $\mathbb{Z}/p^n\mathbb{Z}$ mit p prim und $n \in \mathbb{N}$ besitzt dann eine Subnormalreihe der Form $\{e\} \subseteq \mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{Z}/p^2\mathbb{Z} \subseteq \ldots \subseteq \mathbb{Z}/p^{n-1}\mathbb{Z} \subseteq \mathbb{Z}/p^n\mathbb{Z}$. Damit können wir eine Subnormalreihe von G konstruieren, in der jeder Faktor eine zyklische Gruppe von Primzahlordnung ist, also eine einfache abelsche Gruppe. Besitzt umgekehrt eine Gruppe G eine Subnormalreihe, in der jeder Faktor eine zyklische Gruppe von Primzahlordnung ist, so ist G offensichtlich auflösbar. Damit erhalten wir

Korollar 1.8.3: Eine endliche Gruppe ist auflösbar genau dann, wenn sie eine Subnormalreihe hat, in der jeder Faktor eine zyklische Gruppe von Primzahlordnung ist.

Beispiel 1.8.4.

1. Die triviale Gruppe $G = \{e\}$ ist auflösbar mit der Subnormalreihe $\{e\} = G_0 = G$. Die Subnormalreihe hat null Faktoren.

2. Jede abelsche Gruppe G ist auflösbar mit der Subnormalreihe $\{e\} = G_0 \subseteq G_1 = G$.

3. Die Diedergruppe D_n ist nach Beispiel 1.4.5 das semidirekte Produkt $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, wobei $\mathbb{Z}/n\mathbb{Z} = \langle r \rangle$ die Untergruppe der Rotationen bezeichnet und $\mathbb{Z}/2\mathbb{Z} = \langle s \rangle$ von der Spiegelung an der x-Achse erzeugt wird. Sie ist auflösbar mit Normalreihe

$$\{e\} \subseteq \mathbb{Z}/n\mathbb{Z} \subseteq D_n.$$

4. Die symmetrischen Gruppen $G = S_n$ sind für $n = 0, 1, 2, 3, 4$ auflösbar. Für $n = 0, 1, 2$ sind sie abelsch und damit auflösbar nach 2. Für $n = 3$ ist $A_3 \cong \mathbb{Z}/3\mathbb{Z} \subseteq S_3$ ein Normalteiler und $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$. Man erhält die Subnormalreihe

$$\{e\} \subseteq A_3 \subseteq S_3.$$

   Für $n = 4$ sind nach Beispiel 1.6.15 und 1.6.16 $A_4 \subseteq S_4$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq A_4$ Normalteiler mit $[S_4 : A_4] = 2$ und $[A_4 : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}] = 3$. Daraus folgt $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ und $A_4/(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$, und man erhält die Subnormalreihe

$$\{e\} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq A_4 \subseteq S_4.$$

   Diese lässt sich noch verfeinern, indem man einen der Faktoren in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ auswählt. So erhält man die Subnormalreihe

$$\{e\} \subseteq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq A_4$$

   mit einfachen abelschen Faktoren $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$.

5. Für $n \geq 5$ ist die alternierende Gruppe A_5 *nicht* auflösbar. Denn sie ist nach Satz 1.6.18 einfach und hat damit nur eine einzige Subnormalreihe mit nicht-trivialen Faktoren, nämlich $\{e\} \subseteq A_5$. Aber A_5 ist nicht abelsch.

6. Mit dem gleichen Argument wie in 5. folgt, dass eine einfache Gruppe genau dann auflösbar ist, wenn sie abelsch ist, also eine zyklische Gruppe von Primzahlordnung.

Um sinnvoll mit dem Begriff der Auflösbarkeit arbeiten zu können, muss man untersuchen, wie er sich mit den grundlegenden Konstruktionen für Gruppen verträgt. Insbesondere stellt sich die Frage, ob Untergruppen und Faktorgruppen auflösbarer Gruppen wieder auflösbar sind. Dazu muss man aus einer Subnormalreihe $\{e\} \subseteq G_1 \subseteq ... \subseteq G$ einer Gruppe G eine Subnormalreihe einer Untergruppe $H \subseteq G$ oder einer Faktorgruppe G/N bezüglich eines Normalteilers $N \subseteq G$ konstruieren. Im ersten Fall bietet es sich an, die Schnitte $H_i = H \cap G_i$ zu betrachten.

Satz 1.8.5: Untergruppen auflösbarer Gruppen sind auflösbar.

Beweis:
Sei G eine auflösbare Gruppe und $H \subseteq G$ eine Untergruppe. Sei $\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$ eine Subnormalreihe von G mit abelschen Faktoren und $\pi_i : G_i \to G_i/G_{i-1}$ die zugehörigen kanonischen Surjektionen. Wir setzen $H_i := H \cap G_i$ und bezeichnen mit $\iota_i : H_i \to G_i$, $h \mapsto h$ die Inklusionsabbildungen. Dann sind die Abbildungen $\pi_i \circ \iota_i : H_i \to G_i/G_{i-1}$ Gruppenhomomorphismen mit $\ker(\pi_i \circ \iota_i) = H_i \cap G_{i-1} = H \cap G_i \cap G_{i-1} = H \cap G_{i-1} = H_{i-1}$. Damit ist H_{i-1} ein Normalteiler von H_i für $i = 1, ..., n$ und $\{e\} = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = H$ eine Subnormalreihe von H. Die Abbildungen $\iota_i' : H_i/H_{i-1} \to G_i/G_{i-1}$, $hH_{i-1} \to hG_{i-1}$ sind injektive Gruppenhomomorphismen, denn aus $hG_{i-1} = h'G_{i-1}$ mit $h, h' \in H_i$ folgt $h^{-1}h' \in H_i \cap G_{i-1} = H_{i-1}$ und damit $hH_{i-1} = h'H_{i-1}$. Damit ist der Faktor H_i/H_{i-1} isomorph zu einer Untergruppe einer abelschen Gruppe G_i/G_{i-1} und damit selbst abelsch. □

Korollar 1.8.6: Die symmetrische Gruppe S_n und die alternierende Gruppe A_n sind genau dann auflösbar, wenn $n \leq 4$ ist.

Beweis:
In Beispiel 1.8.4, 4. wurde bereits gezeigt, dass S_n für $n \leq 4$ auflösbar ist und damit nach Satz 1.8.5 auch A_n. In Beispiel 1.8.4, 5. wurde gezeigt, dass A_n für $n \geq 5$ nicht auflösbar ist und damit nach Satz 1.8.5 auch nicht S_n. □

Im Fall von Faktorgruppen G/N einer Gruppe G bezüglich eines Normalteilers $N \subseteq G$ lässt sich etwas mehr aussagen. In diesem Fall kann man für jede Subnormalreihe $\{e\} \subseteq G_1 \subseteq ... \subseteq G$ die Bilder $\pi_N(G_i)$ unter der kanonischen Surjektion $\pi_N : G \to G/N$, $g \mapsto gN$ betrachten. Umgekehrt kann man aus einer Subnormalreihe von N und einer Subnormalreihe von G/N mit Hilfe der Untergruppenkorrespondenz auch eine Subnormalreihe von G konstruieren.

Satz 1.8.7: Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler. Dann sind äquivalent:

(i) G ist auflösbar.

(ii) N und G/N sind auflösbar.

Beweis:
(i)⇒ (ii): Sei G auflösbar und $\{e\} = G_0 \subseteq ... \subseteq G_n = G$ eine Subnormalreihe mit abelschen Faktoren. Dann ist nach Satz 1.8.5 auch $N \subseteq G$ auflösbar. Zu zeigen ist noch, dass G/N auflösbar ist. Sei dazu $\pi_N : G \to G/N$, $g \mapsto gN$ die kanonische Surjektion und $F_i := \pi_N(G_i) \subseteq G/N$. Da G_{i-1} normal in G_i ist und $\pi_N|_{G_i} : G_i \to \pi_N(G_i)$ ein surjektiver Gruppenhomomorphismus, ist $F_{i-1} = \pi_N(G_{i-1}) \subseteq \pi_N(G_i) = F_i$ ein Normalteiler in F_i nach Lemma 1.3.18. Also ist $\{e\} = F_0 \subseteq ... \subseteq F_n = G/N$ eine Subnormalreihe von G/N. Der Gruppenhomomorphismus

$\pi_i = \pi_{F_{i-1}} \circ \pi_N : G \to F_i \to F_i/F_{i-1}$ ist surjektiv mit $G_{i-1} \subseteq \ker(\pi_i)$ Der Homomorphiesatz liefert daher einen surjektiven Homomorphismus $\pi_i' : G_i/G_{i-1} \to F_i/F_{i-1}$. Also sind die Faktoren F_i/F_{i-1} als Bilder von abelschen Gruppen abelsch und G/N auflösbar.

(ii)⇒ (i): Seien N und G/N auflösbar, $\{e\} = N_0 \subseteq ... \subseteq N_m = N$, $\{e\} = F_0 \subseteq ... \subseteq F_n = G/N$ Subnormalreihen von N und G/N mit abelschen Faktoren. Nach der Untergruppenkorrespondenz 1.3.19 für die kanonische Surjektion $\pi_N : G \to G/N$ sind die Untergruppen F_i von der Form $F_i = \pi_N(K_i) = K_i/N$ mit $N \subseteq K_i = \pi_N^{-1}(F_i) \subseteq G$ und K_{i-1} normal in K_i. Damit ist

$$\{e\} = N_0 \subseteq N_1 \subseteq \ldots \subseteq N_{m-1} \subseteq N_m = N = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{n-1} \subseteq K_n = G$$

eine Subnormalreihe von G. Die Faktoren sind gegeben durch N_i/N_{i-1} und durch K_i/K_{i-1}, und nach dem ersten Isomorphiesatz 1.3.26 gilt $K_i/K_{i-1} \cong F_i/F_{i-1}$. Also sind alle Faktoren abelsch, und G ist auflösbar. □

Korollar 1.8.8: Sei p eine Primzahl. Dann ist jede p-Gruppe G auflösbar.

Beweis:
Induktion nach der Gruppenordnung. Für $|G| = 1$ ist G trivial und damit auflösbar. Sei G eine p-Gruppe mit $|G| = p^n = k$. Nach Korollar 1.5.13 ist dann das Zentrum $\mathrm{Z}(G)$ nicht trivial. Also ist $G/\mathrm{Z}(G)$ eine Gruppe der Ordnung $[G : Z(G)] = |G|/|Z(G)| < |G|$, und $G/Z(G)$ ist ebenfalls eine p-Gruppe. Nach Induktionsvoraussetzung ist $G/Z(G)$ auflösbar, und $\mathrm{Z}(G)$ ist als abelsche Gruppe auflösbar nach Beispiel 1.8.4. Also ist nach Satz 1.8.7 auch G auflösbar. □

1.9 Die Sylowschen Sätze

In diesem Abschnitt behandeln wir zwei wichtige Sätze, die sogenannten *Sylowschen Sätze*, die einerseits weitere Informationen zur Auflösbarkeit von Gruppen liefern, andererseits allgemein dabei helfen, die Struktur endlicher Gruppen besser zu verstehen. Die zentrale Idee ist es dabei, eine endliche Gruppe ausgehend von ihren Untergruppen zu untersuchen, deren Ordnung eine maximale Primpotenz ist.

In Definition 1.5.12 wurde eine p-Gruppe als eine Gruppe eingeführt, deren Ordnung eine Potenz einer Primzahl $p \in \mathbb{N}$ ist. Ebenso definiert man eine **p-Untergruppe** einer gegebenen Gruppe G als eine Untergruppe $U \subseteq G$, die eine p-Gruppe ist. Da nach dem Satz von Lagrange die Ordnung jeder Untergruppe ein Teiler der Gruppenordnung ist, kommt als Ordnung einer p-Untergruppe maximal die größte Potenz von p in Frage, die die Ordnung von G teilt. Eine p-Untergruppe dieser Ordnung bezeichnet man als p-Sylowgruppe.

Definition 1.9.1: Sei G eine endliche Gruppe, p eine Primzahl und $n \in \mathbb{N}_0$ die größte Zahl, so dass p^n die Ordnung von G teilt: $|G| = p^n m$ mit $p \nmid m$. Eine Untergruppe $H \subseteq G$ mit $|H| = p^n$ heißt **p-Sylowuntergruppe** oder **p-Sylowgruppe** von G.

Man beachte, dass in Definition 1.9.1 auch $n = 0$ zugelassen ist. Dies bedeutet, dass p kein Teiler von $|G|$ ist. In diesem Fall ist die triviale Untergruppe $\{e\} \subseteq G$ die einzige p-Sylowgruppe.

Wir untersuchen nun, wie sich p-Sylowgruppen $P \subseteq G$ unter der Konjugation mit Elementen aus G verhalten. Nach Beispiel 1.5.3, 8. definiert die Konjugation mit Elementen aus G eine Operation $\triangleright : G \times U_G \to U_G$, $U \mapsto gUg^{-1}$ von G auf der Menge U_G ihrer Untergruppen. Wie für jede Operation ist *in der gleichen Bahn liegen* nach Satz 1.5.4 eine Äquivalenzrelation. Hier liegen zwei Untergruppen U_1, U_2 genau dann in der gleichen Bahn von $\triangleright$, wenn sie zueinander konjugiert sind. Da die Abbildungen $C_g : G \to G$, $h \mapsto ghg^{-1}$ Bijektionen sind, haben zueinander konjugierte Untergruppen die gleiche Gruppenordnung. Zu p-Sylowgruppen oder zu p-Untergruppen konjugierte Untergruppen sind also auch wieder p-Sylowgruppen oder p-Untergruppen. Die Frage ist nun, ob umgekehrt alle p-Sylowgruppen zueinander konjugiert sind. Ebenso fragt man sich, ob die p-Sylowgruppen die p-Gruppen niedrigerer Ordnung als Untergruppen enthalten. Die Antwort auf diese Fragen gibt der zweite Satz von Sylow.

Satz 1.9.2 (2. Satz von Sylow):
Sei G eine endliche Gruppe, p eine Primzahl, und G besitze eine p-Sylowgruppe.

1. Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.
2. Je zwei p-Sylowgruppen sind zueinander konjugiert.

Beweis:
1. Sei $H \subseteq G$ eine p-Untergruppe und $P \subseteq G$ eine p-Sylowgruppe. Dann operiert H durch $\triangleright : H \times G/P \to G/P$, $(h, gP) \mapsto (hg)P$ auf der Menge G/P der Linksnebenklassen. Da P eine p-Sylowgruppe ist und nach dem Satz von Lagrange $|G| = |P| \cdot [G : P]$ gilt, ist $|G/P| = [G : P]$ nicht durch p teilbar. Aus Korollar 1.5.15 folgt, dass die Operation einen Fixpunkt hat, also ein $g \in G$ existiert mit $(hg)P = gP$ für alle $h \in H$. Dies ist äquivalent zu $g^{-1}hg \in P$ für alle $h \in H$ und damit zu $H \subseteq gPg^{-1}$. Da $C_g : P \to gPg^{-1}$ eine Bijektion ist, gilt $|gPg^{-1}| = |P|$, und damit ist auch $gPg^{-1} \subseteq G$ eine p-Sylowgruppe.

2. Wählt man im Beweis von 1. für H eine p-Sylowgruppe $H = P'$, so folgt aus $P' \subseteq gPg^{-1}$ und $|P'| = |P|$ dann $P' = gPg^{-1}$, und damit sind P und P' zueinander konjugiert. □

Korollar 1.9.3: Sei G eine endliche Gruppe, p eine Primzahl und $P \subseteq G$ eine p-Sylowgruppe. Dann ist P ein Normalteiler in G genau dann, wenn P die einzige p-Sylowgruppe von G ist.

Beweis:
Da $|gPg^{-1}| = |P|$ für alle $g \in G$ ist gPg^{-1} eine p-Sylowgruppe für alle p-Sylowgruppen P. Ist P die einzige p-Sylowgruppe, so folgt offensichtlich $gPg^{-1} = P$ für alle $g \in G$, und damit ist P ein Normalteiler in G. Ist umgekehrt P eine p-Sylowgruppe, die normal in G ist, so ist nach dem zweiten Satz von Sylow jede andere p-Sylowgruppe P' zu P konjugiert und damit $P' = P$. □

Der zweite Satz von Sylow klärt die Eindeutigkeit von p-Sylowgruppen und die Frage, wie sich p-Sylowgruppen zu allgemeineren p-Untergruppen verhalten. Insbesondere erlaubt er es uns, die Operation $\triangleright : G \times U_G \to U_G$, $U \mapsto gUg^{-1}$ einer Gruppe G auf der Menge U_G ihrer Untergruppen auf die Menge Syl_p ihrer p-Sylowgruppen einzuschränken. Diese liegen nach dem 2. Satz von Sylow alle in der gleichen Bahn, und damit erhalten wir nach Beispiel 1.5.3, 8. eine *transitive* Operation $\triangleright : G \times \mathrm{Syl}_p \to \mathrm{Syl}_p$, $P \mapsto gPg^{-1}$. Die Existenz von p-Sylowgruppen ist dadurch allerdings nicht gesichert, und auch die Frage, wie viele zueinander konjugierte Sylowgruppen existieren, bleibt offen. Diese Fragen beantwortet der erste Satz von Sylow.

Satz 1.9.4 (1. Satz von Sylow): Sei G eine endliche Gruppe und $p \in \mathbb{N}$ prim. Dann gilt:

1. Die Gruppe G besitzt eine p-Sylowuntergruppe.
2. Ist $|G| = p^n \cdot m$ mit $p \nmid m$, so gilt für die Anzahl s_p der p-Sylowuntergruppen von G

$$s_p \text{ teilt } m \qquad \text{und} \qquad s_p \equiv 1 \bmod p.$$

Beweis:
1. Induktion über $|G|$. Für $|G| = 1$ ist die Aussage trivial. Sei daher $|G| > 1$ und $|G| = p^n \cdot m$ mit $n \in \mathbb{N}_0$ und $p \nmid m$. Wir unterscheiden zwei Fälle.

1. Fall: Gibt es eine echte Untergruppe $H \subsetneq G$ mit $p^n \mid |H|$, so hat H eine p-Sylowuntergruppe nach Induktionsvoraussetzung. Diese ist dann auch eine p-Sylowuntergruppe von G.

2. Fall: Für jede echte Untergruppe $H \subsetneq G$ gilt $p^n \nmid |H|$. Aus dem Satz von Lagrange folgt dann $|G| = p^n \cdot m = |H| \cdot [G : H]$ und damit $p \mid [G : H]$ für jede echte Untergruppe $H \subsetneq G$. Insbesondere gilt $p \mid [G : Z_g]$ für die Zentralisatoren Z_g jedes Elements $g \in G \setminus Z(G)$. Nach der Klassengleichung (1.3) gilt für jedes Repräsentantensystem R der Konjugationsklassen

$$|\mathrm{Z}(G)| = |G| - \sum_{g \in R \setminus Z(G)} [G : Z_g].$$

Da p die Gruppenordnung $|G|$ und $[G : Z_g]$ für alle $g \in G \setminus Z(G)$ teilt, teilt p auch $|Z(G)|$. Da $Z(G)$ endlich und abelsch ist, gibt es nach Korollar 1.7.28 ein Element $z \in \mathrm{Z}(G)$ der Ordnung p.

Die von z erzeugte Untergruppe $\langle z \rangle \subseteq G$ hat dann p Elemente und ist als Untergruppe von $Z(G)$ nach Beispiel 1.3.12 ein Normalteiler von G. Die Faktorgruppe $G/\langle z \rangle$ hat die Ordnung $|G/\langle z \rangle| = p^{n-1} \cdot m$ und besitzt nach Induktionsvoraussetzung eine p-Sylowgruppe, also eine Untergruppe $S \subseteq G/\langle z \rangle$ mit $|S| = p^{n-1}$. Da $\pi : G \to G/\langle z \rangle$ ein Homomorphismus ist, ist $P = \pi^{-1}(S)$ eine Untergruppe von G nach Lemma 1.2.8, und nach dem Satz von Lagrange gilt $|P| = |\langle z \rangle| \cdot |S| = p \cdot p^{n-1} = p^n$. Damit ist P eine p-Sylowgruppe in G.

2. Sei Syl_p die Menge der p-Sylowuntergruppen von G. Nach dem 2. Satz von Sylow operiert G transitiv auf Syl_p durch Konjugation $\triangleright : G \times \mathrm{Syl}_p \to \mathrm{Syl}_p$, $(g, P) \mapsto gPg^{-1}$. Der Stabilisator einer p-Sylowgruppe P ist ihr Normalisator $G_P = N(P) = \{g \in G \mid gPg^{-1} = P\}$ mit $P \subseteq N(P)$. Da die Bahn von $\triangleright$ genau $s_p = [G : N(P)]$ Elemente enthält, folgt mit dem Satz von Lagrange

$$s_p = [G : N(P)] = \frac{|G|}{|N(P)|} = \frac{|G|/|P|}{|N(P)|/|P|} = \frac{[G : P]}{[N(P) : P]} = \frac{m}{[N(P) : P]},$$

und damit ist s_p ein Teiler von m. Wir betrachten nun für jede p-Sylowgruppe P die Operation $\triangleright_P : P \times \mathrm{Syl}_p \to \mathrm{Syl}_p$, $(p, Q) \mapsto pQp^{-1}$. Offensichtlich ist $P \in \mathrm{Syl}_p$ ein Fixpunkt von $\triangleright_P$. Ist $P' \in \mathrm{Syl}_p$ ein weiterer Fixpunkt von $\triangleright_P$, so ist $P \subseteq N(P')$ und P und P' sind zwei p-Sylowgruppen der Gruppe $N(P')$. Also gibt es nach dem 2. Satz von Sylow ein $n \in N(P')$ mit $P = nP'n^{-1} = P'$. Damit ist P der einzige Fixpunkt von $\triangleright_P$. Aus Korollar 1.5.15 folgt dann $1 \equiv |\mathrm{Syl}_p| \bmod p \equiv s_p \bmod p$. □

Bemerkung 1.9.5. In manchen Lehrbüchern wird der 1. Satz von Sylow in zwei Sätze aufgespalten. Dort wird dann die Existenz von p-Sylowuntergruppen als der 1. Satz von Sylow bezeichnet, und die Aussagen über die Anzahlen der p-Sylowgruppen als der 3. Satz von Sylow.

Die Sätze von Sylow besitzen viele nützliche Anwendungen. Insbesondere erlauben sie es einem, Aussagen über die Existenz von Gruppenelementen bestimmter Ordnungen zu machen. Mit Korollar 1.9.3 lässt sich oft die Existenz von Normalteilern beweisen, und man kann folgern, dass gegebene Gruppen direkte oder semidirekte Produkte sind. Ebenso kann man mit den Sylowschen Sätzen oft die Auflösbarkeit bestimmter Gruppen beweisen.

Korollar 1.9.6 (**Satz von Cauchy**)**:** Ist G eine endliche Gruppe und p ein Primteiler der Gruppenordnung $|G|$, so besitzt G ein Element der Ordnung p.

Beweis:
Sei $P \subseteq G$ eine p-Sylowuntergruppe. Dann ist P eine nichttriviale p-Gruppe und hat damit nach Korollar 1.5.13 ein nichttriviales Zentrum $\mathrm{Z}(P)$. Dieses ist eine abelsche Grupe mit $p \mid |Z(P)|$ und hat damit nach Korollar 1.7.28 ein Element der Ordnung p. □

Korollar 1.9.7: Seien p und q Primzahlen. Dann ist jede Gruppe der Ordnung pq auflösbar.

Beweis:
Ist $p = q$, so ist G eine p-Gruppe und damit auflösbar nach Korollar 1.8.8. Ansonsten können wir o. B. d. A. $p > q$ annehmen. Sei s_p die Anzahl der p-Sylowuntergruppen von G. Dann ist nach dem 1. Satz von Sylow s_p ein Teiler von $|G|/p = q$ und damit $s_p = 1$ oder $s_p = q$. Andererseits gilt nach dem 1. Satz von Sylow $s_p \equiv 1 \bmod p$, und aus $q < p$ folgt dann $s_p = 1$. Daher gibt es nur eine p-Sylowuntergruppe P und diese ist nach Korollar 1.9.3 normal in G. Wegen $|P| = p$ und $|G/P| = q$ sind sowohl P als auch G/P primzyklisch und damit nach Korollar 1.8.8 auflösbar. Nach Satz 1.8.7 ist dann auch G auflösbar. □

Korollar 1.9.8: Sind $p, q \in \mathbb{N}$ verschiedene Primzahlen, so ist jede Gruppe der Ordnung pq ein semidirektes Produkt zyklischer Gruppen der Ordnung p und q.

Beweis:
Sei G eine Gruppe der Ordnung $|G| = pq$. Dann besitzt G nach dem 1. Satz von Sylow eine p-Sylowgruppe $P \cong \mathbb{Z}/p\mathbb{Z}$ und eine q-Sylowgruppe $Q \cong \mathbb{Z}/q\mathbb{Z}$. Wie im Beweis von Korollar 1.9.7 können wir ohne Beschränkung der Allgemeinheit annehmen, dass $p > q$ gilt, und wie im Beweis von Korollar 1.9.7 folgt, dass $P \subseteq G$ normal in G ist.

Da $P \cap Q$ eine Untergruppe von P und von Q ist, muss nach dem Satz von Lagrange $|P \cap Q|$ ein Teiler von p und von q sein. Daraus folgt $|P \cap Q| = 1$ und $P \cap Q = \{e\}$. Damit ist $|PQ| = |\{gh \mid g \in P, h \in Q\}| = |P| \cdot |Q| = pq$, denn aus $g, g' \in P$ und $h, h' \in Q$ mit $gh = g'h'$ folgt $g^{-1}g' = hh'^{-1} \in P \cap Q = \{e\}$, also $g = g'$ und $h = h'$. Damit ist $Q \subseteq G$ eine Untergruppe mit $PQ = G$ und $P \cap Q = \{e\}$, und mit Satz 1.4.4 folgt $G \cong P \rtimes Q$. □

Beispiel 1.9.9. Jede Gruppe G der Ordnung $|G| = 30 = 2 \cdot 3 \cdot 5$ ist auflösbar.

G hat für $p = 2, 3, 5$ jeweils mindestens eine p-Sylowgruppe, und diese ist zyklisch und damit auflösbar nach Korollar 1.8.8. Ist eine der p-Sylowgruppen $P \subseteq G$ normal, so ist die Faktorgruppe G/P eine pq-Gruppe und damit nach Korollar 1.9.7 ebenfalls auflösbar. Also ist nach Satz 1.8.7 auch G auflösbar.

Besäße G keine normale p-Sylowgruppe mit $p \in \{2, 3, 5\}$, so wäre die Anzahl s_p der p-Sylowgruppen nach Korollar 1.9.3 mindestens zwei für alle $p \in \{2, 3, 5\}$. Nach dem 1. Satz von Sylow

müsste dann $s_2 \in \{3, 5, 15\}$, $s_3 = 10$ und $s_5 = 6$ gelten. Jede p-Sylowgruppe besitzt als zyklische Gruppe der Ordnung p genau $p-1$ Erzeuger, und jedes Element der Ordnung p erzeugt eine p-Sylowgruppe. Damit gibt es in G genau $n_p = s_p(p-1)$ Elemente der Ordnung p. Aus $s_3 = 10$ und $s_5 = 6$ ergäbe sich dann

$$30 = |G| \geq 1 + n_2 + n_3 + n_5 = 1 + s_2 + 2s_3 + 4s_5 \geq 2s_3 + 4s_5 = 2 \cdot 10 + 4 \cdot 6 = 44.$$

Mit ähnlichen Methoden kann man beweisen, dass jede Gruppe, deren Ordnung ein Produkt dreier Primzahlen ist, auflösbar ist. Dieses Ergebnis ist unter dem Namen *pqr*-Satz bekannt.

Satz 1.9.10 (***pqr*-Satz**)**:** Sei G eine endliche Gruppe, deren Ordnung Produkt von höchstens drei (nicht notwendigerweise verschiedenen) Primzahlen ist. Dann ist G auflösbar.

Zwei Sätze, die ähnlich aussehen, aber deutlich schwieriger zu beweisen sind, sind der *Satz von Burnside*, der 1904 von Burnside bewiesen wurde, und der erst 1962 bewiesene *Satz von Feit-Thompson*, der vorher von Burnside als Vermutung formuliert wurde. Genau wie der *pqr*-Satz dürfen sie in den Übungen, der Klausur und im Staatsexamen nicht verwendet werden. Es wird aber erwartet, dass die Beweismethode des *pqr*-Satzes an Beispielen nachvollzogen werden kann.

Satz 1.9.11 (**Satz von Burnside**)**:** Ist G eine endliche Gruppe, deren Ordnung durch höchstens zwei Primzahlen teilbar ist: $|G| = p^a q^b$ mit $a, b \in \mathbb{N}$ und p, q prim, so ist G auflösbar.

Satz 1.9.12 (**Satz von Feit-Thompson**, ehemalige Burnsidevermutung)**:**
Jede endliche Gruppe ungerader Ordnung ist auflösbar.

Kapitel 2

Ringtheorie

2.1 Ringe und Ringhomomorphismen

Im zweiten Teil der Vorlesung befassen wir uns mit Ringen. Aus der Vorlesung *Lineare Algebra* sind schon viele Beispiele von Ringen bekannt - unter anderem Körper, Endomorphismenringe von Vektorräumen und der Ring der Polynome mit Koeffizienten in einem Körper. Wir führen zunächst den Begriff des Rings ein und untersuchen dann die zugehörigen strukturerhaltenden Abbildungen und grundlegende Konstruktionen mit Ringen.

Definition 2.1.1: Ein **Ring** $(R, +, \cdot)$ ist eine Menge R zusammen mit zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, so dass

(R1) $(R, +)$ eine abelsche Gruppe ist,

(R2) die Verknüpfung $\cdot : R \times R \to R$ **assoziativ** ist: $r \cdot (s \cdot t) = (r \cdot s) \cdot t$ für alle $r, s, t \in R$.

(R3) das **Distributivgesetz** gilt:
$r \cdot (s + t) = r \cdot s + r \cdot t$ und $(r + s) \cdot t = r \cdot t + s \cdot t$ für alle $r, s, t \in R$.

Gilt zusätzlich das **Kommutativgesetz** $r \cdot s = s \cdot r$ für alle $r, s \in R$, so nennt man den Ring $(R, +, \cdot)$ **kommutativ**.

Gibt es zu $\cdot$ ein neutrales Element, also ein Element $1 \in R$ mit $1 \cdot r = r \cdot 1 = r$ für alle $r \in R$, so nennt man $(R, +, \cdot)$ einen **Ring mit Eins**, einen **unitalen Ring** oder einen **unitären Ring**.

Bemerkung 2.1.2.

1. Besitzt ein Ring $(R, +, \cdot)$ ein neutrales Element für die Verknüpfung $\cdot$, so ist es eindeutig. Die beweist man analog zur entsprechenden Aussage für Gruppen.

2. Für die Gruppe $(R, +)$ benutzt man additive Notation. Das neutrale Element wird mit 0 und Inverse mit $-r$ bezeichnet. Das neutrale Element für die Multiplikation $\cdot$ wird mit 1 bezeichnet und multiplikative Inverse mit r^{-1}. Es gilt die Konvention Punkt vor Strich.

3. Die Verknüpfungen werden der Kürze halber oft nicht explizit erwähnt. Man schreibt R statt $(R, +, \cdot)$ und rs statt $r \cdot s$.

4. Es gelten die folgenden **Rechenregeln für Ringe**:
$$0 \cdot r = r \cdot 0 = 0 \qquad (-r) \cdot s = r \cdot (-s) = -r \cdot s \qquad (-r) \cdot (-s) = r \cdot s \qquad \forall r, s \in R.$$
Denn $r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$, und mit der Kürzungsregel in $(R, +)$ folgt $r \cdot 0 = 0$. Daraus ergibt sich $r \cdot s + (-r) \cdot s = (r + (-r)) \cdot s = 0 \cdot s = 0$ und damit $(-r) \cdot s = -r \cdot s$. Die Identitäten $0 \cdot s = 0$ und $r \cdot (-s) = -r \cdot s$ folgen analog, und man erhält $r \cdot s = -(-(r \cdot s)) = -((-r) \cdot s) = (-r) \cdot (-s)$.

Beispiel 2.1.3.

1. Ist $(R, +, \cdot)$ ein unitaler Ring mit $1 = 0$, so folgt aus den Rechenregeln $r = r \cdot 1 = r \cdot 0 = 0$ für alle $r \in R$, also $R = \{0\}$. Dieser Ring heißt **Nullring**.

2. Die ganzen Zahlen bilden einen kommutativen unitalen Ring $(\mathbb{Z}, +, \cdot)$.

3. Jeder Körper $(\mathbb{K}, +, \cdot)$ ist ein kommutativer unitaler Ring. Insbesondere gilt das für die Körper $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$.

4. Für alle $n \in \mathbb{Z}$ ist $(n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring. Er ist unital, wenn $n \in \{0, \pm 1\}$.

5. Für jede Menge $M \neq \emptyset$ und jeden Ring $(R, +, \cdot)$ ist die Menge $\mathrm{Abb}(M, R)$ der Abbildungen $f : M \to R$ mit den Verknüpfungen
$$(f + g)(m) := f(m) + g(m) \qquad (f \cdot g)(m) := f(m) \cdot g(m) \qquad \forall m \in M$$
ein Ring mit der Nullabbildung $0 : M \to R$, $m \mapsto 0_R$ als neutrales Element. Der Ring $\mathrm{Abb}(M, R)$ ist kommutativ genau dann, wenn $(R, +, \cdot)$ kommutativ ist und unital genau dann, wenn $(R, +, \cdot)$ unital ist. Die Eins ist dann die Abbildung $1 : M \to R$, $m \mapsto 1_R$. Für $M = \emptyset$ ist $\mathrm{Abb}(M, R)$ der Nullring. (Warum?).

6. Für jeden Vektorraum V über $\mathbb{K}$ bilden die $\mathbb{K}$-linearen Abbildungen $f : V \to V$ mit der punktweisen Addition und der Verkettung einen unitalen Ring, den **Endomorphismenring** $\mathrm{End}_{\mathbb{K}}(V)$. Er ist kommutativ genau dann, wenn $\dim_{\mathbb{K}}(V) < 2$.

7. Für jede abelsche Gruppe A bilden die Gruppenendomorphismen von A einen unitalen Ring $\mathrm{End}(A)$ mit der punktweisen Addition und der Verkettung.

8. Für $n \in \mathbb{N}_0$ und jeden kommutativen unitalen Ring R bilden die $n \times n$-Matrizen mit Einträgen in R mit der Matrixaddition und Matrixmultiplikation einen Ring $\mathrm{Mat}(n \times n, R)$ mit Eins $\mathbb{1}_n$. Er ist kommutativ genau dann, wenn $n < 2$ oder $R = \{0\}$.

9. Sind $(R, +, \cdot)$ und $(R', +', \cdot')$ (unitale) Ringe, so wird auch die Menge $R \times R'$ zu einem (unitalen) Ring mit den Verknüpfungen
$$(r_1, r_1') + (r_2, r_2') := (r_1 + r_2, r_1' +' r_2') \qquad (r_1, r_1') \cdot (r_2, r_2') := (r_1 \cdot r_2, r_1' \cdot' r_2').$$
Dieser Ring heißt **direktes Produkt** der (unitalen) Ringe $(R, +, \cdot)$, $(R, +', \cdot')$. (Übung).

Beispiel 2.1.4. Für alle $n \in \mathbb{N}_0$ ist $\mathbb{Z}/n\mathbb{Z}$ mit $\bar{z} = z + n\mathbb{Z}$ und den Verknüpfungen
$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ (\bar{k}, \bar{l}) \mapsto \overline{k + l} \qquad \cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ (\bar{k}, \bar{l}) \mapsto \overline{k \cdot l}$$
ein kommutativer Ring mit Einselement $\bar{1}$. Er wird als der **Restklassenring** bezeichnet.

Beweis:
Nach Beispiel 1.3.15 ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine abelsche Gruppe. Die Multiplikation ist wohldefiniert, denn aus $\bar{k} = \bar{k}'$ und $\bar{l} = \bar{l}'$ folgt $k' - k, l' - l \in n\mathbb{Z}$ und damit

$$k' \cdot l' - k \cdot l = k' \cdot l' - k' \cdot l + k' \cdot l - k \cdot l = k'(l' - l) + l(k' - k) \in n\mathbb{Z} \quad \Rightarrow \quad \overline{k' \cdot l'} = \overline{k \cdot l}.$$

Es gilt $\bar{1} \cdot \bar{k} = \overline{1 \cdot k} = k = \overline{k \cdot 1} = \bar{k} \cdot \bar{1}$. Die Assoziativität und Kommutativität der Multiplikation und das Distributivgesetz folgen direkt aus der Assoziativität und Kommutativität der Multiplikation und dem Distributivgesetz in $\mathbb{Z}$. □

Ein weiteres besonders wichtiges Beispiel sind Polynomringe. Sie werden unter anderem dazu genutzt, Körper zu konstruieren, und spielen deswegen auch eine besondere Rolle in der Vorlesung *Körpertheorie*. Polynome werden in der Algebra nicht wie in der Analysis als Abbildungen zwischen verschiedenen Körpern, Vektorräumen oder Ringen aufgefasst, sondern als die Folge ihrer Koeffizienten definiert. Wir werden im Folgenden Koeffizienten in kommutativen, unitalen Ringen zulassen. Die Koeffizienten des Polynoms definieren dann eine Abbildung $p : \mathbb{N}_0 \to R$, die nur an endlich vielen Stellen von Null verschiedene Werte annimmt.

Definition 2.1.5: Sei R ein kommutativer unitaler Ring. Ein **Polynom** mit Koeffizienten in R ist eine Abbildung $p : \mathbb{N}_0 \to R$, $n \mapsto p_n$ mit $p_n = 0$ für fast alle $n \in \mathbb{N}_0$. Die Menge der Polynome mit Koeffizienten in R wird mit $R[x]$ bezeichnet.

- Das Polynom $0 : \mathbb{N}_0 \to R$, $n \mapsto 0$ heißt das **Nullpolynom**.
- Ein Polynom $p \in R[x]$ heißt **konstantes Polynom**, wenn $p_n = 0$ für alle $n \in \mathbb{N}$ gilt.
- Der **Grad** eines Polynoms p ist definiert als $\deg(p) = \max\{n \in \mathbb{N}_0 \mid p_n \neq 0\}$ falls $p \neq 0$ und $\deg(0) = -\infty$.
- Der **Leitkoeffizient** eines Polynoms $0 \neq p \in R[x]$ ist $p_{\deg p}$. Das Polynom heißt **normiert**, falls sein Leitkoeffizient 1 ist.
- Für $k \in \mathbb{N}_0$ bezeichnen wir mit x^k das Polynom mit $x^k_k = 1$ und $x^k_n = 0$ für $n \neq k$ und schreiben $x := x^1$ und $1 := x^0$.

Satz 2.1.6: Für jeden kommutativen unitalen Ring R ist $R[x]$ mit den Verknüpfungen

$$p + q : \mathbb{N}_0 \to R,\ n \mapsto p_n + q_n \qquad p \cdot q : \mathbb{N}_0 \to R,\ n \mapsto \Sigma_{k=0}^{n} p_k q_{n-k} \tag{2.1}$$

ein kommutativer unitaler Ring, der **Polynomring** $R[x]$ mit Nullelement $0 : \mathbb{N}_0 \to R$, $n \mapsto 0$ und Einselement $1 : \mathbb{N}_0 \to R$, $n \mapsto \delta_0(n)$.

Jedes Polynom $p \in R[x]$ lässt sich eindeutig schreiben als $p = \Sigma_{n=0}^{\infty} p_n x^n$ mit $p_n = 0$ für fast alle $n \in \mathbb{N}_0$. Die Addition und Multiplikation bekommen dann die Form

$$(\Sigma_{n=0}^{\infty} a_n x^n) + (\Sigma_{n=0}^{\infty} b_n x^n) = \Sigma_{n=0}^{\infty} (a_n + b_n) x^n, \quad (\Sigma_{n=0}^{\infty} a_n x^n) \cdot (\Sigma_{n=0}^{\infty} b_n x^n) = \Sigma_{n=0}^{\infty} (\Sigma_{k=0}^{n} a_k b_{n-k}) x^n.$$

Beweis:
Dass $(R[x], +)$ eine abelsche Gruppe ist folgt bereits aus Beispiel 2.1.3, 5. Die restlichen Ringaxiome ergeben sich durch Nachrechnen. Da $p_n = 0$ für fast alle $n \in \mathbb{N}_0$, ergibt sich $p_n = \sum_{k=0}^{\infty} p_k x_n^k$ für alle $n \in \mathbb{N}_0$ und damit $p = \sum_{k=0}^{\infty} p_k x^k$ für jedes Polynom $p \in R[x]$. □

Man beachte, dass ein Polynom mit Koeffizienten in R etwas grundsätzlich anderes ist als eine **polynomiale Abbildung** $p : R \to R$, $r \mapsto \Sigma_{n=0}^{\infty} a_n r^n$. Für einen endlichen Ring R gibt es nämlich nur endlich viele Abbildungen $f : R \to R$ und damit auch nur endlich viele polynomiale Abbildungen. Es gibt aber unendlich viele Polynome mit Koeffizienten in R. Dies ist der Grund, warum man mit abstrakten Polynomen statt mit polynomialen Abbildungen arbeitet.

Die Forderung, dass alle bis auf endlich viele Koeffizienten eines Polynoms verschwinden, ist für die Ringstruktur unnötig. Tatsächlich können wir auch beliebige Abbildungen $p : \mathbb{N}_0 \to R$ zulassen und erhalten mit den selben Verknüpfungen einen weiteren Ring. Seine Addition und Multiplikation entsprechen der Addition und Multiplikation von Potenzreihen, nur dass hier keine Forderungen an Konvergenz gestellt werden.

Beispiel 2.1.7. Eine **formale Potenzreihe** mit Koeffizienten in einem kommutativen unitalen Ring R ist eine Abbildung $p : \mathbb{N}_0 \to R$. Die formalen Potenzreihen bilden mit den Verknüpfungen in (2.1) einen kommutativen unitalen Ring $R[[x]]$.

Ebenso kann man Polynome in mehreren Variablen bilden. Dazu betrachtet man Abbildungen $f : \mathbb{N}_0^k \to R$, die fast überall verschwinden, und Verknüpfungen analog zu (2.1). Ebenso kann man auch formale Potenzreihen in mehreren Variablen einführen.

Beispiel 2.1.8. Der **Polynomring** $R[x_1, ..., x_m]$ **in** m **Variablen** mit Koeffizienten in einem kommutativen unitalen Ring R ist die Menge der Abbildungen

$$p : \mathbb{N}_0^m \to R,\ (n_1, ..., n_m) \mapsto p_{n_1,...,n_m} \quad \text{mit} \quad p_{n_1,...,n_m} = 0 \ \text{ für fast alle } (n_1, ..., n_m) \in \mathbb{N}_0^m$$

und den Verknüpfungen

$$p + q : \mathbb{N}_0^m \to R,\ (n_1, ..., n_m) \mapsto p_{n_1,...,n_m} + q_{n_1,...,n_m}$$
$$p \cdot q : \mathbb{N}_0^m \to R,\ (n_1, ..., n_m) \mapsto \sum_{k_1=0}^{n_1} \cdots \sum_{k_m=0}^{n_m} p_{k_1,...,k_m} q_{n_1-k_1,...,n_m-k_m} .$$

Er ist ein kommutativer unitaler Ring. Das Polynom $p : \mathbb{N}_0 \to R$ mit $p_{n_1,...,n_m} = 1$, $p_{k_1,...,k_m} = 0$ für $(k_1, ..., k_m) \neq (n_1, ..., n_m)$ wird mit $x_1^{n_1} \cdots x_m^{n_m}$ bezeichnet.

Nachdem wir Beispiele von Ringen kennengelernt haben, untersuchen wir nun etwas genauer die Struktur von unitalen Ringen. Auch wenn ein Ring unital ist, also ein Einselement für die Multiplikation besitzt, wird in der Definition nicht gefordert, dass multiplikative Inverse zu Elementen eines Rings existieren. Ringelemente, für die dies der Fall ist, heißen *Einheiten*.

Definition 2.1.9: Sei R ein unitaler Ring.

1. Ein Element $r \in R$ heißt **Einheit**, wenn es ein Element $s \in R$ mit $r \cdot s = s \cdot r = 1$ gibt.
2. Die Menge der Einheiten in R wird mit $R^\times$ bezeichnet.
3. Gilt $R^\times = R^* := R \setminus \{0\}$, so nennt man R einen **Schiefkörper**.

Lemma 2.1.10: Die Einheiten in einem unitalen Ring R bilden mit der Multiplikation eine Gruppe mit neutralem Element $1 \in R^\times$.

Beweis:
Für Einheiten $r, r' \in R^\times$ gibt es $s, s' \in R$ mit $rs = sr = 1$ und $s'r' = r's' = 1$. Daraus folgt $(s's)(rr') = s'(sr)r' = s'r' = 1 = rs = r(r's')s = (rr')(s's)$, also auch $rr' \in R^\times$. Die Multiplikation auf R definiert also eine assoziative Verknüpfung $\cdot : R^\times \times R^\times \to R^\times$. Es gilt $1 \cdot r = r \cdot 1 = r$ für alle $r \in R^\times$ (neutrales Element), und für $r \in R^\times$ mit $rs = sr = 1$ ist auch $s \in R^\times$ (Inverse). □

Da $0 \cdot r = r \cdot 0 = 0$ für alle $r \in R$ ist das Nullelement genau dann eine Einheit, wenn $1 = 0$, also $R = \{0\}$ gilt. Ebenso sieht man anhand von Definition 2.1.9, dass der Nullring kein Schiefkörper ist, und dass ein Schiefkörper genau dann ein Körper ist, wenn er kommutativ ist.

Beispiel 2.1.11.

1. Die Einheitengruppe des Rings $\mathbb{Z}$ ist $\mathbb{Z}^\times = \{-1, 1\}$.
2. Die Einheitengruppe eines Polynomrings $R[x]$ besteht genau aus den konstanten Polynomen $r = rx^0 : \mathbb{N}_0 \to R$ mit $r \in R^\times$.
3. Die Einheitengruppe des Endomorphismenrings $\mathrm{End}_{\mathbb{K}}(V)$ eines Vektorraums V ist gerade seine Automorphismengruppe: $\mathrm{End}_{\mathbb{K}}(V)^\times = \mathrm{Aut}_{\mathbb{K}}(V)$.
4. Die Einheitengruppe des Endomorphismenrings $\mathrm{End}(A)$ einer abelschen Gruppe A ist ihre Automorphismengruppe $\mathrm{Aut}(A)$.
5. Die Einheitengruppe eines Matrixrings $\mathrm{Mat}(n \times n, R)$ besteht genau aus den Matrizen, deren Determinante eine Einheit in R ist. Denn nach der Cramerschen Regel, die auch in kommutativen unitalen Ringen gilt, ist eine Matrix $M \in \mathrm{Mat}(n \times n, R)$ invertierbar genau dann, wenn $\det(M) \in R^\times$ gilt.
6. Wir werden später zeigen, dass die Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ genau die Restklassen der zu n teilerfremden Zahlen sind.

Nachdem wir die grundlegenden Strukturmerkmale von Ringen untersucht haben, befassen wir uns nun mit den strukturerhaltenden Abbildungen. Da ein Ring insbesondere eine abelsche Gruppe ist, müssen mit der Ringstruktur verträgliche Abbildungen Gruppenhomomorphismen zwischen den additiven Gruppen sein. Zusätzlich fordert man noch Kompatibilität mit der Multiplikation. Anders als im Fall der Gruppe folgt daraus *nicht* automatisch, dass eine solche Abbildung auch die Einselemente unitaler Ringe aufeinander abbildet. Dies wurde im Fall von Gruppen nämlich aus der Existenz von Inversen gefolgert. Für unitale Ringe kann man dies als zusätzliche Forderung stellen. Je nachdem, ob man diese Forderung stellt oder nicht, erhält man unterschiedliche Begriffe von strukturerhaltenden Abbildungen.

Definition 2.1.12: Seien R, S Ringe. Eine Abbildung $f : R \to S$ heißt **Ringhomomorphismus**, wenn:
(RH1) $f : (R, +) \to (S, +)$ ein Gruppenhomomorphismus ist: $f(r+r') = f(r)+f(r')\ \forall r, r' \in R$,
(RH2) $f(r \cdot r') = f(r) \cdot f(r')$ für alle $r, r' \in R$.

Sind R, S unital und gilt zusätzlich $f(1_R) = 1_S$, so nennt man f einen **unitalen Ringhomomorphismus**. Ein bijektiver Ringhomomorphismus heißt **Ringisomorphismus**.

Monomorphismen, Epimorphismen, Endomorphismen und Automorphismen von Ringen oder unitalen Ringen werden analog definiert. Die Kerne und Bilder von Ringhomomorphismen sind bereits definiert, denn Ringhomomorphismen sind insbesondere Gruppenhomomorphismen, und damit ist ihr Kern der Kern des entsprechenden Gruppenhomomorphismus.

Ebenso wie sich isomorphe Gruppen gruppentheoretisch nicht unterscheiden lassen, lassen sich isomorphe (unitale) Ringe ringtheoretisch nicht unterschieden. Sie gehen im Wesentlichen durch Umbenennung der Elemente auseinander hervor, und man möchte sie als äquivalent betrachten. Damit *isomorph sein* die drei Bedingungen an eine Äquivalenzrelation erfüllt, benötigt man, dass die Identitätsabbildung ein (unitaler) Ringhomomorphismus ist, dass das Inverse eines (unitalen) Ringisomorphismus wieder ein unitaler Ringisomorphismus ist, und die Verkettung zweier (unitaler) Ringhomomorphismen wieder ein unitaler Ringhomomorphismus. Dies sind die Ring-Gegenstücke der Aussagen in Satz 1.1.11 für Gruppen.

Satz 2.1.13: Seien R, S, T (unitale) Ringe.

1. Dann ist $\mathrm{id}_R : R \to R$ ein (unitaler) Ringautomorphismus.
2. Für jeden (unitalen) Ringisomorphismus $f : R \to S$ ist auch die Umkehrabbildung $f^{-1} : S \to R$ ein (unitaler) Ringisomorphismus.
3. Sind $f : R \to S$ und $g : S \to T$ (unitale) Ringhomomorphismen, so ist auch die Verkettung $g \circ f : R \to T$ ein (unitaler) Ringhomomorphismus.

Beweis:
Da die entsprechenden Aussagen für Homomorphismen von Gruppen bereits in Satz 1.1.11 bewiesen wurden, ist nur noch zu zeigen, dass die entsprechenden Abbildung mit der Ringmultiplikation und im Fall unitaler Ringe mit den Einselementen verträglich sind. Für id_R ist dies offensichtlich. Ist $f : R \to S$ ein unitaler Ringisomorphismus, so ergibt sich für alle $s, s' \in S$ $f^{-1}(s) \cdot f^{-1}(s') = f^{-1}(f(f^{-1}(s) \cdot f^{-1}(s'))) = f^{-1}(f(f^{-1}(s)) \cdot f(f^{-1}(s'))) = f^{-1}(s \cdot s')$ und $f^{-1}(1_S) = f^{-1}(f(1_R)) = 1_R$. Ebenso erhält man $g \circ f(r \cdot r') = g(f(r) \cdot f(r')) = g(f(r)) \cdot g(f(r'))$ und $g(f(1_R)) = g(1_S) = 1_T$ für alle unitalen Ringhomomorphismen $f : R \to S$ und $g : S \to T$. □

Korollar 2.1.14: Für jeden (unitalen) Ring R bilden die (unitalen) Ringautomorphismen von R mit der Verkettung eine Gruppe. Diese wird als die **Automorphismengruppe** von R und mit $\mathrm{Aut}(R)$ bezeichnet.

Beispiel 2.1.15.

1. Zu jedem Ring R gibt es genau einen Ringhomomorphismus $f : R \to 0$ und genau einen Ringhomomorphismus $f : 0 \to R$.
2. Die Abbildung $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ mit $f(\bar{0}) = \bar{0}$ und $f(\bar{1}) = \bar{3}$ ist ein Ringhomomorphismus zwischen unitalen Ringen aber kein unitaler Ringhomomorphismus.

3. Ist $\mathrm{ggT}(m,n)=1$, so ist $f:\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, $k+mn\mathbb{Z}\mapsto(k+m\mathbb{Z},k+n\mathbb{Z})$ ein unitaler Ringisomorphismus. Die Bijektivität folgt aus dem chinesischen Restsatz.

4. Die komplexe Konjugation $^-:\mathbb{C}\to\mathbb{C}$, $x+\mathrm{i}y\mapsto x-\mathrm{i}y$ ist ein unitaler Ringautomorphismus.

5. Für jeden unitalen Ring R und jede Einheit $r\in R^\times$ ist $C_r:R\to R$, $s\mapsto rsr^{-1}$ ein unitaler Ringautomorphismus.

6. Für jeden kommutative unitalen Ring R ist die Inklusionsabbildung $\iota:R\to R[x]$, $r\mapsto rx^0$ ein unitaler Ringmonomorphismus.

7. Für jeden kommutative unitalen Ring R und jedes $r\in R$ ist die **Evaluationsabbildung** $\mathrm{ev}_r:R[x]\to R$, $p=\Sigma_{n=0}^\infty a_nx^n\mapsto p(r):=\Sigma_{n=0}^\infty a_nr^n$ ein unitaler Ringhomomorphismus.

8. Für jeden kommutativen unitalen Ring R ist die Abbildung $\mathrm{ev}:R[x]\to\mathrm{Abb}(R,R)$ die einem Polynom p die Polynomabbildung $\mathrm{ev}(p):R\to R$, $r\mapsto\mathrm{ev}_r(p)=p(r)$ zuordnet, ein unitaler Ringhomomorphismus. Ob sie injektiv und surjektiv ist, hängt von R ab.

9. Für jeden unitalen Ringhomomorphismus $f:R\to S$ ist die Abbildung $f_*:R[x]\to S[x]$, $p\mapsto f\circ p$ ein unitaler Ringhomomorphismus.

10. Für jeden kommutativen unitalen Ring R ist die Abbildung

$$\varphi:R[x_1,...,x_m]\to R[x_1,...,x_{m-1}][x_m],\quad p\mapsto\Sigma_{k=0}^\infty\varphi_k(p)x_m^k$$

mit $\varphi_k(p):\mathbb{N}_0^{m-1}\to R$, $(n_1,...,n_{m-1})\mapsto p_{n_1,...,n_{m-1},k}$ ein unitaler Ringisomorphismus. Dies zeigt, dass wir den Polynomring $R[x_1,...,x_m]$ aus Beispiel 2.1.8 auch als den Polynomring in *einer* Variablen x_m mit Koeffizienten im Ring $R[x_1,...,x_{m-1}]$ auffassen können.

Der Ring $\mathbb{Z}$ spielt bezüglich der unitalen Ringhomomorphismen eine besondere Rolle. Da jeder Gruppenhomomorphismus $f:\mathbb{Z}\to R$ durch $f(1)$ bereits eindeutig bestimmt ist, gibt es zu jedem unitalen Ring R genau einen unitalen Ringhomomorphismus $f:\mathbb{Z}\to R$, nämlich den Gruppenhomomorphismus $f:\mathbb{Z}\to R$ mit $f(1)=1_R$. Sein Kern ist eine Untergruppe von $\mathbb{Z}$ und damit nach Beispiel 1.2.6 von der Form $\ker(f)=n\mathbb{Z}$ für ein $n\in\mathbb{N}_0$. Er enthält wichtige Informationen über den Ring R.

Satz 2.1.16: Zu jedem unitalen Ring R gibt es genau einen unitalen Ringhomomorphismus $f:\mathbb{Z}\to R$, den **kanonischen Ringhomomorphismus** $f:\mathbb{Z}\to R$, $n\mapsto n1_R$.

Sein Kern ist von der Form $\ker(f)=n\mathbb{Z}$ mit $n\in\mathbb{N}_0$. Die Zahl n heißt **Charakteristik** von R und wird mit $n=\mathrm{char}(R)$ bezeichnet.

Beispiel 2.1.17.

1. Die Körper $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und der Ring $\mathbb{Z}$ haben Charakteristik 0.
2. Der Ring $\mathbb{Z}/n\mathbb{Z}$ hat Charakteristik $\mathrm{char}(\mathbb{Z}/n\mathbb{Z})=n$.
3. Für jeden endlichen Ring R ist $\mathrm{char}(R)$ ein Teiler von $|R|$.

   Denn die Charakteristik ist dann nichts anderes als die Ordnung von 1_R in der abelschen Gruppe $(R,+)$, die nach dem Satz von Lagrange die Gruppenordnung teilt.
4. Ist $R=\mathbb{K}$ ein Körper, so gilt entweder $\mathrm{char}(\mathbb{K})=0$, oder $\mathrm{char}(\mathbb{K})$ ist eine Primzahl. Denn wäre $\mathrm{char}(\mathbb{K})=m\cdot n$ mit $m,n>1$, so wäre $(n1_\mathbb{K})\cdot(m1_\mathbb{K})=(nm)1_\mathbb{K}=0$, aber $m1_\mathbb{K},n1_\mathbb{K}\neq 0$ - ein Widerspruch.

Ein unitaler Ringhomomorphismus $f : \mathbb{Z} \to S$ ist also bereits durch die Eigenschaft, ein unitaler Ringhomomorphismus zu sein, vollständig bestimmt. Auch ein unitaler Ringhomomorphismus $f' : R[x] \to S$ aus einem Polynomring $R[x]$ ist durch relativ wenige Daten bestimmt. Er wird durch seine Werte auf den konstanten Polynomen und auf dem Polynom x eindeutig festgelegt. Erstere definieren einen Ringhomomorphismus $f : R \to S$ und letzterer kann beliebig vorgegeben werden. Der zugehörige Ringhomomorphismus $f' : R[x] \to S$ ist dann durch die Inklusion $\iota_{R[x]} : R \to R[x]$, die Evaluation $\mathrm{ev}_s : S[X] \to S$ und die Abbildung $f_* : R[x] \to S[x]$ aus Beispiel 2.1.15, 6., 7. und 9 gegeben.

Satz 2.1.18: Sei $f : R \to S$ ein unitaler Ringhomomorphismus und $\iota : R \to R[x]$ die kanonische Inklusion aus Beispiel 2.1.15, 6. Dann gibt es zu jedem Element $s \in S$ genau einen unitalen Ringhomomorphismus $f' : R[x] \to S$ mit $f' \circ \iota = f$ und $f'(x) = s$, nämlich

$$f' = \mathrm{ev}_s \circ f_* : \quad \Sigma_{n=0}^{\infty} a_n x^n \mapsto \Sigma_{n=0}^{\infty} f(a_n) s^n.$$

Dies bezeichnet man als die **universelle Eigenschaft des Polynomrings**

$$\begin{array}{ccc} R & \xhookrightarrow{\iota} & R[x] \\ {\scriptstyle f}\downarrow & \swarrow_{\exists! f'} & \\ S & & \end{array}$$

Beweis:
Die Abbildung $\mathrm{ev}_s \circ f_* : R[x] \to S$ ist ein Ringhomomorphismus als Verkettung zweier Ringhomomorphismen (vgl. Beispiel 2.1.15). Es gilt $\mathrm{ev}_s \circ f_* \circ \iota(r) = \mathrm{ev}_s(f(r)) = f(r)$ für alle $r \in R$ und $\mathrm{ev}_s \circ f_*(x) = \mathrm{ev}_s(x) = s$. Ist $f' : R[x] \to S$ ein weiterer unitaler Ringhomomorphismus mit $f' \circ \iota = f$ und $f'(x) = s$, so folgt

$$f'\left(\Sigma_{n=0}^{\infty} a_n x^n\right) = \Sigma_{n=0}^{\infty} f(a_n) \cdot f'(x)^n = \Sigma_{n=0}^{\infty} f(a_n) s^n = \mathrm{ev}_s\left(\Sigma_{n=0}^{\infty} f(a_n) x^n\right) = \mathrm{ev}_s \circ f_*\left(\Sigma_{n=0}^{\infty} a_n x^n\right).$$

□

2.2 Unterringe

Wie im Fall von Gruppen untersuchen wir nun systematisch die grundlegenden Konstruktionen für Ringe, nämlich Ringe, die in anderen Ringen enthalten sind und anschließend Quotienten von Ringen. Da Ringe immer auch abelsche Gruppen sind, ergibt sich die Hälfte der Konstruktion bereits aus der entsprechenden Konstruktion für Gruppen. Es müssen nur noch Zusatzbedingungen an die Multiplikation auferlegt werden und gegebenenfalls für unitale Ringe entsprechende Bedingungen an die Einselemente.

Definition 2.2.1: Sei R ein Ring. Ein **Unterring** oder **Teilring** von R ist eine Teilmenge $U \subseteq R$, so dass

(UR1) $(U, +)$ eine Untergruppe von $(R, +)$ ist,

(UR2) $r \cdot s \in U$ für alle $r, s \in U$ gilt.

Ist R unital, so nennt man einen Teilring $U \subseteq R$ **unitalen Unterring** oder **unitalen Teilring** falls zusätzlich $1_R \in U$ gilt.

Bemerkung 2.2.2.

1. Man kann einen (unitalen) Unterring äquivalent auch als eine Teilmenge von R definieren, die mit den Einschränkungen der Verknüpfungen auf R (und der Eins von R) einen (unitalen) Ring bildet.
2. Die Inklusionsabbildung $\iota : U \to R$, $u \mapsto u$ ist ein (unitaler) Ringmonomorphismus.
3. Ein unitaler Unterring $U \subseteq R$ hat die gleiche Charakteristik wie R. Denn aus $1_R \in U$ folgt, dass auch die von 1_R erzeugte Untergruppe von $(R, +)$ in U enthalten ist.

Beispiel 2.2.3.

1. Für jeden Ring R sind $\{0\} \subseteq R$ und $R \subseteq R$ Unterringe. Unterringe $U \subsetneq R$ heißen **echte Unterringe** und Unterringe $\{0\} \subsetneq U$ heißen **nichttriviale Unterringe**.
2. Für $n \in \mathbb{Z}$ ist $n\mathbb{Z} \subseteq \mathbb{Z}$ ein Unterring. Er ist ein unitaler Unterring genau dann, wenn $n \in \{\pm 1\}$ gilt.
3. Die Teilmenge $\{\bar{0}, \bar{3}\} \subseteq \mathbb{Z}/6\mathbb{Z}$ ist ein unitaler Ring mit Einselement $\bar{3}$ und ein Unterring von $\mathbb{Z}/6\mathbb{Z}$, aber kein unitaler Unterring.
4. Das **Zentrum** $Z(R) = \{r \in R \mid rs = sr \; \forall s \in R\}$ eines (unitalen) Rings R ist ein (unitaler) Unterring von R.
5. Für jeden kommutativen unitalen Ring R bilden die oberen Dreiecksmatrizen, die unteren Dreiecksmatrizen und die Diagonalmatrizen unitale Unterringe von $\mathrm{Mat}(n \times n, R)$.
6. Für jeden unitalen Unterring $U \subseteq R$ eines kommutativen unitalen Rings R ist der Ring $\mathrm{Mat}(n \times n, U)$ ein unitaler Unterring von $\mathrm{Mat}(n \times n, R)$.
7. Der **Quaternionenring**
$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$$
ist ein unitaler Unterring von $\mathrm{Mat}(2 \times 2, \mathbb{C})$. Er ist ein Schiefkörper.
8. Der Ring $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$ der **Gaußschen Zahlen** ist ein unitaler Unterring von $\mathbb{C}$.
9. Für jede Zahl $n \in \mathbb{N}$ ist $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ ein unitaler Unterring von $\mathbb{R}$.
10. Ist R ein (unitaler) Ring und $R_i \subseteq R$ (unitale) Unterringe von R für alle $i \in I$, so ist auch $\cap_{i \in I} R_i$ ein (unitaler) Unterring von R. Der Beweis ist analog zu dem von Satz 1.2.9.

Analog zu den entsprechenden Aussagen für Gruppen in Lemma 1.2.8, sind auch Bilder und Urbilder von (unitalen) Unterringen unter Ringhomomorphismen immer (unitale) Unterringe. Aufpassen muss man dabei nur beim Kern eines unitalen Ringhomomorphismus, der im allgemeinen *kein unitaler Unterring* ist.

Lemma 2.2.4: Sei $f : R \to S$ ein (unitaler) Ringhomomorphismus. Dann gilt:

1. Für jeden (unitalen) Unterring $U \subseteq R$ ist das Bild $f(U) \subseteq S$ ein (unitaler) Unterring.
2. Für jeden (unitalen) Unterring $V \subseteq S$ ist das Urbild $f^{-1}(V) \subseteq R$ ein (unitaler) Unterring.
3. Insbesondere ist das **Bild** $\mathrm{im}(f) = f(R) \subseteq S$ ein (unitaler) Unterring und der **Kern** $\ker(f) = f^{-1}(0) \subseteq R$ ein Unterring.

Beweis:
In Lemma 1.2.8 wurde bereits gezeigt, dass diese Mengen Untergruppen der abelschen Gruppen $(R,+)$ oder $(S,+)$ bilden. Zu zeigen ist nur noch die Abgeschlossenheit unter der Multiplikation und die Unitalität. Ersteres ist völlig analog zum Beweis von Lemma 1.2.8. Sind R, S und $f : R \to S$ zusätzlich unital, so gilt $f(1_R) = 1_S$. Also ist für jeden unitalen Unterring $U \subseteq R$ auch $1_S = f(1_R) \in f(U)$ und für jeden unitalen Unterring $V \subseteq S$ auch $1_R \in f^{-1}(1_S) \subseteq f^{-1}(V)$. Damit sind Bilder und Urbilder unitaler Unterringe unital, insbesondere das Bild $f(R)$. □

2.3 Ideale und Faktorringe

In Analogie zu den entsprechenden Konstruktionen für Vektorräume und Gruppen möchten wir nun Quotienten von Ringen bezüglich geeigneter Unterringe bilden. Da jeder Ring $(R,+,\cdot)$ eine abelsche Gruppe $(R,+)$ definiert und ein Unterring $U \subseteq R$ eine Untergruppe $(U,+) \subseteq (R,+)$, sollten die resultierenden Quotienten durch die Faktorgruppe R/U gegeben sein. Zusätzlich möchte man diese Faktorgruppe aber mit einer Multiplikation versehen, die durch die Multiplikation auf R definiert wird, und ihr die Struktur eines Rings verleiht.

Wir betrachten also eine Untergruppe $U \subseteq R$ und die Äquivalenzrelation $r \sim r' \Leftrightarrow r - r' \in U$ mit den Nebenklassen $r + U$ als Äquivalenzklassen. Dann ist nach Satz 1.3.14 die Quotientenmenge $R/U = \{r + U \mid r \in R\}$ eine abelsche Gruppe mit $(r + U) + (s + U) = (r + s) + U$, und die kanonische Surjektion $\pi_U : R \to R/U$, $r \mapsto r + U$ ist ein Gruppenhomomorphismus.

Wir möchten nun eine Multiplikation auf R/U definieren, indem wir $(r+U)\cdot(s+U) = (rs)+U$ setzen. Dazu müssen wir Wohldefiniertheit nachweisen. Sind $r' \sim r$ und $s' \sim s$, so gibt es $u, v \in U$ mit $r' = r + u$ und $s' = s + v$. Daraus folgt $r's' - rs = r(s' - s) + (r' - r)s' = rv + us$. Eine vernünftige Bedingung, die sicherstellt, dass $r's' - rs \in U$ und damit $r's' + U = rs + U$ gilt, ist also die Forderung $ru, ur \in U$ für alle $r \in R$ und $u \in U$. Dies führt auf den Begriff des Ideals. Analog gibt es auch den Begriff des Linksideals und des Rechtsideals, die jeweils nur eine dieser beiden Forderungen stellen.

Definition 2.3.1: Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt

1. **Ideal**, falls $(I,+) \subseteq (R,+)$ eine Untergruppe ist und $r \cdot i, i \cdot r \in I$ für alle $i \in I$, $r \in R$,
2. **Linksideal**, falls $(I,+) \subseteq (R,+)$ eine Untergruppe ist und $r \cdot i \in I$ für alle $i \in I$, $r \in R$,
3. **Rechtsideal** falls $(I,+) \subseteq (R,+)$ eine Untergruppe ist und $i \cdot r \in I$ für alle $i \in I$, $r \in R$.

Offensichtlich ist ein Ideal in R ein Unterring von R, aber im allgemeinen kein unitaler Unterring. Ist nämlich R unital und I ein Ideal in R mit $1_R \in I$, so folgt $r = r \cdot 1_R \in I$ für alle $r \in R$, also $I = R$. Ideale übernehmen für Quotienten von Ringen die Rolle, die Normalteiler für Quotienten von Gruppen spielen. In der Tat erhält man analog zu Satz 1.3.14

Satz 2.3.2: Sei R ein (unitaler) Ring und $I \subseteq R$ ein Ideal.

1. Dann ist R/I ein (unitaler) Ring mit den Verknüpfungen
$$(r + I) + (s + I) := (r + s) + I \qquad (r + I) \cdot (s + I) := (rs) + I.$$
Er heißt **Faktorring** oder **Quotientenring** von R bezüglich I.

2. Die **kanonische Surjektion** $\pi_I : R \to R/I$, $r \mapsto r + I$ ist ein surjektiver (unitaler) Ringhomomorphismus mit Kern $\ker(\pi_I) = I$.

Beweis:
Nach Satz 1.3.14 ist R/I eine abelsche Gruppe und die kanonische Surjektion π_I ein surjektiver Gruppenhomomorphismus mit $\ker(\pi_I) = I$. Die Multiplikation ist wohldefiniert, denn aus $r+I = r'+I$ und $s+I = s'+I$ folgt $r-r', s-s' \in I$ und $r's'-rs = (r'-r)s'+r(s'-s) \in I$. Die Assoziativität der Multiplikation und die Distributivgesetze folgen direkt aus der Definition der Verknüpfungen und den entsprechenden Aussagen für R

$$\begin{aligned}((r+I)\cdot(s+I)))\cdot(t+I) &= ((rs)+I)\cdot(t+I) = ((rs)t)+I = (r(st))+I\\ &= (r+I)\cdot((st)+I) = (r+I)\cdot((s+I)\cdot(t+I))\\ ((r+I)+(s+I)))\cdot(t+I) &= ((r+s)+I)\cdot(t+I) = (r+s)t+I = (rt+st)+I\\ &= (rt+I)+(st+I) = (r+I)\cdot(t+I)+(s+I)\cdot(t+I)\\ (r+I)\cdot((s+I)+(t+I)) &= (r+I)\cdot((s+t)+I) = r(s+t)+I = (rs+rt)+I\\ &= (rs+I)+(rt+I) = (r+I)\cdot(s+I)+(r+I)\cdot(t+I).\end{aligned}$$

Dass die kanonische Surjektion ein Ringhomomorphismus ist, folgt aus der Definition der Multiplikation auf R/I, denn $\pi_I(r\cdot s) = (rs)+I = (r+I)\cdot(s+I) = \pi_I(r)\cdot\pi_I(s)$. Ist R unital, so ergibt sich $(1_R+I)\cdot(r+I) = (1_R\cdot r)+I = r+I = (r\cdot 1_R)+I = (r+I)\cdot(1_R+I)$ und damit ist auch R/I ein unitaler Ring mit Einselement $1_R+I = \pi_I(1_R)$ und π_I ein unitaler Ringhomomorphismus. □

Beispiel 2.3.3.

1. Für jeden Ring R sind $\{0\} \subseteq R$ und $R \subseteq R$ Ideale in R. Ein Ideal $I \subseteq R$ heißt **echtes Ideal** wenn $I \neq R$ und **nichttriviales Ideal** wenn $\{0\} \neq I$.

2. Ist R ein Schiefkörper, so sind $\{0\}$ und R die einzigen Ideale in R.

   Denn ist $I \subseteq R$ ein Ideal und $0 \neq r \in I$, so folgt auch $r^{-1}r = 1_R \in I$ und damit $s = s\cdot 1_R \in I$ für alle $s \in R$, also $I = R$.

3. Die Ideale im Ring $\mathbb{Z}$ sind genau die Teilmengen $n\mathbb{Z} \subseteq \mathbb{Z}$. Dies sind nach Beispiel 1.2.6 genau die Untergruppen von $\mathbb{Z}$.

4. Für jeden Ring R, jede Menge M und jede Teilmenge $U \subseteq M$ ist

   $$I_U = \{f : M \to R \mid f(u) = 0\ \forall u \in U\}$$

   ein Ideal im Ring $\mathrm{Abb}(M,R)$ aus Beispiel 2.1.3, 5.

5. Die Teilmenge $C_c^\infty(\mathbb{R})$ der glatten Funktionen mit kompaktem Träger ist ein Ideal im Ring $C^\infty(\mathbb{R})$ der glatten Funktionen auf $\mathbb{R}$ mit der punktweisen Addition und Multiplikation.

6. Für jeden Körper $\mathbb{K}$ ist $I_A = \{p \in \mathbb{K}[x] \mid p(A) = 0\}$ für eine Matrix $A \in \mathrm{Mat}(n\times n, \mathbb{K})$ ein Ideal im Polynomring $\mathbb{K}[x]$.

7. Für jeden Körper $\mathbb{K}$ und $1 \leq k \leq n$ sind die Teilmengen

   $$L_k = \{A \in \mathrm{Mat}(n\times n, \mathbb{K}) \mid a_{1k} = a_{2k} = \ldots = a_{nk} = 0\}$$

   Linksideale im Ring $\mathrm{Mat}(n\times n, \mathbb{K})$, aber keine Rechtsideale, und die Teilmengen

   $$R_k = \{A \in \mathrm{Mat}(n\times n, \mathbb{K}) \mid a_{k1} = a_{k2} = \ldots = a_{kn} = 0\}$$

   Rechtsideale, aber keine Linksideale. Die einzigen Ideale in $\mathrm{Mat}(n\times n, \mathbb{K})$ sind das Nullideal $\{0\} \subseteq \mathrm{Mat}(n\times n, \mathbb{K})$ und $\mathrm{Mat}(n\times n, \mathbb{K})$ selbst.

Ideale spielen also für Ringe die gleiche Rolle wie Normalteiler für Gruppen. Da wir damit Faktorringe konstruieren können, lohnt es sich, die Eigenschaften von Idealen zu untersuchen und systematisch Ideale zu konstruieren. Wir verallgemeinern die entsprechenden Konstruktionen für Untergruppen und Normalteiler auf Ideale.

Lemma 2.3.4: Sei R ein Ring, I eine Indexmenge und J_i ein Ideal in R für alle $i \in I$. Dann ist auch $\cap_{i\in I} J_i$ ein Ideal in R.

Beweis:
Nach Satz 1.2.9 ist der Schnitt $J := \cap_{i\in I} J_i$ eine Untergruppe von $(R, +)$. Ist nun $j \in J$, so gilt $j \in J_i$ für alle $i \in I$, und da J_i ein Ideal in R ist, folgt $r \cdot j, j \cdot r \in J_i$ für alle $i \in I$ und $r \in R$. Damit ist aber auch $r \cdot j, j \cdot r \in \cap_{i\in I} J_i$ für alle $r \in R$ und damit $r \cdot j, j \cdot r \in J$. Also ist J ein Ideal. □

Damit können wir auch das von einer Teilmenge eines Rings erzeugte Ideal definieren als das kleinste Ideal, das diese Teilmenge enthält, also den Schnitt aller Ideale, die diese Teilmenge enthalten. Dies wurde in Definition 1.2.11 analog für Untergruppen durchgeführt, und es gibt auch eine entsprechende Konstruktion für Normalteiler.

Definition 2.3.5: Sei R ein Ring und $M \subseteq R$ eine Teilmenge. Dann ist das **von M erzeugte Ideal** (M) das kleinste Ideal in R, das M enthält

$$(M) = \bigcap_{I\subseteq R \text{ Ideal},\ M\subseteq I} I. \tag{2.2}$$

Ein Ideal $I \subseteq R$ heißt **endlich erzeugt** falls es eine endliche Menge $M \subseteq R$ gibt mit $I = (M)$ und **Hauptideal** falls es eine einelementige Menge M gibt mit $I = (M)$.

Für $M = \{r_1, ..., r_n\}$ mit $n \in \mathbb{N}$ schreibt man auch $(M) = (r_1, ..., r_n)$.

Hauptideale nehmen unter den Idealen eine ähnliche Rolle ein, wie zyklische Gruppen unter den Gruppen. Dementsprechend ist auch die Struktur eines Hauptideals viel einfacher als die eines allgemeinen Ideals. Für nicht-kommutative Ringe, ist es oft kompliziert, das von einer Teilmenge erzeugte Ideal explizit zu beschreiben. Dies vereinfacht sich wesentlich für kommutative unitale Ringe. Dort enthält das von einer Teilmenge erzeugte Ideal gerade die endlichen Linearkombinationen von Elementen aus der Menge mit Koeffizienten im betrachteten Ring. Für eine einelementige Menge reduziert sich das auf die Vielfachen des Elements.

Lemma 2.3.6: Ist R ein kommutativer unitaler Ring, so ist das von $M \subseteq R$ erzeugte Ideal

$$(M) = \{\Sigma_{k=0}^{n} m_k r_k \mid n \in \mathbb{N}, m_k \in M, r_k \in R\} \qquad (\emptyset) = \{0\}.$$

Insbesondere gilt: $(m) = Rm = \{rm \mid r \in R\}$ für alle $m \in R$.

Beweis:
Ist $M = \emptyset$, so ist $(M) = \{0\}$. Sei also $M \neq \emptyset$ und $M' := \{\sum_{k=0}^{n} r_k m_k \mid n \in \mathbb{N}, m_k \in M, r_k \in R\}$.

1. $(M) \subseteq M'$: Wir zeigen, dass $M' \subseteq R$ ein Ideal ist, das M enthält. Damit nimmt M' am Schnitt in (2.2) teil, und es folgt $(M) \subseteq M'$. Offensichtlich ist $0 = 0 \cdot m \in M'$ für alle $m \in M$. Sind $u, v \in M'$, so können wir ohne Beschränkung der Allgemeinheit annehmen, dass

$u = \Sigma_{k=0}^{n} r_k m_k$ und $v = \Sigma_{k=0}^{n} s_k m_k$ mit $m_k \in M$ und $r_k, s_k \in R$ gilt. Denn tritt in einer der Linearkombinationen ein Element aus M auf, das in der anderen nicht auftritt, so können wir es dort mit Koeffizient $0 \in R$ hinzufügen. Daraus ergibt sich $u+v = \Sigma_{k=0}^{n}(r_k+s_k)m_k \in M'$ und $-u = \Sigma_{k=0}^{n}(-r_k)m_k \in M'$. Damit ist M' eine Untergruppe von R. Für alle $r \in R$ gilt außerdem $r \cdot u = \Sigma_{k=0}^{n}(rr_k)m_k \in M'$ und $u \cdot r = \Sigma_{k=0}^{n}(r_k r)m_k \in M'$, und damit ist M' ein Ideal in R. Ausserdem gilt $M \subseteq M'$, denn $m = 1 \cdot m \in M'$ für alle $m \in M$.

2. $M' \subseteq (M)$: Ist I ein Ideal in R mit $M \subseteq I$, so ist $rm \in I$ für alle $r \in R$, $m \in M$. Induktiv folgt, dass auch alle endlichen Summen solcher Elemente in I enthalten sind. Damit ist $M' \subseteq I$ für alle Ideale I in R mit $M \subseteq I$, und damit auch in ihrem Schnitt (M) enthalten. □

Wie auch das Verhalten von Normalteilern unter Gruppenhomomorphismen untersucht wurde, bietet es sich an, das Verhalten von Idealen unter Ringhomomorphismen zu untersuchen. Es zeigt sich, dass auch die Urbilder von Idealen unter Ringhomomorphismen Ideale sind. Damit ist nicht nur jedes Ideal Kern eines Ringhomomorphismus, nämlich der kanonischen Surjektion aus Satz 2.3.2, sondern auch jeder Kern eines Ringhomomorphismus ein Ideal. Ideale sind also nichts anderes als Kerne von Ringhomomorphismen. Damit auch die Bilder von Idealen wieder Ideale sind, muss man wie bei der entsprechenden Aussage für Normalteiler Surjektivität fordern. Analog zu Lemma 1.3.18 erhalten wir dann die folgenden Aussagen.

Lemma 2.3.7: Für jeden Ringhomomorphismus $f : R \to S$ gilt:

1. Das Urbild $f^{-1}(J)$ jedes Ideals $J \subseteq S$ ist ein Ideal in R.
2. Ist f surjektiv, so ist das Bild $f(I)$ jedes Ideals $I \subseteq R$ ein Ideal in S.
3. Insbesondere ist der Kern $\ker(f) = f^{-1}(0)$ ein Ideal in R.

Beweis:
Dass Urbilder und Bilder von Idealen Untergruppen sind, folgt aus Lemma 1.3.18. Zu zeigen ist noch, dass die zweite Bedingung erfüllt ist. Ist $J \subseteq S$ ein Ideal in S, so gilt $f(r \cdot i) = f(r) \cdot f(i) \in J$ und $f(i \cdot r) = f(i) \cdot f(r) \in J$ für alle $r \in R$ und $i \in f^{-1}(J)$ und damit ist auch $f^{-1}(J)$ ein Ideal in R. Ist I ein Ideal in R und f surjektiv, so gibt es zu jedem $s \in S$ ein $r \in R$ mit $f(r) = s$, und es folgt $s \cdot f(i) = f(r) \cdot f(i) = f(r \cdot i) \in f(I)$ und $f(i) \cdot s = f(i) \cdot f(r) = f(i \cdot r) \in f(I)$ für alle $j = f(i) \in f(I)$. Also ist auch $f(I)$ ein Ideal in S. □

Die Surjektivitätsbedingung für Bilder von Idealen kann erfüllt werden, indem wir statt dem Ringhomomorphismus $f : R \to S$ seine Koeinschränkung $f : R \to f(R)$ betrachten. Indem wir Lemma 2.3.7 mit den Ergebnissen für Unterringe aus Lemma 2.2.4 kombinieren, erhalten wir ein Analogon der Untergruppenkorrespondenz 1.3.19 für Ringe, das unter dem Namen *Idealkorrespondenz* bekannt ist. Der Beweis ist analog zu dem von Satz 1.3.19 (Übung).

Satz 2.3.8 (Idealkorrespondenz):

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

$$\varphi_f : \{\text{Unterringe } U \text{ von } R \text{ mit } \ker(f) \subseteq U\} \to \{\text{Unterringe von } f(R)\}, \quad U \mapsto f(U)$$

eine Bijektion mit Inversem

$$\varphi_f^{-1} : \{\text{Unterringe von } f(R)\} \to \{\text{Unterringe } U \text{ von } R \text{ mit } \ker(f) \subseteq U\}, \quad V \mapsto f^{-1}(V).$$

Ein Unterring $U \subseteq R$ ist ein Ideal in R genau dann, wenn $\varphi_f(U) = f(U)$ ein Ideal in $f(R)$ ist.

Die Untergruppenkorrespondenz erlaubt es einem, statt Untergruppen und Normalteilern in der Faktorgruppe G/N Untergruppen und Normalteiler in der Gruppe G zu betrachten, die N enthalten. Analog erlaubt es uns die Idealkorrespondenz, statt Unterringen und Idealen im Ring R/I Untergruppen und Ideale im Ring R zu betrachten, die das Ideal I enthalten. Dazu wendet man Satz 2.3.8 auf die kanonische Surjektion $\pi_I : R \to R/I$ mit $\ker(\pi_I) = I$ an.

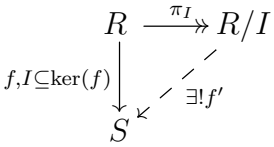
Korollar 2.3.9: Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann stehen die Unterringe (Ideale) in R/I in Bijektion mit den Unterringen (Idealen) in R, die I enthalten.

Ebenso wie Korollar 2.3.9 Unterringe und Ideale eines Faktorrings R/I durch Unterringe und Ideale in R beschreibt, können wir auch Ringhomomorphismen aus dem Faktorring $f : R/I \to S$ durch Ringhomomorphismen $f : R \to S$ beschreiben, die das Ideal $I \subseteq R$ in ihrem Kern enthalten. Dies entspricht der entsprechenden Aussage für Faktorgruppen in Satz 1.3.21.

Satz 2.3.10:
Sei R ein (unitaler) Ring und I ein Ideal in R. Dann gibt es zu jedem (unitalen) Ringhomomorphismus $f : R \to S$ mit $I \subseteq \ker(f)$ genau einen (unitalen) Ringhomomorphismus $f/I : R/I \to S$ mit $f/I \circ \pi_I = f$, nämlich

$$f/I : R/I \to S, \quad r + I \mapsto f(r).$$

Die bezeichnet man als die **charakteristische Eigenschaft des Faktorrings**



Beweis:
Ist $f : R \to S$ ein Ringhomomorphismus mit $I \subseteq \ker(f)$, so ist f auch ein Gruppenhomomorphismus zwischen R und S. Nach Satz 1.3.21 gibt es dazu genau einen Gruppenhomomorphismus $f' : R/I \to S$ mit $f' \circ \pi_I = f$, nämlich $f' = f/I : R/I \to S$, $r + I \mapsto f(r)$. Zu zeigen ist nur noch, dass f/I ein Ringhomomorphismus ist und unital, falls f unital ist. Dazu berechnet man $(f/I)((r+I)\cdot(s+I)) = (f/I)((rs)+I) = f(rs) = f(r)\cdot f(s) = (f/I)(r+I)\cdot(f/I)(s+I)$ für alle $r, s \in R$ und $(f/I)(1_R + I) = f(1_R) = 1_S$. □

Indem man für einen Ringhomomorphismus $f : R \to S$ das Ideal $I = \ker(f)$ anwendet, ergibt sich aus Satz 2.3.10 dann ein Analogon des Noetherschen Homomorphiesatzes 1.3.23 für Ringe. Man erhält nämlich einen Ringhomomorphismus $f/\ker(f) : R/\ker(f) \to S$ mit $\ker(f/\ker(f)) = \{r + \ker(f) \mid f(r) = 0\} = \ker(f)$, und damit ist $f/\ker(f)$ injektiv.

Satz 2.3.11 (Homomorphiesatz):
Sei $f : R \to S$ ein (unitaler) Ringhomomorphismus. Dann ist die Abbildung

$$f/\ker(f) : R/\ker(f) \to S, \quad r + \ker(f) \mapsto f(r)$$

ein injektiver (unitaler) Ringhomomorphismus, also ein Isomorphismus auf ihr Bild.

Der Homomorphiesatz ist hilfreich, um die Isomorphie eines Faktorrings R/I zu einem anderen Ring S zu beweisen. Dazu reicht es aus, einen surjektiven Ringhomomorphismus $f : R \to S$ mit $\ker(f) = I$ zu konstruieren. Dieses Verfahren wird oft angewendet, um Körper oder Ringe als Quotienten von Polynomringen zu konstruieren.

Beispiel 2.3.12. Wir betrachten einen kommutativen unitalen Ring R und das von dem Polynom x erzeugte Hauptideal $(x) \subseteq R[x]$. Dann gilt: $R[x]/(x) \cong R$.

Beweis:
Die Evaluationsabbildung $\mathrm{ev}_0 : R[x] \to R$, $\Sigma_{n=0}^{\infty} a_n x^n \mapsto a_0$ ist ein surjektiver unitaler Ringhomomorphismus, deren Kern gerade die Polynome $\Sigma_{n=0}^{\infty} a_n x^n$ mit $a_0 = 0$ enthält. Damit gilt $\ker(f) = (x)$ und nach dem Homomorphiesatz 2.3.11 erhalten wir einen Ringisomorphismus

$$\mathrm{ev}_0/\ker(\mathrm{ev}_0) : \mathbb{R}[x]/(x) \to R, \quad \Sigma_{n=0}^{\infty} a_n x^n + (x) \mapsto a_0. \qquad \square$$

Beispiel 2.3.13. Wir betrachten den Polynomring $\mathbb{R}[x]$ und das von dem Polynom $x^2 + 1$ erzeugte Hauptideal $(x^2 + 1)$. Der Faktorring $\mathbb{R}[x]/(x^2 + 1)$ ist isomorph zum Körper $\mathbb{C}$.

Beweis:
Nach Satz 2.1.18 gibt es genau einen Ringhomomorphismus $f : \mathbb{R}[x] \to \mathbb{C}$ mit $f(a) = a$ für alle $a \in \mathbb{R}$ und $f(x) = \mathrm{i}$, nämlich

$$f : \mathbb{R}[x] \to \mathbb{C}, \quad \Sigma_{n=0}^{\infty} a_n x^n \mapsto \Sigma_{n=0}^{\infty} a_n \mathrm{i}^n = \Sigma_{n=0}^{\infty} (-1)^n a_{2n} + \mathrm{i}\, \Sigma_{n=0}^{\infty} (-1)^n a_{2n+1}$$

Da $f(1) = 1$ und $f(a + bx) = a + \mathrm{i}b$ ist dies ein surjektiver unitaler Ringhomomorphismus. Da $f(x^2 + 1) = 0$ folgt $(x^2 + 1) = \mathbb{R}[x] \cdot (x^2 + 1) \subseteq \ker(f)$. Mit Satz 2.3.10 erhalten wir einen surjektiven unitalen Ringhomomorphismus

$$f/\ker(f) : \mathbb{R}[x]/(x^2 + 1) \to \mathbb{C}, \quad p + (x^2 + 1) \mapsto f(p).$$

Mit Polynomdivision können wir jedes Polynom $p \in \mathbb{R}[x]$ schreiben als $p = q(x^2 + 1) + r$ mit $q, r \in \mathbb{R}[x]$ und $\deg(r) < 2$. Damit ist $\mathbb{R}[x]/(x^2 + 1) = \{a + bx + (x^2 + 1) \mid a, b \in \mathbb{R}\}$. Da $f/\ker(f)(a + bx + (x^2 + 1)) = f(a + bx) = a + \mathrm{i}b$ ist $\ker(f/\ker(f)) = (x^2 + 1)$. Also ist $f/\ker(f)$ ein Ringisomorphismus, und es folgt $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. $\square$

Beispiel 2.3.14. Der Ring $\mathbb{Z}[x]/(x^2 + 1)$ ist isomorph zum Ring $\mathbb{Z}[\mathrm{i}]$ der Gaußschen Zahlen.

Beweis:
Dies folgt direkt aus Beispiel 2.3.13, indem wir den Ringhomomorphismus $f : \mathbb{R}[x] \to \mathbb{C}$ aus Beispiel 2.3.13 einschränken zu einem Ringhomomorphismus $f : \mathbb{Z}[x] \to \mathbb{Z}[\mathrm{i}]$. $\square$

2.4 Konstruktion von Körpern

Im letzten Abschnitt haben wir bekannte Konstruktionen für Gruppen systematisch auf Ringe verallgemeinert, wobei Unterringe den Untergruppen, Ideale den Normalteilern und Faktorringe den Faktorgruppen entsprechen. In diesem Abschnitt werden wir die Konstruktionen systematisch benutzen, um Körper zu konstruieren. Dabei gibt es im Wesentlichen zwei Verfahren. Das erste ist, Körper als Quotienten von Ringen zu konstruieren, wie die Konstruktion der komplexen Zahlen in Beispiel 2.3.13. Um dies systematisch zu betreiben, benötigen wir Kriterien, die garantieren, dass der entstehende Faktorring ein Körper ist. Das zweite Verfahren verallgemeinert die Konstruktion des Körper $\mathbb{Q}$ aus den ganzen Zahlen.

2.4.1 Faktorringe maximaler Ideale

Wir beginnen mit der Konstruktion von Körpern als Faktorringe von kommutativen unitalen Ringen. Ausgangspunkt ist die Beobachtung, dass Körper unter den kommutativen unitalen Ringen eine ähnliche Rolle spielen wie einfache Gruppen unter den Gruppen. Eine einfache Gruppe ist eine nichttriviale Gruppe, die außer sich selbst und der trivialen Untergruppe keine Normalteiler enthält. Analog können wir einen Körper charakterisieren als einen nichttrivialen kommutativen unitalen Ring, der außer sich selbst und dem Nullideal keine Ideale enthält.

Lemma 2.4.1: Ein kommutativer unitaler Ring R ist genau dann ein Körper, wenn $R \neq \{0\}$ und R außer $I = \{0\}$ und $I = R$ keine weiteren Ideale besitzt.

Beweis:
Sei zunächst R ein Körper und $I \neq \{0\}$ ein Ideal in R. Dann enthält I ein Element $0 \neq r \in I$. Da R ein Körper ist, ist r eine Einheit und es gilt $1 = r^{-1}r \in I$. Daraus folgt $s = s \cdot 1 \in I$ für alle $s \in R$ und damit $I = R$. Ist umgekehrt $\{0\}$ das einzige echte Ideal von R und $r \in R \setminus \{0\}$, so gilt $r \in (r) = I$ und damit $(r) \neq \{0\}$. Also ist $(r) = R$, es folgt $1 \in (r)$ und damit gibt es ein Element $r^{-1} \in r$ mit $r^{-1} \cdot r = r \cdot r^{-1} = 1$. □

Damit ist es eine naheliegende Strategie, einen kommutativen, unitalen Ring zu einem Körper zu machen, indem man ein Ideal maximaler Größe aus dem Ring herausteilt. Das richtige Konzept von maximaler Größe ergibt sich aus der Idealkorrespondenz. Denn nach der Idealkorrespondenz entsprechen Ideale in einem Faktorring R/I Idealen in R, die I enthalten. Damit kann R/I nur dann ein Körper sein, wenn es kein echtes Ideal J in R gibt, das I enthält und echt größer ist als I. Diese Bedingung ist auch hinreichend.

Definition 2.4.2: Sei R ein kommutativer Ring. Ein Ideal $I \subseteq R$ heißt **maximal**, wenn $I \subsetneq R$ gilt und es kein echtes Ideal $I \subsetneq J \subsetneq R$ gibt.

Satz 2.4.3: Sei R ein kommutativer unitaler Ring und I ein Ideal in R. Dann ist der Faktorring R/I genau dann ein Körper, wenn I maximal ist.

Beweis:
Nach Lemma 2.4.1 ist R/I genau dann ein Körper, wenn $R/I \neq \{0\}$ und R/I außer $\{0\}$ und R/I keine echten Ideale besitzt. Nach der Idealkorrespondenz 2.3.8 stehen die Ideale in R/I in Bijektion mit den Idealen von R, die I enthalten. Also ist R/I genau dann ein Körper, wenn $I \subsetneq R$ das einzige echte Ideal ist, das I enthält. Das bedeutet, dass I ein maximales Ideal ist. □

Korollar 2.4.4: Sei $p \in \mathbb{N}_0$. Dann ist $\mathbb{Z}/p\mathbb{Z}$ ein genau dann ein Körper, wenn p eine Primzahl ist. Dieser Körper wird auch mit $\mathbb{F}_p$ bezeichnet.

Beweis:
Nach Satz 2.4.3 ist $\mathbb{Z}/p\mathbb{Z}$ genau dann ein Körper, wenn $p\mathbb{Z}$ ein maximales Ideal in $\mathbb{Z}$ ist. Daraus folgt schon $p \neq 1$. Nach Beispiel 2.3.3, 3. sind die Ideale in $\mathbb{Z}$ genau die Teilmengen $n\mathbb{Z}$ für $n \in \mathbb{N}_0$, und es gilt $p\mathbb{Z} \subseteq n\mathbb{Z}$ genau dann, wenn n ein Teiler von p ist. Also ist $p\mathbb{Z}$ genau dann maximal, wenn $n = 1$ und $n = p$ die einzigen Teiler von p sind. □

Wir werden das Argument aus dem Beweis von Korollar 2.4.4 später auf andere kommutative unitale Ringe verallgemeinern, in denen ein vernünftiges Konzept von Teilbarkeit existiert. Zunächst stellt sich aber die Frage, ob überhaupt jeder kommutative unitale Ring maximale Ideale besitzt, also durch Quotientenbildung einen Körper liefert. Dies folgt aus dem Zornschen Lemma, das wiederum äquivalent zum Auswahlaxiom ist. Es handelt sich also im Wesentlichen um ein Postulat. Um das Zornsche Lemma zu formulieren, benötigen wir die Begriffe einer partiell geordneten Menge, einer Kette und einer oberen Schranke.

Definition 2.4.5: Eine **partiell geordnete Menge** $(X, \preceq)$ ist eine Menge X zusammen mit einer Relation $\preceq$ auf X mit den folgenden Eigenschaften:

(PO1) reflexiv: $x \preceq x$ für alle $x \in X$,
(PO2) transitiv: $x \preceq y$, $y \preceq z \Rightarrow x \preceq z$,
(PO3) antisymmetrisch: $(x \preceq y) \wedge (y \preceq x) \Rightarrow x = y$.

- Eine Teilmenge $K \subseteq X$ heißt **Kette** oder **total geordnet** falls $k \preceq k'$ oder $k' \preceq k$ $\forall k, k' \in K$.
- Eine **obere Schranke** einer Teilmenge $M \subseteq X$ ist ein Element $x \in X$ mit $m \preceq x$ $\forall m \in M$.

Beispiel 2.4.6.

1. Die Relation $\leq$ ist eine partielle Ordnung auf jeder Teilmenge von $\mathbb{R}$.
2. Die Relation $a \preceq b$, wenn a ein Teiler von b ist, ist eine partielle Ordnung auf $\mathbb{N}$.
3. Für jede Menge M ist $\subseteq$ eine partielle Ordnung auf der Potenzmenge von M und auf jeder Teilmenge der Potenzmenge.

Lemma 2.4.7 (Zornsches Lemma): Sei $(\emptyset \neq X, \preceq)$ eine partiell geordnete Menge, so dass jede Kette eine obere Schranke besitzt. Dann besitzt X ein **maximales Element**, ein Element $x \in X$, so dass aus $x \preceq y$ für ein $y \in X$ folgt $y = x$.

Den Beweis, dass das Zornsche Lemma äquivalent zum Auswahlaxiom ist, werden wir in der Vorlesung nicht führen. Wir beweisen aber mit dem Zornschen Lemma, dass jeder kommutative unitale Ring ein maximales Ideal besitzt. Dies liefert zwar kein Verfahren, um maximale Ideale zu bestimmen, zeigt aber, dass jeder kommutative unitale Ring einen Körper definiert.

Satz 2.4.8: Jeder kommutative unitale Ring $R \neq \{0\}$ besitzt ein maximales Ideal.

Beweis:
Sei X die Menge der echten Ideale von R mit der partiellen Ordnung $\subseteq$ aus Beispiel 2.4.6, 3.

Wir zeigen, dass jede total geordnete Teilmenge $Y \subseteq X$ eine obere Schranke besitzt. Für $Y = \varnothing$ ist $\{0\}$ eine obere Schranke (hier geht $R \neq \{0\}$ ein, denn in $R = \{0\}$ ist $\{0\}$ kein echtes Ideal). Sei nun $Y \neq \varnothing$. Wir setzen $J := \cup_{I \in Y} I$.

- J ist ein Ideal:
Seien $j_1, j_2 \in J$ und $r \in R$ beliebig. Dann gibt es Ideale $I_1, I_2 \in Y$ mit $j_1 \in I_1$ und $j_2 \in I_2$. Da Y total geordnet ist, gilt $I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$. Dann sind $j_1 + j_2$, 0, $-j_1$ und rj_1 Elemente von I_2 bzw. I_1 und damit auch von J.

- J ist ein echtes Ideal:
Wäre $J = R$, so wäre $1 \in J$ und damit auch $1 \in I$ für ein $I \in Y$. Daraus folgt $R = R \cdot 1 \subseteq I$, und damit $I \notin X$, ein Widerspruch.

Damit ist $J \in X$. Da offensichtlich $I \preceq J$ für alle $I \in Y$, ist J eine obere Schranke von Y. Damit ist gezeigt, dass jede total geordnete Teilmenge Y eine obere Schranke besitzt. Das Zornsche Lemma 2.4.7 liefert dann ein maximales Ideal in R. □

Korollar 2.4.9: Sei R ein kommutativer Ring mit Eins und I ein echtes Ideal von R. Dann ist I in einem maximalen Ideal von R enthalten.

Beweis:
Da $I \neq R$ ist $R/I \neq \{0\}$ und besitzt damit nach Satz 2.4.8 ein maximales Ideal. Dieses entspricht nach der Idealkorrespondenz 2.3.8 einem maximalen Ideal von R, das I enthält. □

Korollar 2.4.10: Sei R ein kommutativer Ring mit Eins und I ein echtes Ideal von R. Dann gibt es einen Körper $\mathbb{K}$ und einen unitalen surjektiven Ringhomomorphismus $\varphi : R \to \mathbb{K}$ mit $\varphi(I) = \{0\}$.

Beweis:
Da $I \neq R$, gibt es nach Korollar 2.4.9 ein maximales Ideal $J \subsetneq R$ mit $I \subseteq J$. Damit ist nach Satz 2.4.3 R/J ein Körper und die kanonische Surjektion $\pi_J : R \to R/J$ ein unitaler surjektiver Ringhomomorphismus mit $I \subseteq J = \ker(\pi_J)$. □

2.4.2 Integritätsbereiche und Quotientenkörper

Wir wenden uns nun dem zweiten wichtigen Verfahren zur Konstruktion von Körpern zu. Dabei wird kein Quotient eines Rings gebildet sondern es werden verallgemeinerte Brüche von Elementen aus einem kommutativen unitalen Ring gebildet. Dies verallgemeinert die Konstruktion der rationalen Zahlen aus den ganzen Zahlen. Damit bei der Multiplikation von Brüchen im Nenner keine Null entsteht, keine muss sichergestellt werden, dass das Produkt zweier von Null verschiedener Zahlen nie Null ist.

Definition 2.4.11: Sei R ein Ring.

1. Ein Element $r \in R$ heißt **Nullteiler**, wenn es ein $s \in R \setminus \{0\}$ gibt mit $rs = 0$ oder $sr = 0$.
2. Der Ring R heißt **nullteilerfrei**, wenn $R \neq \{0\}$ gilt und $0 \in R$ der einzige Nullteiler ist.
3. Der Ring R heißt **Integritätsbereich** oder **Integritätsring**, wenn er kommutativ, unital und nullteilerfrei ist.

Beispiel 2.4.12.

1. Der Ring $\mathbb{Z}$ ist Integritätsbereich.
2. Jeder Körper ist ein Integritätsbereich. Denn zu jedem Element $r \neq 0$ gibt es ein multiplikatives Inverses r^{-1}. Ist $r \cdot s = 0$, so folgt $0 = r^{-1} \cdot (r \cdot s) = (r^{-1}r) \cdot s = s$.
3. Unitale Unterringe von Integritätsbereichen sind Integritätsbereiche. Insbesondere gilt dies für unitale Unterringe von Körpern, wie den Ring $\mathbb{Z}[\mathrm{i}]$ der Gaußschen Zahlen.

4. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist Integritätsbereich genau dann, wenn n eine Primzahl ist.

   Ist nämlich $n = p \cdot k$ mit $p, k \in \{2, ..., n-1\}$, so gilt $\bar{p} \cdot \bar{k} = \bar{n} = \bar{0}$ und $\bar{p}, \bar{k} \neq 0$, und damit sind $\bar{p}, \bar{k}$ Nullteiler. Ist dagegen n eine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper nach Korollar 2.4.4 und damit auch ein Integritätsbereich.

Die Nullteilerfreiheit in einem Integritätsbereich R wirkt sich auch auf die Polynome mit Koeffizienten in R aus. Sie garantiert nämlich, dass im Produkt zweier Polynome das Produkt der höchsten nichtverschwindenden Koeffizienten nicht verschwindet. Damit addieren sich unter der Multiplikation von Polynomen deren Grade. Daraus kann man folgern, dass auch der Polynomring $R[x]$ ein Integritätsbereich ist.

Lemma 2.4.13: Sei R ein Integritätsbereich. Dann gilt:

1. $\deg(p \cdot q) = \deg(p) + \deg(q)$ für alle $p, q \in R[x]$, wobei $-\infty + n := -\infty$ für $n \in \mathbb{N}_0 \cup \{-\infty\}$.
2. Der Polynomring $R[x]$ ist ein Integritätsbereich.

Beweis:
1. Ist $p = 0$ oder $q = 0$ ist die Aussage wahr. Ist $\deg(p) = n \in \mathbb{N}_0$ und $\deg(q) = m \in \mathbb{N}_0$, so sind p, q von der Form $p = \sum_{k=0}^{n} a_k x^k$ und $q = \sum_{l=0}^{m} b_l x^l$ mit $a_n, b_m \neq 0$, und es ergibt sich $p \cdot q = \sum_{k=0}^{n+m} (\sum_{l=0}^{k} a_l b_{k-l}) x^k$. Da R nullteilerfrei ist, folgt $a_n b_m \neq 0$ und $\deg(p \cdot q) = n + m$.

2. Sind $p, q \in R[x]$ mit $p \cdot q = 0$, so folgt $\deg(p) + \deg(q) = \deg(p \cdot q) = -\infty$ und damit $\deg(p) = -\infty$ und $p = 0$ oder $\deg(q) = -\infty$ und $q = 0$. Damit ist $R[x]$ nullteilerfrei, also ein Integritätsbereich. □

Durch Iteration dieses Arguments kann man zeigen, dass auch die Polynomringe in mehreren Variablen über einem Integritätsbreich R wieder Integritätsbereiche sind. Denn nach Beispiel 2.1.15, 10 ist der Polynomring in $R[x_1, ..., x_m]$ isomorph zu dem Polynomring $R[x_1, ..., x_{m-1}][x_m]$. Aus Lemma 2.4.13 folgt dann induktiv, dass $R[x_1, ..., x_m]$ ein Integritätsbereich ist.

Korollar 2.4.14: Für jeden Integritätsbereich R ist auch der Polynomring $R[x_1, ..., x_m]$ ein Integritätsbereich für alle $m \in \mathbb{N}$.

Ähnlich wie bei der Konstruktion von Körpern kann man auch Bedingungen an ein Ideal angeben, unter denen der zugehörige Faktorring ein Integritätsbereich ist. Während für Körper maximale Ideale benötigt werden, benötigt man für Integritätsbereiche Primideale.

Definition 2.4.15: Sei R ein kommutativer Ring. Ein Ideal $I \subset R$ heißt **Primideal**, wenn $I \neq R$ und aus $r, s \in R$ mit $rs \in I$ folgt, dass $r \in I$ oder $s \in I$ gilt.

Satz 2.4.16: Sei R ein kommutativer (unitaler) Ring und I ein Ideal in R. Dann ist R/I nullteilerfrei (ein Integritätsbereich) genau dann, wenn $I \subseteq R$ ein Primideal ist.

Beweis:
Ist $I \subsetneq R$ ein Primideal, so folgt aus $(r + I) \cdot (s + I) = rs + I = I$ auch $r \in I$ oder $s \in I$, also $r + I = I$ oder $s + I = I$. Damit ist R/I nullteilerfrei. Ist umgekehrt R/I nullteilerfrei, so gilt $I \neq R$. Aus $r, s \in R$ mit $rs \in I$ ergibt sich $(r + I) \cdot (s + I) = rs + I = I$ und wegen der Nullteilerfreiheit damit $r + I = I$ oder $s + I = I$, also $r \in I$ oder $s \in I$. Damit ist I ein Primideal. Nach Satz 2.3.2 ist R/I unital, falls R unital ist, und damit folgt die Behauptung. □

Korollar 2.4.17: Maximale Ideale in einem kommutativen unitalen Ring sind Primideale.

Beweis:
Ist R ein kommutativer unitaler Ring und $I \subseteq R$ ein maximales Ideal, so ist nach Satz 2.4.3 der Faktorring R/I ein Körper, und damit auch ein Integritätsbereich. Daraus folgt mit Satz 2.4.16, dass I ein Primideal ist. □

Beispiel 2.4.18.

1. Für jede Primzahl p ist $p\mathbb{Z} \subseteq \mathbb{Z}$ ein Primideal.
2. Das Nullideal in einem kommutativen unitalen Ring R ist genau dann ein Primideal, wenn R nullteilerfrei ist.
3. Das Ideal $I = 4\mathbb{Z}$ im Ring $2\mathbb{Z}$ ist ein maximales Ideal, aber kein Primideal, denn $2 \notin I$, aber $2 \cdot 2 \in I$. Die Voraussetzung in Korollar 2.4.17, dass R unital ist ist also notwendig.
4. Das Ideal (x) in $\mathbb{Z}[x]$ ist ein Primideal, aber kein maximales Ideal.

   Denn nach nach Beispiel 2.3.12 ist $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ und damit ist (x) ein Primideal nach Satz 2.4.16. Da $\mathbb{Z}$ kein Körper ist, kann (x) nach Satz 2.4.3 kein maximales Ideal sein. In der Tat gilt $(x) \subsetneq (x, 2) \subsetneq \mathbb{Z}[x]$, denn $2 \in (x, 2) \setminus (x)$ und $3 \in \mathbb{Z}[x] \setminus (x, 2)$.

Aus einen Integritätsbereich R können wir nun in Analogie zur Konstruktion von $\mathbb{Q}$ aus den ganzen Zahlen einen Körper konstruieren, indem wir Brüche bilden. Das bedeutet, dass wir Zahlenpaare (a, b) mit $a \in R$ und $0 \neq b \in R$ betrachten und zwei Zahlenpaare (a, b) und (c, d) identifizieren, wenn $ad = bc$ gilt. Dies entspricht genau dem üblichen Kürzen von Brüchen, denn zwei Brüche $a/b \in \mathbb{Q}$ und $c/d \in \mathbb{Q}$ sind genau dann gleich, wenn $ad = bc$ gilt.

Satz 2.4.19: Sei R ein Integritätsbereich.

1. Dann ist $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ eine Äquivalenzrelation auf $R \times R \setminus \{0\}$.
   Die Äquivalenzklasse von $(a, b) \in R \times R \setminus \{0\}$ wird mit a/b bezeichnet und $a := a/1$.
2. Die Quotientenmenge $Q(R)$ wird ein Körper mit den Verknüpfungen

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

   Er heißt der **Quotientenkörper** des Integritätsbereichs R.

Beweis:
1. Wegen $ab = ab$ gilt $(a, b) \sim (a, b)$ für alle $a \in R$, $0 \neq b \in R$ (Reflexivität). Die Bedingung $ad = bc$ ist invariant unter Vertauschen von (a, b) mit (c, d) und damit gilt $(a, b) \sim (c, d)$ genau dann wenn $(c, d) \sim (a, b)$ (Symmetrie). Ist $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$, so folgt $ad = bc$ und $cf = ed$. Daraus ergibt sich $d(af - be) = adf - bde = bcf - bde = b(cf - ed) = 0$. Da $d \neq 0$ und R nullteilerfrei ist, folgt $af - be = 0$, also $(a, b) \sim (e, f)$ (Transitivität).

2. Wir zeigen, dass die Verknüpfungen wohldefiniert sind. Ist $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$, so ist $a'b = ab'$ und $c'd = cd'$, und daraus ergibt sich

$$(a'd' + b'c')bd - (ad + bc)b'd' = d'd(a'b - ab') + b'b(c'd - d'c) = 0,$$

also $(a'd' + b'c', b'c') \sim (ad + bc, bd)$. Ebenso erhalten wir

$$(a'c')(bd) - (ac)(b'd') = (a'b)(c'd) - (ab')(cd') = (ab')(cd') - (ab')(cd') = 0,$$

also $(a'c', b'd') \sim (ac, bd)$. Damit sind die Verknüpfungen wohldefiniert. Beide Verknüpfungen sind offensichtlich kommutativ, und $\cdot$ ist offenbar assoziativ. Die Assoziativität von $+$ folgt aus einer direkten Rechnung:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + ebd}{bdf} = \frac{a}{b} + \frac{cf + ed}{df} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right).$$

Offensichtlich ist $0 = 0/1$ das neutrale Element der Addition und $-a/b$ das additive Inverse von a/b. Es ist $1 = 1/1$ das neutrale Element der Multiplikation, und für $a/b \neq 0$ ist $a \neq 0$ und damit b/a das multiplikative Inverse von a/b. Das Distributivgesetz folgt durch Nachrechnen:

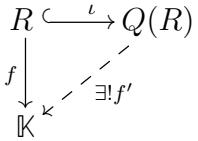
$$\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ad + bc}{bd} \cdot \frac{e}{f} = \frac{ade + bce}{bdf} = \frac{ae}{bf} + \frac{ce}{df} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}. \qquad \square$$

Ähnlich wie Faktorringe zeichnen sich auch Quotientenkörper von Integritätsbereichen durch eine charakteristische Eigenschaft aus. Diese erlaubt es, jeden injektiven unitalen Ringhomomorphismus $f : R \to \mathbb{K}$ aus einem Integritätsbereich R in einen Körper $\mathbb{K}$ zu einem injektiven unitalen Ringhomomorphismus $f' : Q(R) \to \mathbb{K}$ fortzusetzen. Ähnlich wie die charakteristische Eigenschaft des Faktorrings erspart sie es einem, immer wieder die die Wohldefiniertheit einer Abbildung und ihre Kompatibilität mit der Ringstruktur nachzurechnen. Sie ist auch sehr nützlich, um die Isomorphie eines Quotientenkörpers zu einem anderen Körper zu beweisen.

Satz 2.4.20: Sei R ein Integritätsbereich und $Q(R)$ sein Quotientenkörper. Dann gilt:

1. Die Einbettung $\iota : R \to Q(R)$, $r \mapsto r/1$ ist ein injektiver unitaler Ringhomomorphismus.
2. Zu jedem injektiven unitalen Ringhomomorphismus $f : R \to \mathbb{K}$ in einen Körper $\mathbb{K}$ gibt es genau einen unitalen Ringhomomorphismus $f' : Q(R) \to \mathbb{K}$ mit $f' \circ \iota = f$, nämlich $f' : Q(R) \to \mathbb{K}$, $r/s \mapsto f(r)f(s)^{-1}$. Er ist injektiv.

Dies bezeichnet man als die **charakteristische Eigenschaft** des Quotientenkörpers..



Beweis:
1. Offensichtlich ist ι injektiv, denn aus $r/1 = s/1$ folgt $(r, 1) \sim (s, 1)$, also $r = r \cdot 1 = s \cdot 1 = s$. Sie ist ein unitaler Ringhomomorphismus, denn

$$\iota(r) + \iota(s) = \frac{r}{1} + \frac{s}{1} = \frac{r + s}{1} = \iota(r + s), \qquad \iota(r) \cdot \iota(s) = \frac{r}{1} \cdot \frac{s}{1} = \frac{rs}{1} = \iota(rs), \qquad \iota(1) = \frac{1}{1} = 1.$$

2. Sei $f : R \to \mathbb{K}$ ein injektiver unitaler Ringhomomorphismus. Ist $f' : Q(R) \to \mathbb{K}$ ein unitaler Ringhomomorphismus mit $f' \circ \iota = f$, so folgt für alle $r \in R$ und $0 \neq s \in R$

$$f'\left(\frac{r}{s}\right) = f'\left(\frac{r}{1} \cdot \frac{1}{s}\right) = f'\left(\frac{r}{1} \cdot \left(\frac{s}{1}\right)^{-1}\right) = f'\left(\frac{r}{1}\right) \cdot f'\left(\frac{s}{1}\right)^{-1} = f(r) \cdot f(s)^{-1}.$$

Damit ist f' eindeutig bestimmt. Die Abbildung $f' : Q(R) \to \mathbb{K}$, $r/s \mapsto f(r)f(s)^{-1}$ ist wohldefiniert. Denn wegen der Injektivität von f gilt $f(s) \neq 0$ für alle $s \neq 0$, und da $\mathbb{K}$ ein Körper ist, hat $f(s)$ dann ein multiplikatives Inverses $f(s)^{-1}$. Ist $(r, s) \sim (r', s')$ für $r, r', s, s' \in R$ mit $s, s' \neq 0$, so ist $rs' = r's$ und damit auch $f(r)f(s') = f(rs') = f(r's) = f(r')f(s)$. Da $f(s)$, $f(s')$ invertierbar sind, ergibt sich $f'(r/s) = f(r)f(s)^{-1} = f(r')f(s')^{-1} = f'(r'/s')$.Es gilt $f' \circ \iota(r) = f'(r/1) = f(r)$ und

$$f'\left(\frac{r}{s}+\frac{t}{u}\right)=f'\left(\frac{ru+st}{tu}\right)=f(ru+st)f(su)^{-1}=f(r)f(s)^{-1}+f(t)f(u)^{-1}=f'\left(\frac{r}{s}\right)+f'\left(\frac{t}{u}\right)$$
$$f'\left(\frac{r}{s}\cdot\frac{t}{u}\right)=f'\left(\frac{rt}{su}\right)=f(rt)f(su)^{-1}=f(r)f(t)f(u)^{-1}f(s)^{-1}=f'\left(\frac{r}{s}\right)\cdot f'\left(\frac{t}{u}\right)$$

für alle $r, t \in R$ und $0 \neq s, u \in R$. Damit ist f' ein unitaler Ringhomomorphismus. Er ist injektiv, denn aus $f(r/s) = f(r)f(s)^{-1} = f(t)f(u)^{-1} = f(t/u)$ folgt $f(r)f(u) = f(t)f(s)$, also $f(ru - ts) = 0$ und wegen der Injektivität von f dann auch $ru = st$ und $r/s = t/u$. □

Beispiel 2.4.21.

1. Der Quotientenkörper des Integritätsbereichs $\mathbb{Z}$ ist der Körper $\mathbb{Q}$ der rationale Zahlen.
2. Der Quotientenkörper eines Polynomrings $R[x]$ mit Koeffizienten in einem Integritätsbereich R heißt Körper der **gebrochen rationalen Funktionen** über R.
3. Der Quotientenkörper des Rings $\mathbb{Z}$[i] der Gaußschen Zahlen ist isomorph zum Körper $\mathbb{Q}(i) = \{a + \mathrm{i}b \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ (Übung).
4. Für jeden Körper $\mathbb{K}$ ist $Q(\mathbb{K}) \cong \mathbb{K}$, denn in diesem Fall gilt $(r, s) \sim (rs^{-1}, 1)$ für alle $r \in \mathbb{K}$ und $0 \neq s \in \mathbb{K}$. Damit ist $\iota : \mathbb{K} \to Q(\mathbb{K})$, $r \mapsto r/1$ surjektiv, also ein Isomorphismus.

Wendet man Satz 2.4.20 auf den Integritätbereich $R = \mathbb{Z}$ und den kanonischen Ringhomomorphismus $f : \mathbb{Z} \to \mathbb{K}$ an, so erhält man die Aussage, dass der Körper $\mathbb{K}$ entweder $\mathbb{Q}$ oder einen Körper $\mathbb{Z}/p\mathbb{Z}$ als unitalen Unterring enthält. Diese Körper spielen also eine besondere Rolle und können als die kleinsten Körper oder Grundbausteine aller Körper aufgefasst werden.

Korollar 2.4.22: Sei $\mathbb{K}$ ein Körper und $f : \mathbb{Z} \to \mathbb{K}$, $n \mapsto n1_{\mathbb{K}}$ der kanonische Ringhomomorphismus aus Beispiel 2.1.16. Dann gilt:

- Ist $\ker(f) = \{0\}$, so setzt sich f zu einer kanonischen Einbettung $f' : \mathbb{Q} \to \mathbb{K}$ fort.
- Ist $\ker(f) = p\mathbb{Z}$ mit $p \in \mathbb{N}$ prim, so induziert f eine kanonische Einbettung $f' : \mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$.

Der Körper $f(\mathbb{Z})$ heißt **Primkörper** von $\mathbb{K}$. Er ist der kleinste Körper, der in $\mathbb{K}$ enthalten ist.

Beweis:
Ist $\ker(f) = 0$, so induziert f nach Satz 2.4.20 einen injektiven unitalen Ringhomomorphismus $f' : \mathbb{Q} \to \mathbb{K}$ mit $\mathrm{im}(f') \cong \mathbb{Q}$. Ansonsten ist $\ker(f) = p\mathbb{Z}$ mit $p = \mathrm{char}(\mathbb{K})$ prim nach Beispiel 2.1.16 und Beispiel 2.1.17, 4. Nach dem Homomorphiesatz 2.3.11 induziert f dann einen injektiven unitalen Ringhomomorphismus $f' = f/\ker(f) : \mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$ mit $\mathrm{im}(f') \cong \mathbb{Z}/p\mathbb{Z}$. Ist $U \subseteq \mathbb{K}$ ein unitaler Unterring von $\mathbb{K}$, der ein Körper ist, so gilt $1 = f(1) \in U$ und damit $f(\mathbb{Z}) \subseteq U$. Ist $\ker(f) = \{0\}$, so folgt $f'(\mathbb{Q}) \subseteq U$, da U als Körper abgeschlossen unter der Inversenbildung ist. Ansonsten gilt $f'(\mathbb{Z}/p\mathbb{Z}) = f(\mathbb{Z}) \subseteq U$. □

2.5 Teilbarkeit in Integritätsbereichen

In Beispielen 2.1.4, 2.3.13 und 2.3.14 wurden, respektive, der Ring $\mathbb{Z}/n\mathbb{Z}$ als Quotient des Integritätsbereichs $\mathbb{Z}$, der Körper $\mathbb{C}$ der komplexen Zahlen als Quotient des Integritätsbereichs $\mathbb{R}[x]$ und der Integritätsbereich $\mathbb{Z}[\mathrm{i}]$ der Gaußschen Zahlen als Quotient des Integritätsbereichs $\mathbb{Z}[x]$ konstruiert. Dies zeigt, dass sich mit Hilfe von Idealen in Integritätsbereichen interessante Ringe oder sogar Körper konstruieren lassen. Die am einfachsten zu handhabenden Ideale sind dabei Hauptideale, also Ideale, die von einem einzigen Element erzeugt werden. Die Eigenschaften dieses Elements entscheiden dann darüber, welche Eigenschaften der zugehörige Faktorring hat. So ist nach Korollar 2.4.4 der Faktorring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist. Ebenso garantiert die Tatsache, dass sich das Polynom x^2+1 nicht in zwei reelle lineare Polynome faktorisieren lässt, dass der Quotient $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$ ein Körper und der Quotient $\mathbb{Z}[\mathrm{i}] = \mathbb{Z}[x]/(x^2+1)$ ein Integritätsbereich ist. Um dies systematisch zu verstehen, befassen wir uns nun mit Teilbarkeit in Integritätsbereichen.

Definition 2.5.1: Sei R ein Integritätsbereich und $r, s \in R$.

1. Das Element r heißt **Teiler** von s und s heißt **Vielfaches** von r, wenn es ein Element $t \in R$ mit $s = t \cdot r$ gibt. Man schreibt dann $r|s$.
2. Die Elemente r, s heißen zueinander **assoziiert**, wenn $r|s$ und $s|r$. Man schreibt $r \sim s$.

Bemerkung 2.5.2. Sei R ein Integritätsbereich.

1. Es gilt $1|r$, $r|0$ und $r|r$ für alle $r \in R$.
2. Es gilt $r|s \Leftrightarrow s \in (r) \Leftrightarrow (s) \subseteq (r)$.
3. *Zueinander assoziiert sein* ist eine Äquivalenzrelation auf R, und es gilt:
   $r \sim s \Leftrightarrow (r) = (s) \Leftrightarrow \exists u \in R^\times : s = ur$.

   Die erste Äquivalenz folgt aus 2. Ist $s = ur$ mit $u \in R^\times$, so folgt $r = u^{-1}s$, also $r|s$ und $s|r$. Ist $r \sim s$, so gibt es $u, v \in R$ mit $s = ur$ und $r = vs$. Daraus folgt $s = uvs$, und da R nullteilerfrei ist, $s = 0$ oder $uv = 1$. Ersteres impliziert $r = s = 0$ und letzteres $u, v \in R^\times$.
4. Ist $u \in R^\times$ eine Einheit, so gilt $u|s$ und $us|s$ für alle $s \in R$. Denn $s = u \cdot (u^{-1}s) = (us) \cdot u^{-1}$. Die Teiler us und u mit $u \in R^\times$ bezeichnet man als **triviale Teiler** von s. Die übrigen Teiler heißen **nichttriviale Teiler**.

Die Multiplikation mit Einheiten in einem Ring R ändert also offensichtlich nichts daran, ob ein Element ein anderes Element teilt oder von ihm geteilt wird. Teilbarkeitsaussagen sind daher immer nur eindeutig bis auf Multiplikation mit Einheiten. Im Ring $\mathbb{Z}$ gestaltet sich das besonders einfach, da es dort nur sehr wenige Einheiten gibt, nämlich 1 und -1. Dort kann man Eindeutigkeit erzielen, indem man Positivität fordert. Dies ist jedoch für allgemeinere Integritätsbereiche nicht möglich.

Ähnlich wie im Ring $\mathbb{Z}$ kann man auch in Integritätsbereichen ein Konzept von größten gemeinsamen Teilern und kleinsten gemeinsamen Vielfachen formulieren. Diese sind jedoch nur bis auf Einheiten bestimmt und sollten daher als *Teilmengen* des Integritätsbereichs, *nicht als Elemente* des Integritätsbereichs aufgefasst werden.

Definition 2.5.3: Sei R ein Integritätsbereich und $X \subseteq R$ eine Teilmenge.

1. Ein Element $s \in R$ heißt **größter gemeinsamer Teiler** von X, wenn

$$r|x \text{ für alle } x \in X \;\Leftrightarrow\; r|s$$

   Die Menge der größten gemeinsamen Teiler von X wird mit $\mathrm{ggT}(X)$ bezeichnet oder mit $\mathrm{ggT}(x_1, .., x_n)$ für $X = \{x_1, ..., x_n\}$.

2. Ein Element $s \in R$ heißt **kleinstes gemeinsames Vielfaches** von X, wenn

$$x|r \text{ für alle } x \in X \;\Leftrightarrow\; s|r$$

   Die Menge der kleinsten gemeinsamen Vielfachen von X mit $\mathrm{kgV}(X)$ bezeichnet oder mit $\mathrm{kgV}(x_1, .., x_n)$ für $X = \{x_1, ..., x_n\}$.

3. Die Menge X heißt **teilerfremd**, wenn $1 \in \mathrm{ggT}(X)$, und **paarweise teilerfremd**, wenn $1 \in \mathrm{ggT}(x, y)$ für alle $x \neq y \in X$.

Bemerkung 2.5.4.

1. Größte gemeinsame Teiler und kleinste gemeinsame Vielfache sind eindeutig bis auf Multiplikation mit Einheiten: Es gilt $rR^\times = \mathrm{ggT}(X)$ und $sR^\times = \mathrm{kgV}(X)$ für alle $r \in \mathrm{ggT}(X)$ und $s \in \mathrm{kgV}(X)$.

2. Es gilt $\mathrm{ggT}(\emptyset) = \{0\}$ und $\mathrm{kgV}(\emptyset) = R^\times$, denn für $X = \emptyset$ sind die Bedingungen $r|x$ für alle $x \in X$ und $x|r$ für alle $x \in X$ leer. Damit müssen größte gemeinsame Teiler Vielfache von allen Elementen in R sein, kleinste gemeinsame Vielfache alle Elemente von R teilen.

3. Ist $0 \in X$, so folgt $\mathrm{ggT}(X) = \mathrm{ggT}(X \setminus \{0\})$ und $\mathrm{kgV}(X) = \{0\}$. Ist $r \in X$ eine Einheit, so folgt $\mathrm{ggT}(X) = R^\times$ und $\mathrm{kgV}(X) = \mathrm{kgV}(X \setminus \{r\})$.

4. Es gilt $s \in \mathrm{kgV}(X)$ genau dann, wenn $(s) = \bigcap_{r \in X}(r)$.

5. Jede paarweise teilerfremde Teilmenge $X \subseteq R$ ist auch teilerfremd, aber die Umkehrung gilt nicht. Beispielsweise ist $\{2, 3, 4\} \subseteq \mathbb{Z}$ teilerfremd, aber nicht paarweise teilerfremd.

Die Existenz von größten gemeinsamen Teilern und kleinsten gemeinsamen Vielfachen ist durch Definition 2.5.3 nicht gesichert. Definition 2.5.3 liefert auch kein Verfahren, um die größten gemeinsamen Teiler oder kleinsten gemeinsamen Vielfachen zu bestimmen. Im Ring $\mathbb{Z}$ benutzt man dafür die Primfaktorzerlegung. Möchte man dieses Verfahren verallgemeinern, so muss man sich zunächst über die Definition von Primzahlen Gedanken machen. In $\mathbb{Z}$ kann man eine Primzahl entweder als eine (von Null verschiedene) Zahl definieren, die nur triviale Teiler hat, oder als eine Zahl, die ein Produkt teilt genau dann, wenn sie einen der Faktoren teilt. In einem allgemeinen Integritätsbereich müssen diese zwei Forderungen aber nicht übereinstimmen.

Definition 2.5.5: Sei R ein Integritätsbereich. Ein Element $r \in R \setminus (R^\times \cup \{0\})$ heißt

1. **unzerlegbar** oder **irreduzibel**, falls r nur triviale Teiler hat.
2. **Primelement**, wenn aus $r|ab$ folgt $r|a$ oder $r|b$.

Beispiel 2.5.6.

1. In einem Körper $\mathbb{K}$ gibt es weder Prim- noch irreduzible Elemente, denn $\mathbb{K} = \{0\} \cup \mathbb{K}^\times$.
2. Die Primelemente in $\mathbb{Z}$ und die irreduziblen Elemente in $\mathbb{Z}$ stimmen überein. Es sind genau die Elemente $\pm p$ mit $p \in \mathbb{N}$ prim.
3. Im Integritätsbereich $\mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ist das Element $3 \in \mathbb{Z}[i\sqrt{5}]$ irreduzibel, aber kein Primelement.

   Denn aus $3 = r_1 \cdot r_2$ mit $r_j = a_j + i\sqrt{5}b_j$ folgt $9 = |3|^2 = |r_1|^2|r_2|^2 = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2)$, und das impliziert $b_1 = b_2 = 0$ und $r_1, r_2 \in \{\pm 1, \pm 3\}$. Die Elemente $\pm 1 \in \mathbb{Z}[i\sqrt{5}]$ sind offensichtlich Einheiten. Damit hat 3 keine nichttrivialen Teiler und ist irreduzibel. Es gilt aber $3|9 = 4 + 5 = (2 + i\sqrt{5})(2 - i\sqrt{5})$, aber $3 \nmid (2 + i\sqrt{5}), (2 - i\sqrt{5})$, und damit ist 3 kein Primelement in $\mathbb{Z}[i\sqrt{5}]$.

Lemma 2.5.7: In jedem Integritätsbereich R gilt:

1. Primelemente sind irreduzibel.
2. Ist $p \in R$ ein Primelement oder irreduzibel, so sind auch alle zu p assoziierten Elemente Primelemente oder irreduzibel.

Beweis:
1. Ist $p \in R$ ein Primelement und $p = rs$, so gilt $r, s|p$, und aus $p|p = rs$ folgt $p|r$ oder $p|s$. Damit folgt $p \sim r$ oder $p \sim s$. Ist $p \sim r$, so gibt es nach Bemerkung 2.5.2, 4. eine Einheit $u \in R^\times$ mit $r = up$, und es folgt $s = u^{-1} \in R^\times$. Damit sind r, s triviale Teiler von p. Für $p \sim s$ argumentiert man analog.

2. Ist $r \sim p$, so gilt $(r) = (p)$ nach Bemerkung 2.5.2, 4. und damit $p|s \Leftrightarrow r|s$ und $s|p \Leftrightarrow s|r$ für alle $s \in R$ nach Bemerkung 2.5.2, 2. Damit ist p prim genau dann, wenn r prim ist, und p irreduzibel genau dann, wenn r irreduzibel. □

Die Idee ist es nun, Elemente in einem Integritätsbereich in Primelemente und Einheiten zu zerlegen, sie also als Produkt von Primelementen und Einheiten zu schreiben. Dabei stellt sich die Frage nach der Existenz und der Eindeutigkeit einer solchen Zerlegung. Die Eindeutigkeit der Zerlegung folgt induktiv aus der Definition eines Primelements und der Tatsache, dass Primelemente irreduzibel sind.

Lemma 2.5.8: Sei R ein Integritätsbereich, $u, v \in R^\times$ Einheiten und $p_1, ..., p_m, q_1, ..., q_n \in R$ Primelemente mit $m, n \geq 0$ und $up_1 \cdots p_m = vq_1 \cdots q_n$. Dann ist $m = n$ und es gibt eine Permutation $\sigma \in S_n$ mit $p_i \sim q_{\sigma(i)}$ für $i = 1, \ldots, n$.

Beweis:
Ohne Beschränkung der Allgemeinheit können wir $m \leq n$ annehmen und den Beweis durch Induktion nach m führen. Für $m = 0$ ist $vq_1 \cdots q_n = u$. Daraus folgt $R = (uv^{-1}) = (q_1 \cdots q_n) \subseteq (q_i)$ und damit $q_i \in R^\times$ für alle $i \in \{1, .., n\}$. Also muss $n = 0$ gelten.

Sei nun $m > 0$. Da p_m prim ist und $p_m|up_1 \cdots p_m = vq_1 \cdots q_n$, gibt es ein $j \in \{1, \ldots, n\}$ mit $p_m|q_j$. Durch Umordnen der q_i können wir $j = n$ erreichen. Da q_n auch prim und damit irreduzibel ist, gilt $q_n = wp_m$ mit $w \in R^\times$. Daraus folgt $p_m(up_1 \ldots p_{m-1} - (vw)q_1 \ldots q_{n-1}) = 0$, und da R nullteilerfrei ist und $p_m \neq 0$ auch $up_1 \ldots p_{m-1} = (vw)q_1 \ldots q_{n-1}$. Mit der Induktionsannahme folgt die Behauptung. □

2.5.1 Faktorielle Ringe

Lemma 2.5.8 sichert zwar die Eindeutigkeit einer Zerlegung in Primfaktoren, aber nicht deren Existenz. Schon am Ring $\mathbb{Z}[i\sqrt{5}]$ aus Beispiel 2.5.6, 3. zeigt sich, dass diese im Allgemeinen nicht gesichert ist. Nach Beispiel 2.5.6, 3. sind nämlich ± 1 und ± 3 die einzigen Teiler von 3. Die Elemente ± 1 sind als Einheiten keine Primelemente. Das Element 3 ist keine Einheit, aber nach Beispiel 2.5.6 auch kein Primelement. Damit ist $3 \in \mathbb{Z}[i\sqrt{5}]$ kein Produkt von Primelementen, und man erkennt, dass im Ring $\mathbb{Z}[i\sqrt{5}]$ keine Primfaktorzerlegung existiert. Wir müssen die Existenz von Primfaktorzerlegungen also separat fordern.

Definition 2.5.9: Ein Integritätsbereich R heißt **faktorieller Ring**, wenn sich jedes Element $r \in R \setminus (R^\times \cup \{0\})$ als endliches Produkt von Primelementen schreiben lässt.

Beispiel 2.5.10.

1. Jeder Körper $\mathbb{K}$ ist trivialerweise faktoriell, denn $\mathbb{K} = \{0\} \cup \mathbb{K}^\times$.
2. Der Ring $\mathbb{Z}$ ist faktoriell.
3. Wir werden zeigen, dass für jeden faktoriellen Ring R auch der Polynomring $R[x]$ faktoriell ist (vgl. Satz 2.6.7). Insbesondere gilt dies für den Polynomring $\mathbb{Z}[x]$ und für Polynomringe $\mathbb{K}[x]$ über Körpern $\mathbb{K}$.
4. Wir werden zeigen, dass der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen faktoriell ist (Satz 3.3.2).
5. Der Ring $\mathbb{Z}[i\sqrt{5}]$ ist nicht faktoriell.
6. Unitale Unterringe von $\mathbb{C}$ der Form $\mathbb{Z}[c] = \mathbb{Z} + c\mathbb{Z}$ für $c \in \mathbb{C}$ wurden erstmals von Gauß untersucht. Insbesondere betrachtete er Ringe der Form

$$R_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \bmod 4 \end{cases} \qquad \sqrt{d} := i\sqrt{-d} \text{ für } d < 0$$

   für **quadratfreie** Zahlen $d \in \mathbb{Z}$, also Zahlen $d \in \mathbb{Z}$, die durch keine Quadratzahl $\neq 1$ teilbar sind. Gauß vermutete, dass der Ring R_d für $d < 0$ faktoriell ist genau dann, wenn $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. Dies wurde erst 1966 bewiesen.

   Ebenso ist bekannt, dass R_d für 38 quadratfreie Zahlen d zwischen 2 und 100 faktoriell ist. Gauß vermutete, dass es unendlich viele quadratfreie Zahlen $d \in \mathbb{N}$ gibt, für die R_d faktoriell ist, aber diese Vermutung ist bis heute nicht bewiesen.

Ist die Existenz einer Primfaktorzerlegung in einem Ring R gesichert, so folgt aus 2.5.8 ihre Eindeutigkeit, aber nur bis auf Multiplikation der Primelemente mit Einheiten. Um diese Uneindeutigkeit zu vermeiden, kann man ein Repräsentantensystem der Primelemente in R betrachten, also eine Menge P von Primelementen, so dass jedes Primelement zu genau einem Primelement aus P assoziiert ist. Für den Ring $\mathbb{Z}$ kann man beispielsweise die Menge der positiven Primelemente wählen.

Damit wird die Primfaktorzerlegung in einem faktoriellen Ring eindeutig. Indem man den Zähler und Nenner eines Bruchs in Primelemente faktorisiert und diejenigen Primelemente kürzt, die in beiden auftreten, erhält man auch direkt eine analoge Zerlegung für Elemente des zugehörigen Quotientenkörpers. Der einzige Unterschied ist, dass hier auch negative Potenzen von Primelementen auftreten können.

Satz 2.5.11: Sei R ein faktorieller Ring und P ein Repräsentantensystem der Primelemente.

1. Zu jedem Element $0 \neq r \in R$ gibt es eine eindeutig bestimmte Einheit $\varepsilon(r) \in R^\times$ und eindeutig bestimmte $v_p(r) \in \mathbb{N}_0$ mit $v_p(r) = 0$ für fast alle $p \in P$, so dass

$$r = \varepsilon(r) \prod_{p \in P} p^{v_p(r)}. \tag{2.3}$$

2. Zu jedem Element $0 \neq r \in Q(R)$ gibt es eine eindeutige Einheit $\varepsilon(r) \in R^\times$ und eindeutige $v_p(r) \in \mathbb{Z}$ mit $v_p(r) = 0$ für fast alle $p \in P$, so dass r durch (2.3) gegeben ist.

3. Für $0 \neq r \in Q(R)$ gilt $r \in R$ genau dann, wenn $v_p(r) \in \mathbb{N}_0$ für alle $p \in P$. Für $0 \neq r, s \in R$ gilt $r|s$ genau dann, wenn $v_p(r) \leq v_p(s)$ für alle $p \in P$.

Beweis:
1. Dies folgt direkt aus der Definition eines faktoriellen Ringes sowie aus Lemma 2.5.8.

2. Für $0 \neq r \in Q(R)$ ist $r = s/u$ mit $0 \neq s, u \in R$. Aus der Zerlegung (2.3) für u, s folgt

$$\frac{s}{u} = \varepsilon(s)\varepsilon(u)^{-1} \prod_{p \in P} p^{v_p(s) - v_p(u)}$$

Ist $r = s/u = s'/u'$, so folgt $us' = su'$. Aus der Eindeutigkeit von (2.3) für u, u', s, s' folgt $v_p(u) + v_p(s') = v_p(s) + v_p(u')$, $\varepsilon(u)\varepsilon(s') = \varepsilon(u')\varepsilon(s)$, also auch $v_p(s) - v_p(u) = v_p(s') - v_p(u')$, $\varepsilon(s)\varepsilon(u)^{-1} = \varepsilon(s')\varepsilon(u')^{-1}$. Damit ist die Zerlegung (2.3) auch eindeutig für nichttriviale Elemente aus $Q(R)$.

3. Offensichtlich ist auch $0 \neq r \in R$ genau dann, wenn $v_p(r) \in \mathbb{N}_0$ für alle $p \in P$ gilt. Für $0 \neq r, s \in R$ gilt $r|s$ genau dann, wenn $s/r \in R$, also genau dann, wenn $v_p(s) - v_p(r) \geq 0$. □

Ein wichtige Konsequenz aus der Primfaktorzerlegung in einem faktoriellen Ring ist, dass Primelemente und irreduzible Elemente übereinstimmen. Dies ist auch in Anwendungen nützlich, da sich Irreduzibilität meist leichter überprüfen lässt als die Bedingung, ein Primelement zu sein.

Korollar 2.5.12: Sei R ein faktorieller Ring und $0 \neq r \in R$. Dann ist r genau dann prim, wenn r irreduzibel ist.

Beweis:
Nach Lemma 2.5.7 sind Primelemente in einem Integritätsbereich irreduzibel. Ist R faktoriell und $0 \neq r \in R$ irreduzibel, so enthält die Primfaktorzerlegung (2.3) von r genau ein Primelement, und damit ist auch r ein Primelement. □

Aus der Primfaktorzerlegung in einem faktoriellen Ring ergibt sich nun ähnlich wie im Ring $\mathbb{Z}$ die Existenz von größten gemeinsamen Teilern und kleinsten gemeinsamen Vielfachen und ihre Eindeutigkeit bis auf Multiplikation mit Einheiten. Ebenso erhält man direkt, dass sich jedes Element des zugehörigen Quotientenkörpers als gekürzter Bruch darstellen lässt. Auch die Produktformel für größte gemeinsame Teiler und kleinste gemeinsame Vielfache sowie die Charakterisierung für paarweise teilerfremden Teilmengen verallgemeinern sich.

Satz 2.5.13: Sei R ein faktorieller Ring, $X \subseteq R$ und $P \subseteq R$ ein Repräsentantensystem der Primelemente in R. Dann gilt:

1. Es ist $\mathrm{ggT}(\emptyset) = \mathrm{ggT}(\{0\}) = \{0\}$ und ansonsten
$$\mathrm{ggT}(X) = (\Pi_{p\in P}\, p^{m_p})R^\times \qquad \text{mit} \quad m_p := \min\{v_p(x) \mid x \in X\}.$$
2. Es ist $\mathrm{kgV}(\emptyset) = R^\times$, $\mathrm{kgV}(X) = \{0\}$, falls $|\{v_p(x) \mid x \in X\}| = \infty$ für ein $p \in P$ und sonst
$$\mathrm{kgV}(X) = (\Pi_{p\in P}\, p^{M_p})R^\times \qquad \text{mit} \quad M_p := \max\{v_p(x) \mid x \in X\}.$$
3. Jedes Element $r \in Q(R)$ lässt sich als **gekürzter Bruch** $r = s/t$ mit teilerfremden $s, t \in R$ schreiben. Dabei sind s und t eindeutig bis auf Multiplikation mit Einheiten.

Beweis:
1. Ist $X = \emptyset$ oder $X = \{0\}$, so folgt $\mathrm{ggT}(X) = \{0\}$ nach Bemerkung 2.5.4, 2. und 3. Ansonsten gilt $\mathrm{ggT}(X) = \mathrm{ggT}(X \setminus \{0\})$ und jedes Element $r \in X \setminus \{0\}$ hat eine Primfaktorzerlegung (2.3). Da nach Satz 2.5.11 $r|s$ für $r, s \neq 0$ genau dann, wenn $v_p(r) \leq v_p(s)$, gilt $r|x$ für alle $x \in X \setminus \{0\}$ genau dann, wenn $v_p(r) \leq \min\{v_p(x) \mid x \in X\}$.

2. Ist $X = \emptyset$, so gilt $\mathrm{kgV}(X) = R^\times$ nach nach Bemerkung 2.5.4, 2. Gibt es ein $p \in P$ mit $|\{v_p(x) \mid x \in X\}| = \infty$, so ist 0 das einzige gemeinsame Vielfache aller Elemente in X und damit $\mathrm{kgV}(X) = \{0\}$. Ansonsten gilt nach Satz 2.5.11 $x|r$ für alle $x \in X$ genau dann, wenn $v_p(r) \geq \max\{v_p(x) \mid x \in X\}$.

3. Für $0 \neq r, s \in R$ gibt es Elemente $0 \neq r', s' \in R$ mit $r = r' \cdot \mathrm{ggT}(r, s)$ und $s = s' \cdot \mathrm{ggT}(r, s)$. Per Definition des größten gemeinsamen Teilers gilt $\mathrm{ggT}(r', s') = R^\times$, und per Definition des Quotientenkörpers $Q(R)$ gilt $r/s = r'/s'$. Die Eindeutigkeit von r', s' bis auf Einheiten ergibt sich aus der Eindeutigkeit des ggT bis auf Einheiten. □

Korollar 2.5.14: Sei R ein faktorieller Ring und $x, y \in R$. Dann gilt
$$\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = (xy)R^\times.$$
Beweis:
Ist $0 \in \{x, y\}$, so ist $\mathrm{kgV}(x, y) = \{0\} = (xy)R^\times$ nach Bemerkung 2.5.4, 3. Ansonsten gilt nach Satz 2.5.13 für jedes Repräsentantensystem P der Primelemente
$$\mathrm{ggT}(x, y) = (\Pi_{p\in P}\, p^{\min\{v_p(x),v_p(y)\}})R^\times \qquad \mathrm{kgV}(x, y) = (\Pi_{p\in P}\, p^{\max\{v_p(x),v_p(y)\}})R^\times.$$
Da $\min(m, n) + \max(m, n) = m + n$ für alle $m, n \in \mathbb{Z}$, folgt
$$\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = (\Pi_{p\in P}\, p^{v_p(x)+v_p(y)})R^\times = (xy)R^\times. \qquad \square$$

Korollar 2.5.15: Sei R ein faktorieller Ring und $0 \neq r_1, ..., r_n \in R$. Dann sind äquivalent:

(i) Die Menge $\{r_1, ..., r_n\}$ ist paarweise teilerfremd.
(ii) Es gilt $\mathrm{kgV}(r_1, ..., r_n) = (r_1 \cdots r_n)R^\times$.
(iii) Es gilt $\bigcap_{i=1}^n (r_i) = (r_1 \cdots r_n)$.

Beweis:
Die Äquivalenz (ii) $\Leftrightarrow$ (iii) folgt aus Bemerkung 2.5.4, 4. Nach Satz 2.5.13, 2. ist (ii) äquivalent zu $\max\{v_p(r_1), \ldots, v_p(r_n)\} = v_p(r_1 \cdots r_n) = v_p(r_1) + \ldots + v_p(r_n)$ für alle Primelemente $p \in P$ und jedes Repräsentantensystem P der Primelemente. Wegen $v_p(r_i) \geq 0$ bedeutet dies, dass $v_p(r_i)$ für höchstens ein i ungleich 0 ist. Dies ist aber äquivalent zu (i). □

2.5.2 Hauptidealringe

Im letzten Abschnitt wurden faktorielle Ringe als die allgemeinsten Ringe eingeführt, in denen eine eindeutige Primfaktorzerlegung existiert und in denen sich damit Teilbarkeitsprobleme gut behandeln lassen. Allerdings kann der Beweis, dass ein gegebener Integritätsbereich faktoriell ist, sehr schwierig sein. Dies wird beispielsweise am Beispiel der Ringe R_d aus Beispiel 2.5.10, 6. deutlich, bei denen die Klärung dieser Frage Jahrhunderte gedauert hat oder noch aussteht. Es ist also sinnvoll, nach einfach handhabbaren Beispielen von faktoriellen Ringen zu suchen.

Dazu betrachten wir Ideale. Im Ring $\mathbb{Z}$ können wir den größten gemeinsamen Teiler einer Teilmenge $X \subseteq \mathbb{Z}$ auch definieren als die bis auf ihr Vorzeichen eindeutige ganze Zahl, die dasselbe Ideal erzeugt wie X. Eine solche Zahl existiert, da jedes Ideal in $\mathbb{Z}$ von der Form $(r) = r\mathbb{Z}$ für ein $r \in \mathbb{Z}$ ist. Wir untersuchen nun Ringe, die eine analoge Eigenschaft besitzen.

Definition 2.5.16: Ein Integritätsbereich R heißt **Hauptidealring**, wenn jedes Ideal in R ein Hauptideal ist: zu jedem Ideal $I \subseteq R$ gibt es ein $r \in R$ mit $I = (r)$.

Beispiel 2.5.17.

1. Jeder Körper $\mathbb{K}$ ist ein Hauptidealring. Denn nach Lemma 2.4.1 sind $\{0\} = (0)$ und $\mathbb{K} = (1)$ die einzigen Ideale in $\mathbb{K}$.

2. Der Ring $R = \mathbb{Z}$ ist ein Hauptidealring.

   Denn jedes Ideal $I \subseteq \mathbb{Z}$ ist eine Untergruppe und damit nach Beispiel 1.2.6 von der Form $I = n\mathbb{Z} = (n)$ für ein $n \in \mathbb{N}_0$.

3. Wir werden in Satz 2.5.31 zeigen, dass Polynomringe über Körpern Hauptidealringe sind.

4. Wir werden zeigen, dass der Ring $\mathbb{Z}[\mathrm{i}]$ der Gaußschen Zahlen aus Beispiel 2.2.3, 8. ein Hauptidealring ist (vgl. Satz 2.5.28 und Satz 3.3.2).

5. Der Ring R_d für quadratfreie Zahlen $d \in \mathbb{Z}$ aus Beispiel 2.5.10

$$R_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \bmod 4, \end{cases}$$

   ist für $d < 0$ ein Hauptidealring genau dann, wenn $-d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Für $d > 0$ gibt es viele Beispiele von Hauptidealringen R_d, aber keine komplette Liste.

6. Der Polynomring $\mathbb{Z}[x]$ ist kein Hauptidealring.

   Denn das Ideal $I = (2, x) = \{2 \cdot f + x \cdot g \mid f, g \in \mathbb{Z}[x]\} \subsetneq \mathbb{Z}[x]$ ist kein Hauptideal. Gäbe es ein Polynom $p \in \mathbb{Z}[x]$ mit $I = (p)$, so müsste p ein Teiler von 2 und von x sein, also ein konstantes Polynom, das x teilt. Daraus würde $p \in \{\pm 1\}$ und $(p) = R \supsetneq I$ folgen.

7. Der Polynomring $\mathbb{K}[x, y]$ in zwei Variablen über einem Körper $\mathbb{K}$ ist kein Hauptidealring.

   Denn das Ideal $I = (x, y) = \{x \cdot f + y \cdot g \mid f, g \in \mathbb{K}[x, y]\} \subseteq \mathbb{K}[x, y]$ ist kein Hauptideal. Gäbe es ein $p \in \mathbb{K}[x, y]$ mit $I = (p)$, so wäre p ein Teiler von x und von y und damit ein konstantes Polynom $p \neq 0$, also eine Einheit. Daraus würde $(p) = \mathbb{K}[x, y]$ folgen, aber es gilt $1 \notin I$ und damit $I \subsetneq \mathbb{K}[x, y]$.

In Hauptidealringen ist die Existenz von größten gemeinsamen Teilern immer gesichert, und diese lassen sich durch Ideale beschreiben. Denn es gibt zu jeder Teilmenge $X \subseteq R$ ein Element, das das von X erzeugte Ideal (X) erzeugt. Dieses Element ist dann ein Teiler aller Elemente aus X und ein maximaler, denn jedes echte Vielfache erzeugt ein kleineres Ideal.

Lemma 2.5.18: Sei R ein Hauptidealring. Dann gilt $\mathrm{ggT}(X) \neq \emptyset$ und $(X) = (s)$ für alle Teilmengen $X \subseteq R$ und größte gemeinsame Teiler $s \in \mathrm{ggT}(X)$.

Beweis:
Da R ein Hauptidealring ist, gibt es ein Element $s \in R$ mit $(X) = (s)$. Daraus folgt

$$r|x \text{ für alle } x \in X \Leftrightarrow X \subseteq (r) \Leftrightarrow (X) \subseteq (r) \Leftrightarrow (s) \subseteq (r) \Leftrightarrow r|s$$

und damit $s \in \mathrm{ggT}(X)$ nach Definition 2.5.3. □

Ist $X \subseteq R$ eine endliche Menge, so enthält das von X erzeugte Ideal in R genau die Linearkombinationen von Elementen aus X mit Koeffizienten in R. Gibt es ein Element, das dieses Ideal erzeugt, können wir es also als Linearkombination der Elemente aus X schreiben. Dies ist das sogenannte *Lemma von Bézout*, mit dem sich unter anderem die Einheiten in Faktorringen von Hauptidealringen explizit beschreiben lassen.

Korollar 2.5.19 (Lemma von Bézout):
Sei R ein Hauptidealring, $r_1, ..., r_n \in R$ und $s \in \mathrm{ggT}(r_1, ..., r_n)$. Dann gibt es $s_1, \ldots, s_n \in R$ mit $s_1r_1 + \cdots + s_nr_n = s$. Insbesondere sind $r_1, ..., r_n$ teilerfremd genau dann, wenn es $s_1, ..., s_n \in R$ gibt mit $s_1r_1 + \cdots + s_nr_n = 1$.

Beweis:
Da R ein Hauptidealring ist, ist $\mathrm{ggT}(r_1, ..., r_n) \neq \emptyset$ und $(r_1, ..., r_n) = (s)$ für alle $s \in \mathrm{ggT}(r_1, ..., r_n)$ nach Lemma 2.5.18. Damit ist $s \in (r_1, ..., r_n)$, und es gibt $s_1, ..., s_n \in R$ mit $s = s_1r_1 + ... + s_nr_n$. Sind $r_1, ..., r_n$ teilerfremd, so folgt $1 \in \mathrm{ggT}(r_1, ..., r_n)$, und damit gibt es $s_1, ..., s_n \in R$ mit $1 = s_1r_1 + ... + s_nr_n$. Gibt es umgekehrt $s_1, ..., s_n \in R$ mit $1 = s_1r_1 + ... + r_ns_n$, so folgt wegen $\mathrm{ggT}(r_1, ..., r_n) \mid r_i$ für alle $i \in \{1, ..., n\}$ auch $\mathrm{ggT}(r_1, ..., r_n) \mid 1$ und damit $1 \in \mathrm{ggT}(r_1, ..., r_n)$ und $r_1, ..., r_n$ teilerfremd. □

Korollar 2.5.20: Sei R ein Hauptidealring und $0 \neq d \in R$. Dann gilt:

$$(R/(d))^\times = \{r + (d) \mid r \text{ ist teilerfremd zu } d\}.$$

Beweis:
Für $a, b \in R$ sind $a + (d)$ und $b + (d)$ genau dann, zueinander invers, wenn $ab + (d) = 1 + (d)$, also genau dann, wenn $ab - 1 \in (d)$. Letzteres ist der Fall genau dann, wenn es ein $c \in R$ gibt mit $ab + cd = 1$. Das gibt es nach dem Lemma von Bézout genau dann, wenn $1 \in \mathrm{ggT}(a, d)$. □

Ebenfalls mit dem Lemma von Bézout können wir beweisen, dass Hauptidealringe immer faktoriell sind. Auch die Maximalität eines echten Ideals in R lässt sich damit durch Teilbarkeitsaussagen charakterisieren, nämlich dass das echte Ideal von einem Primelement erzeugt wird.

Satz 2.5.21: Für jeden Hauptidealring R gilt:

1. Jedes irreduzible Element in R ist ein Primelement.
2. Der Ring R ist faktoriell.

Beweis:
1. Sei $r \in R$ irreduzibel und $a, b \in R$ mit $r|ab$. Da r irreduzibel ist und $\mathrm{ggT}(a, r)$ ein Teiler von r, gilt entweder $\mathrm{ggT}(r, a) \sim r$ oder $\mathrm{ggT}(r, a) \in R^\times$. Im ersten Fall ist r ein Teiler von $\mathrm{ggT}(r, a)$ und damit von a, im zweiten gibt es nach dem Lemma von Bézout $x, y \in R$ mit $xr + ya = 1$ und r ist ein Teiler von $b = xrb + yab$.

2. Es reicht, zu zeigen, dass jedes Element $r \in R \setminus (\{0\} \cup R^\times)$ Produkt von endlich vielen irreduziblen Elementen ist. Angenommen $r \in R \setminus (\{0\} \cup R^\times)$ ist ein Element, das kein Produkt endlich vieler irreduzibler Elemente ist. Dann gibt es Elemente $x, y \in R \setminus (R^\times \cup \{0\})$ mit $xy = r$. Wären x und y endliche Produkte irreduzibler Elemente, so wäre auch r ein endliches Produkt irreduzibler Elemente. Also gibt es ein $r_1 \in \{x, y\}$, das nicht Produkt endlich vieler irreduzibler Elemente ist, und es gilt $r_1|r$ und $r_1 \not\sim r$, also $(r) \subsetneq (r_1)$. Durch Iteration dieses Arguments erhalten wir induktiv eine unendliche Folge $r_0 = r, r_1, r_2 \ldots$, so dass

$$(r_0) \subsetneq (r_1) \subsetneq \ldots.$$

eine echt aufsteigende Kette von Idealen ist. Die Vereinigung $I = \cup_{i=0}^{\infty}(r_i)$ ist dann nach dem Beweis von Satz 2.4.8 wieder ein Ideal in R und damit ein Hauptideal. Sei also $I = (s)$. Dann gibt es ein $i \in \mathbb{N}_0$ mit $s \in (r_i)$, und es folgt $(s) \subseteq (r_i) \subsetneq (r_{i+1}) \subsetneq I = (s)$ - ein Widerspruch. Also lässt sich jedes Element $r \in R \setminus (\{0\} \cup R^\times)$ als Produkt endlich vieler irreduzibler Elemente schreiben und damit nach 1. als Produkt endlich vieler Primelemente. □

Auch die Maximalität von echten Idealen in Hauptidealringen lässt sich durch Teilbarkeitsaussagen charakterisieren. Denn es gilt $(r) \subseteq (p)$ genau dann, wenn p ein Teiler von r ist, und $(r) \subsetneq (p) \subsetneq R$ genau dann, wenn p ein echter Teiler von r ist. Damit sind maximale Ideale in R genau die Ideale, die von Elementen ohne echte Teiler erzeugt werden, also die von irreduziblen und damit Primelementen erzeugten Ideale.

Satz 2.5.22: Sei R ein Hauptidealring. Dann ist $R/(r)$ genau dann ein Körper, wenn $r \in R^*$ ein Primelement ist.

Beweis:
Der Faktorring $R/(r)$ ist genau dann ein Körper, wenn (r) ein maximales Ideal in R ist. Daraus folgt insbesondere $r \notin R^\times$. Da $r = pq$ mit $p, q \in R \setminus (R^\times \cup \{0\})$ äquivalent ist zu $(r) \subsetneq (p) \subsetneq R$, folgt, dass (r) genau dann maximal ist, wenn r irreduzibel, also prim ist. □

Damit ist also der Faktorring $R/(r)$ eines Hauptidealrings R bezüglich des von einem Primelement $r \in R$ erzeugten Hauptideal (r) ein Körper. Hat r dagegen echte Teiler, so hat der Faktorring $R/(r)$ nichttriviale Nullteiler. Allgemein lässt sich ein Element $0 \neq r \in R$ als Produkt von paarweise teilerfremden Primpotenzen $r = p_1^{n_1} \cdots p_k^{n_k}$ schreiben, und es stellt sich die Frage wie der Faktorring $R/(r)$ mit den Faktorringen $R/(p_1^{n_1})$, ..., $R/(p_k^{n_k})$ zusammenhängt. Dies erinnert an die Situation bei der Klassifikation abelscher Gruppen, wo mit Hilfe des chinesischen Restsatzes jede endliche abelsche Gruppe als Produkt zyklischer Gruppen von Primpotenzordnung dargestellt werden konnte. Für teilerfremde $m, n \in \mathbb{Z}$ besagt der chinesische Restsatz 1.7.6 nämlich, dass $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. In der Tat erhält man für Hauptidealringe eine analoge Aussage, die ebenfalls unter dem Namen chinesischer Restsatz bekannt ist.

Satz 2.5.23 (**Chinesischer Restsatz**): Sei R ein Hauptidealring und seien $d_1, \ldots, d_n \in R$ paarweise teilerfremd. Dann ist die Abbildung

$$\varphi : R/(d_1 \cdots d_n) \to R/(d_1) \times \ldots \times R/(d_n) : x + (d_1 \cdots d_n) \mapsto (x + (d_1), \ldots, x + (d_n))$$

ein unitaler Ringisomorphismus.

Beweis:
Die Abbildung φ ist offensichtlich ein unitaler Ringhomomorphismus. Zu zeigen ist noch die Bijektivität. Gibt es ein $i \in \{1, ..., n\}$ mit $d_i = 0$, so folgt aus der paarweisen Teilerfremdheit, dass $d_j \in R^\times$ für $j \neq i$. Dann ist $R/(d_1 \cdots d_n) \cong R/(d_i) \cong R/(0) \cong R$, $R/(d_j) \cong R/R \cong \{0\}$ für $j \neq i$, und φ ist bijektiv. Sei nun $d_i \neq 0$ für alle $i = 1, .., n$.

Ist $x + (d_1 \cdots d_n) \in \ker \varphi$, so gilt $x \in (d_i)$ für alle $i = 1, ..., n$, also $x \in \bigcap_{i=1}^n (d_i)$. Nach Korollar 2.5.15 gilt $\bigcap_{i=1}^n (d_i) = (d_1 \cdots d_n)$, und damit $x \in (d_1 \cdots d_n)$. Also ist $x + (d_1 \cdots d_n) = 0 \in R/(d)$ und φ ist injektiv.

Seien nun nun Nebenklassen $x_1 + (d_1), \ldots, x_n + (d_n)$ mit $x_1, \ldots, x_n \in R$ gegeben. Da $d_1, ..., d_n$ paarweise teilerfremd sind, sind auch die Elemente d_i und $D_i := d_1 \cdots d_n / d_i$ teilerfremd, und nach dem Lemma von Bézout gibt es Elemente $a_i, b_i \in R$ mit $a_i D_i + b_i d_i = 1$. Dann gilt $(*)$ $d_i | D_j | a_j D_j$ für $j \neq i$, und für $x := a_1 D_1 x_1 + \cdots + a_n D_n x_n \in R$ erhält man

$$x + (d_i) = \Sigma_{j=1}^n a_j D_j x_j + (d_i) \overset{(*)}{=} a_i D_i x_i + (d_i) = (1 - b_i d_i) x_i + (d_i) = x_i + (d_i).$$

Damit ist $\varphi(x + (d_1 \cdots d_n)) = (x_1 + (d_1), ..., x_n + (d_n))$ und φ surjektiv. □

Da die Situation für Hauptidealringe stark an den Ring $\mathbb{Z}$ erinnert, schreibt man für Elemente $x, y \in R$ in einem Hauptidealring R auch $x \equiv y \bmod d$ statt $x + (d) = y + (d) \in R/(d)$ oder, dazu äquivalent, $x - y \in (d)$. Der chinesische Restsatz lässt sich dann auch als Aussage über die Lösbarkeit gewisser Gleichungen interpretieren und liefert auch eine Methode zu ihrer Lösung.

Korollar 2.5.24: Sei R ein Hauptidealring und $d_1, \ldots, d_n, x_1, \ldots, x_n \in R$, so dass $d_1, ..., d_n$ paarweise teilerfremd sind. Dann hat das System von Kongruenzen

$$\begin{aligned} x &\equiv x_1 \mod d_1 \\ &\vdots \\ x &\equiv x_n \mod d_n \end{aligned} \tag{2.4}$$

eine Lösung $x \in R$. Diese ist eindeutig modulo $d = d_1 \cdots d_n$.

Beispiel 2.5.25. Wir betrachten den Hauptidealring $R = \mathbb{Z}$ und das System von Kongruenzen

$$\begin{aligned} x &\equiv x_1 \bmod 9 \\ x &\equiv x_2 \bmod 10 \\ x &\equiv x_3 \bmod 11. \end{aligned}$$

Dann ist $d_1 = 9$, $d_2 = 10$ und $d_3 = 11$, und die Elemente $D_i = d_1 \cdots d_n / d_i$ und $a_i D_i$ sind

$$\begin{aligned} D_1 = d_2 d_3 &= 110 \equiv \ \ 2 \bmod d_1, & a_1 &= -4, & a_1 D_1 &= -440, \\ D_2 = d_1 d_3 &= 99 \ \equiv -1 \bmod d_2, & a_2 &= -1, & a_2 D_2 &= -\ \ 99, \\ D_3 = d_1 d_2 &= 90 \ \equiv \ \ 2 \bmod d_3, & a_3 &= -5, & a_3 D_3 &= -450. \end{aligned}$$

Die allgemeine Lösung lautet also

$$x = -440 x_1 - 99 x_2 - 450 x_3 + 990\mathbb{Z}.$$

2.5.3 Euklidische Ringe

Im letzten Abschnitt haben wir die Eigenschaften von Hauptidealringen untersucht, die nach Satz 2.5.21 Beispiele von faktoriellen Ringen sind. Allerdings konnten wir bis jetzt nur für Körper und den Ring $\mathbb{Z}$ beweisen, dass es sich tatsächlich um Hauptidealringe handelt. Der Beweis, dass $\mathbb{Z}$ ein Hauptidealring ist, in Beispiel 2.5.17 beruht auf Beispiel 1.2.6, das hauptsächlich von der Division mit Rest Gebrauch macht. Die entscheidende Aussage dabei ist, dass man jeder ganzen Zahl eine Zahl in $\mathbb{N}_0$ zuordnen kann, nämlich ihren Betrag, und erreichen kann, dass der Rest bei der Division einen kleineren Betrag hat, als die Zahl, durch die dividiert wird. Auf diese Weise hat man die bei der Division auftretenden Reste unter Kontrolle. Wir verallgemeinern dies zu der folgenden Definition.

Definition 2.5.26: Ein Integritätsbereich R heißt **euklidischer Ring**, wenn es eine Funktion $h : R \setminus \{0\} \to \mathbb{N}_0$, $r \mapsto h(r)$ gibt, die **Höhenfunktion** von R, so dass zu jedem Paar $a, b \in R$ mit $b \neq 0$ Elemente $m, r \in R$ existieren mit

$$a = mb + r \text{ und } r = 0 \text{ oder } h(r) < h(b).$$

Beispiel 2.5.27. Der Ring $R = \mathbb{Z}$ ist euklidisch mit Höhenfunktion $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0$, $z \mapsto |z|$.

Der Beweis, dass es sich bei $\mathbb{Z}$ um einen Hauptidealring handelt, verallgemeinert sich nun direkt auf euklidische Ringe. Dazu wählt man im zu betrachtenden Ideal ein Element minimaler Höhe, und zeigt, dass dieses das ganze Ideal erzeugt.

Satz 2.5.28: Jeder euklidische Ring ist ein Hauptidealring.

Beweis:
Sei R ein euklidischer Ring und $I \subseteq R$ ein Ideal. Ist $I = \{0\}$, so ist $I = (0)$ ein Hauptideal. Ansonsten wählt man ein $b \in I \setminus \{0\}$ mit $h(b) = \min\{h(a) \mid a \in I \setminus \{0\}\}$. Dann ist $(b) \subseteq I$. Da R euklidisch ist, gibt es zu $a \in I$ Elemente $m, r \in R$ mit $a = mb + r$ und $r = 0$ oder $h(r) < h(b)$. Da $r = a - mb \in I$ folgt aus der Minimalität von $h(b)$ dann $r = 0$, also $a \in (b)$. Damit ist $(b) = I$. □

Beispiel 2.5.29.

1. Wir werden in Satz 3.3.2 zeigen, dass der Ring $\mathbb{Z}[\mathrm{i}]$ der Gaußschen Zahlen euklidisch ist.
2. Die Ringe R_d für quadratfreie Zahlen $d \in \mathbb{Z}$ aus Beispiel 2.5.10, 6. und 2.5.17, 5.

$$R_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \bmod 4, \end{cases}$$

   sind für $d < 0$ euklidisch mit der Höhenfunktion $h : R_d \setminus \{0\} \to \mathbb{N}_0$, $a + \sqrt{d}b \mapsto a^2 - db^2$ genau dann, wenn $d \in \{-1, -2, -3, -7, -11\}$. Die Ringe R_{-19}, R_{-43}, R_{-67} und R_{-163} sind nach Beispiel 2.5.17, 5. Hauptidealringe, aber sie sind nicht euklidisch. Der Beweis dieser Aussagen ist sehr aufwändig.

Das zweite zentrale Beispiel euklidischer Ringe sind Polynomringe über Körpern. Hier übernimmt der Polynomgrad die Rolle der Höhenfunktion. Dazu muss aber bewiesen werden, dass eine Polynomdivision mit einem Rest kleineren Grades immer möglich ist. Für Division durch *normierte* Polynome gilt dies über beliebigen kommutativen Ringen mit Eins.

Satz 2.5.30 (Polynomdivision): Sei R ein kommutativer unitaler Ring, $f, g \in R[x]$ und g normiert. Dann gibt es eindeutige Polynome $h, r \in R[x]$ mit $f = hg + r$ und $\deg(r) < \deg(g)$.

Beweis:
Existenz: Induktion über $m = \deg(f)$. Ist $\deg(f) = 0$, so ist $\deg(g) > \deg(f)$ und damit $f = 0 \cdot g + f$, oder $\deg(f) = \deg(g) = 0$, also $g = 1$ und $f = f \cdot g + 0$.

Sei die Aussage bewiesen für alle $f, g \in R[x]$ mit g normiert und $\deg(f) \leq m - 1$.
Sei $f = a_m x^m + \cdots + a_0$ mit $a_m \neq 0$ und $g = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Ist $\deg(g) = n > m = \deg(f)$, so können wir $f = 0 \cdot g + f$ wählen. Ist $n \leq m$, so ist $f' = f - a_m x^{m-n} \cdot g$ ein Polynom vom Grad $\deg(f') \leq m - 1$, und nach Induktionsvoraussetzung gibt es Polynome $h, r \in R[x]$ mit $f' = hg + r$ und $\deg(r) < \deg(g)$. Daraus folgt $f = (h + a_m x^{m-n})g + r$ mit $\deg(r) < \deg(g)$.

Eindeutigkeit: Sei $f = h_1 g + r_1 = h_2 g + r_2$ mit $h_1, h_2, r_1, r_2 \in R[x]$ und $\deg r_1, \deg r_2 < \deg g$. Dann gilt $(h_1 - h_2)g = r_2 - r_1$ und damit $\deg((h_1 - h_2)g) = \deg(r_2 - r_1) < \deg g$. Da g normiert ist, folgt $h_1 - h_2 = 0$ und damit auch $r_1 - r_2 = 0$. □

Offensichtlich können wir durch Multiplikation mit geeigneten Einheiten jedes Polynom mit Koeffizienten in einem Körper $\mathbb{K}$ normieren außer dem Nullpolynom. Damit ist der Polynomgrad eine Höhenfunktion, und der Polynomring $\mathbb{K}[x]$ ein euklidischer Ring. Kombinieren wir dieses Ergebnis mit den Ergebnissen zu Primidealen und maximalen Idealen aus Satz 2.5.22, so erhalten wir die folgende, etwas umfassendere Aussage.

Satz 2.5.31: Sei R ein Integritätsbereich. Dann sind äquivalent:

(i) R ist ein Körper.
(ii) $R[x]$ ist ein euklidischer Ring mit Höhenfunktion $\deg : R[x] \setminus \{0\} \to \mathbb{N}_0$.
(iii) $R[x]$ ist ein Hauptidealring.

Beweis:
(ii)⇒(iii) gilt nach Satz 2.5.28.

(iii)⇒(i): Ist $R[x]$ ein Hauptidealring, so ist der Kern des surjektiven unitalen Ringhomomorphismus $\mathrm{ev}_0 : R[x] \to R$ ein Hauptideal in $R[x]$, also $\ker(\mathrm{ev}_0) = (p)$ für ein $p \in R[x]^*$. Nach dem Homomorphiesatz 2.3.11 gilt $R \cong R[x]/\ker(\mathrm{ev}_0) = R[x]/(p)$. Da R nullteilerfrei ist, ist $(p) \subseteq R[x]$ ein Primideal nach Satz 2.4.16, und damit ist $p \in R[x]^*$ ein Primelement. Nach Satz 2.5.22 ist damit $R = R[x]/(p)$ ein Körper.

(i)⇒(ii): Ist R ein Körper, so können wir jedes Polynom $0 \neq g \in R[x]$ durch Multiplikation mit einer Einheit normieren. Nach Satz 2.5.30 gibt es damit zu den Polynomen $f, g \in R[x]$ eindeutige Polynome $k, r \in R[x]$ mit $r = 0$ oder $\deg(r) < \deg(g)$ und $f = kg + r$. Damit ist $R[x]$ ein euklidischer Ring mit Höhenfunktion $h : R \setminus \{0\} \to \mathbb{N}_0$, $f \mapsto \deg(f)$. □

Nach Satz 2.5.22 ist der Faktorring $R/(r)$ eines Hauptidealrings ein Körper genau dann, wenn $r \in R^*$ ein Primelement ist, was wiederum nach Lemma 2.5.7 und Satz 2.5.21 dazu äquivalent ist, dass r irreduzibel ist. Im Fall eines Polynomrings über einem Körper $\mathbb{K}$ lassen sich dazu noch weitergehende Aussagen machen. In diesem Fall ist nämlich der Faktorring $\mathbb{K}[x]/(r)$ nicht nur ein kommutativer unitaler Ring, sondern auch ein Vektorraum über $\mathbb{K}$.

Korollar 2.5.32: Sei $\mathbb{K}$ ein Körper und $0 \neq f \in \mathbb{K}[x]$. Dann gilt:

1. Es ist $\mathrm{ev}_k(f) = 0$ für ein $k \in \mathbb{K}$ genau dann, wenn $x - k$ ein Teiler von f ist.
2. Das Polynom f hat höchstens $\deg(f)$ verschiedene Nullstellen in $\mathbb{K}$.
3. Der Faktorring $\mathbb{K}[x]/(f)$ ist ein $\deg(f)$-dimensionaler Vektorraum über $\mathbb{K}$. Die Elemente $1 + (f), x + (f), \ldots, x^{\deg(f)-1} + (f)$ bilden eine Basis von $\mathbb{K}[x]/(f)$.
4. Der Faktorring $\mathbb{K}[x]/(f)$ ist ein Körper genau dann, wenn f irreduzibel ist.

Beweis:
1. Da $\mathbb{K}[x]$ euklidisch ist mit Höhenfunktion $h : \mathbb{K}[x] \setminus \{0\} \to \mathbb{N}_0$, $p \mapsto \deg(p)$, gibt es zu $f \in \mathbb{K}[x]$ ein $m \in \mathbb{K}[x]$ und ein konstantes Polynom r mit $f = m(x - k) + r$. Daraus folgt $\mathrm{ev}_k(f) = \mathrm{ev}_k(m) \cdot 0 + r = r$. Damit gilt $\mathrm{ev}_k(f) = 0$ genau dann, wenn $(x - k)$ ein Teiler von f ist.

2. Hat f die verschiedenen Nullstellen $\lambda_1, ..., \lambda_m \in \mathbb{K}$, so ist $f = (x - \lambda_1) \cdots (x - \lambda_m) \cdot h$ mit $h \neq 0$ nach 1. Daraus folgt $\deg(f) = m + \deg(h) \geq m$.

3. Der Polynomring $\mathbb{K}[x]$ ist ein Vektorraum über $\mathbb{K}$, wobei die Skalarmultiplikation der Multiplikation mit konstanten Polynomen entspricht. Damit ist das Ideal $(f) \subseteq \mathbb{K}[x]$ ein Untervektorraum und $\mathbb{K}[x]/(f)$ der zugehörige Quotientenraum. Die $\mathbb{K}$-lineare Abbildung

$$\varphi : \mathrm{span}_{\mathbb{K}}\{1, x, ..., x^{\deg(f)-1}\} \to \mathbb{K}[x]/(f), \quad r \mapsto r + (f)$$

ist bijektiv nach Satz 2.5.30, also ein Vektorraumisomorphismus. Da die Monome $1, x, ..., x^{\deg(f)-1}$ linear unabhängig sind, ist $\dim_{\mathbb{K}} \mathbb{K}[x]/(f) = \deg(f)$.

4. Dies ist ein Spezialfall von Satz 2.5.22 für $R = \mathbb{K}[x]$. □

Beispiel 2.5.33.

1. Der Faktorring $\mathbb{R}[x]/(p)$ mit $p = x^2 - 1$ ist ein zweidimensionaler reeller Vektorraum mit Basis $\{\bar{1} = 1+(p), \bar{x} = x+(p)\}$. Die Ringstruktur ist durch die Produkte der Basiselemente eindeutig bestimmt. Da $\bar{1}$ das neutrale Element ist, also durch $\bar{x} \cdot \bar{x} = \bar{x}^2 = \bar{1} + \bar{x}^2 - \bar{1} = \bar{1}$. Man kann zeigen, dass dieser Ring isomorph ist zu $\mathbb{R}^2$ mit der Multiplikation

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc) \qquad a, b, c, d \in \mathbb{R}.$$

2. Der Faktorring $\mathbb{R}[x]/(q)$ mit $q = x^2$ ist ebenfalls ein zweidimensionaler reeler Vektorraum mit Basis $\{\bar{1} := 1 + (q), \bar{x} := x + (q)\}$. Die Multiplikation ist gegeben durch $\bar{x} \cdot \bar{x} = \bar{x}^2 = \bar{0}$. Dieser Ring ist isomorph zu $\mathbb{R}^2$ mit der Multiplikation

$$(a, b) \cdot (c, d) = (ac, ad + bc) \qquad a, b, c, d \in \mathbb{R}.$$

Ein entscheidender Vorteil euklidischer Ringe ist, dass sie als Hauptidealringe nicht nur größte gemeinsame Teiler aller Teilmengen besitzen, sondern dass man diese mit Hilfe der Division mit Rest auch effizient bestimmen kann. Dies leistet der sogenannte *euklidische Algorithmus*. Man kann damit nicht nur größte gemeinsame Teiler effizient berechnen, sondern auch größte gemeinsame Teiler als Linearkombinationen darstellen wie im Lemma von Bézout.

Satz 2.5.34 (erweiterter euklidischer Algorithmus):
Sei R ein euklidischer Ring mit Höhenfunktion $h : R \setminus \{0\} \to \mathbb{N}_0$ und $a, b \in R$.
Wir definieren induktiv Tripel $x_i = (a_i, b_i, q_i)$ durch $x_0 := (a, 1, 0)$, $x_1 := (b, 0, 1)$ und

$$x_{i+1} = x_{i-1} - m_i x_i, \quad \text{wobei} \quad a_{i-1} = m_i a_i + r_i \ \text{ mit } \ m_i \in R, \ h(r_i) < h(a_i),$$

bis $a_{n+1} = 0$ gilt. Dann ist $a_n = b_n \cdot a + q_n \cdot b \in \mathrm{ggT}(a, b)$.

Beweis:
Da $h(a_1) > h(a_2) > \ldots > 0$ bricht der erweiterte euklidische Algorithmus ab. Die größten gemeinsamen Teiler von a und b sind definiert durch $(k) = (a, b)$ für alle $k \in \mathrm{ggT}(a, b)$. Per Definition der Variablen $x_i = (a_i, b_i, q_i)$ gilt $(a_i, a_{i+1}) = (a_i, a_{i-1} - m_i a_i) = (a_i, a_{i-1})$ und damit $\mathrm{ggT}(a_i, a_{i-1}) = \mathrm{ggT}(a_{i+1}, a_i)$ für alle $i = 1, ..., n$. Daraus folgt $a_n \in \mathrm{ggT}(a_n, 0) = \mathrm{ggT}(a, b)$.

Wir beweisen per Induktion über i, dass $a_i = b_i a + q_i b$ für alle $i \in \{0, 1, ..., n\}$ gilt. Für $i \in \{0, 1\}$ gilt dies per Definition. Sei die Aussage nun bewiesen für alle $i \leq k$. Dann folgt aus der rekursiven Definition von $x_i = (a_i, b_i, q_i)$

$$\begin{aligned} a_{k+1} &= a_{k-1} - m_k a_k = (b_{k-1} a + q_{k-1} b) - m_k (b_k a + q_k b) \\ &= (b_{k-1} - m_k b_k) a + (q_{k-1} - m_k q_k) b = b_{k+1} a + q_{k+1} b. \end{aligned}$$

□

Bemerkung 2.5.35. Ist man nur an den größten gemeinsamen Teilern von $a, b \in R$ interessiert, so kann man die Variablen b_k, q_k im erweiterten euklidischen Algorithmus weglassen und in jedem Schritt nur a_k bestimmen. Dies wird als der **euklidische Algorithmus** bezeichnet.

Bemerkung 2.5.36. In der Schule normiert man den Rest r bei der Division durch n in $\mathbb{Z}$ meistens mit $0 \leq r < n$. Durch Zulassen von negativen Resten kann man aber offenbar auch $|r| \leq \frac{n}{2}$ erreichen. Dadurch wird der Euklidische Algorithmus oft signifikant schneller.

Beispiel 2.5.37. Wir betrachten $R = \mathbb{Z}$ und $a = 3528$ und $b = 1540$.
Mit dem erweiterten euklidischen Algorithmus erhält man:

$$\begin{aligned} x_0 &= (3528, 1, 0) \\ x_1 &= (1540, 0, 1) && 3528 = 2 \cdot 1540 + 448 \\ x_2 &= x_0 - 2x_1 = (448, 1, -2) && 1540 = 3 \cdot 448 + 196 \\ x_3 &= x_1 - 3x_2 = (196, -3, 7) && 448 = 2 \cdot 196 + 56 \\ x_4 &= x_2 - 2x_3 = (56, 7, -16) && 196 = 3 \cdot 56 + 28 \\ x_5 &= x_3 - 3x_4 = (28, -24, 55) && 56 = 2 \cdot 28 + 0 \end{aligned}$$

$$\Rightarrow 28 = -24 \cdot 3528 + 55 \cdot 1540 \in \mathrm{ggT}(3528, 1540).$$

Beispiel 2.5.38. Wir betrachten den euklidischen Ring $\mathbb{Q}[x]$ und die Polynome

$$a = x^4 - x^3 - 7x^2 + x + 6 \qquad b = x^3 - 4x^2 + x + 6.$$

Dann liefert der erweiterte euklidische Algorithmus

$$\begin{aligned} x_0 &= (a, 1, 0) \\ x_1 &= (b, 0, 1) && a = (x+3)b + 4x^2 - 8x - 12 \\ x_2 &= (4x^2 - 8x - 12, 1, -x - 3) && b = \tfrac{1}{4}(x-2)(4x^2 - 8x - 12) + 0 \end{aligned}$$

$$\Rightarrow \quad 4x^2 - 8x - 12 = a - (x+3)b \in \mathrm{ggT}(a, b).$$

Insbesondere lassen sich mit dem euklidischen Algorithmus die Inversen von Einheiten in den Faktorringen $R/(a)$ bestimmen. Denn nach Korollar 2.5.20 sind die Einheiten in $R/(a)$ gerade die Elemente $b+(a)$ für $b \in R$ mit $\mathrm{ggT}(a,b) = R^\times$. Berechnet man also mit dem euklidischen Algorithmus Elemente aus $\mathrm{ggT}(a,b)$, so liefert einem der letzte Schritt eine Einheit in R und ein Inverses von $b+(a)$ in $R/(a)$. Dies ist auch in Anwendungen von Nutzen, etwa beim Lösen von Kongruenzsystemen wie in Beispiel 2.5.25.

Korollar 2.5.39: Sei R ein euklidischer Ring, $a, b \in R$ teilerfremd und $x_n = (a_n, b_n, q_n)$ das Ergebnis aus dem letzten Schritt des erweiterten euklidischen Algorithmus für $a, b \in R$. Dann ist a_n eine Einheit in R und $a_n^{-1}q_n + (a)$ ist ein Inverses von $b+(a)$ in $R/(a)$.

Beweis:
Da a, b teilerfremd sind gilt $\mathrm{ggT}(a,b) = R^\times$. Nach Satz 2.5.34 gilt $a_n = b_n a + q_n b \in \mathrm{ggT}(a,b)$. Es folgt $a_n^{-1}q_n b = a_n^{-1}a_n - a_n^{-1}b_n a \in 1+(a)$ und damit ist $a_n^{-1}q_n+(a)$ invers zu $b+(a)$ in $R/(a)$. □

Für diese Anwendung werden offensichtlich nur die erste und letzte Komponente der Tripel im euklidischen Algorithmus gebraucht. Man kann daher die mittlere Komponente auch weglassen. Man erkennt dabei auch, ob es ein Inverses gibt, wenn dies nicht bekannt ist. Das ist nämlich genau dann der Fall, wenn die erste Komponente des letzten Tripels eine Einheit ist.

Beispiel 2.5.40. Wir berechnen das Inverse von $\overline{11}$ in $\mathbb{Z}/17\mathbb{Z}$:

$$\begin{aligned}
&x_0 = (17, 0) && \\
&x_1 = (11, 1) && 17 = 1 \cdot 11 + 6 \\
&x_2 = x_0 - 1 \cdot x_1 = (6, -1) && 11 = 1 \cdot 6 + 5 \\
&x_3 = x_1 - 1 \cdot x_2 = (5, 2) && 6 = 1 \cdot 5 + 1 \\
&x_4 = x_2 - 1 \cdot x_3 = (1, -3) && 5 = 5 \cdot 1 + 0 \\
\Rightarrow\quad & -\overline{3} \cdot \overline{11} = \overline{14} \cdot \overline{11} = \overline{1} \quad \text{in} \quad \mathbb{Z}/17\mathbb{Z}. &&
\end{aligned}$$

Beispiel 2.5.41. Wir zeigen, dass die Restklasse von x^2+x+1 im Ring $\mathbb{Q}[x]/(x^3+2x^2-x+1)$ ein Inverses besitzt und bestimmen das Inverse mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned}
&x_0 = (x^3 + 2x^2 - x + 1, 0) && \\
&x_1 = (x^2 + x + 1, 1) && x^3 + 2x^2 - x + 1 = (x+1)(x^2 + x + 1) - 3x \\
&x_2 = (-3x, -x - 1) && x^2 + x + 1 = -\tfrac{1}{3}(x+1)(-3x) + 1 \\
&x_3 = (1, -\tfrac{1}{3}x^2 - \tfrac{2}{3}x + \tfrac{2}{3}) && \\
\Rightarrow\quad & (-\tfrac{1}{3}x^2 - \tfrac{2}{3}x + \tfrac{2}{3}) \cdot (x^2 + x + 1) \equiv 1 \bmod x^3 + 2x^2 - x + 1. &&
\end{aligned}$$

Ebenso zeigt der euklidische Algorithmus, das sich an den Teilern von Polynomen in $\mathbb{L}[x]$ nichts ändert, wenn wir sie als Elemente eines Polynomrings $\mathbb{K}[x]$ betrachten, wobei $\mathbb{K}$ ein Körper ist, der den Körper $\mathbb{L}$ enthält. Dies ist beispielsweise nützlich, wenn man Teilbarkeitsaussagen über Polynomen mit reellen Koeffizienten in $\mathbb{R}[x]$ oder $\mathbb{C}[x]$ gewinnen möchte.

Korollar 2.5.42: Sei $\mathbb{K}$ ein Körper, $\mathbb{L} \subseteq \mathbb{K}$ ein Teilkörper und $f, g \in \mathbb{L}[x]$. Dann gilt

1. Das Polynom g teilt f in $\mathbb{L}[x]$ genau dann, wenn g das Polynom f in $\mathbb{K}[x]$ teilt.
2. Größte gemeinsame Teiler von f, g in $\mathbb{L}[x]$ sind größte gemeinsame Teiler von f, g in $\mathbb{K}[x]$.

Beweis:
Sei $f = hg + r$ die Division mit Rest in $\mathbb{L}[x]$. Dies ist auch eine Division mit Rest in $\mathbb{K}[x]$. Also liefert der Euklidische Algorithmus in $\mathbb{K}[x]$ dasselbe Ergebnis wie in $\mathbb{L}[x]$.

Angenommen g teilt f in $\mathbb{K}[x]$ mit $f = hg$. Dann ist $f = hg + 0$ auch eine Division mit Rest. Aus der Eindeutigkeit folgt $r = 0$, d.h. g teilt f in $\mathbb{L}[x]$. □

2.6 Irreduzibilitätskriterien

In diesem Abschnitt beschäftigen wir uns mit Irreduzibilität und Faktorisierung im Polynomring $R[x]$ für einen faktoriellen Ring R und im Polynomring $\mathbb{K}[x]$ seines Quotientenkörpers $\mathbb{K} = Q(R)$. Dies hat zwei wesentliche Motivationen.

Die erste ist, dass wir Teilbarkeit im Polynomring $R[x]$ untersuchen wollen. Insbesondere wollen wir beweisen, dass der Polynomring über einem faktoriellen Ring wieder faktoriell ist. In Satz 2.5.31 haben wir bereits gezeigt, dass Polynomringe über Körpern Hauptidealringe sind und damit auch faktorielle Ringe nach Satz 2.5.21. Damit ist es naheliegend, Teilbarkeit im Polynomring $R[x]$ zu untersuchen, indem man ihn mit dem Polynomring $Q(R)[x]$ des Quotientenkörpers $Q(R)$ vergleicht, von dem bereits bekannt ist, das er faktoriell ist.

Die zweite Motivation ist die Konstruktion von Körpern als Quotienten eines kommutativen Rings R bezüglich maximaler Ideale. Ist der zugrundeliegende Ring R ein Hauptidealring, etwa ein Polynomring über einem Körper, so ist nach Satz 2.5.21 jedes irreduzible Element ein Primelement und nach Satz 2.5.22 ist $R/(p)$ genau dann ein Körper, wenn $p \in R^*$ irreduzibel ist. Wir benötigen also einfache Kriterien für die Irreduzibilität von Polynomen über Körpern. Ein besonders wichtiger Körper ist dabei der Quotientenkörper $\mathbb{Q} = Q(\mathbb{Z})$ der ganzen Zahlen.

Auch hierfür ist es hilfreich, Teilbarkeit und Irreduzibilität von Polynomen in einem faktoriellen Ring R in den Ringen $R[x]$ und $Q(R)[x]$ zu vergleichen. Denn durch Multiplikation mit einem geeigneten Element aus R können wir jedes Polynom in $Q(R)[x]$ zu einem Polynom mit Koeffizienten aus R machen, und seine Teilbarkeit in den Ringen $R[x]$ und $Q(R)[x]$ vergleichen. Offensichtliche Unterschiede ergeben sich hierbei, wenn wir ein Polynom $f = a_0 + a_1x + ... + a_nx^n$ in $R[x]$ betrachten, dessen Koeffizienten nicht teilerfremd sind. In diesem Fall können $\mathrm{ggT}(a_0, ..., a_n) \in R$ abfaktorisieren und erhalten damit sofort, dass das Polynom f reduzibel in $R[x]$ ist. In $Q(R)[x]$ ist $\mathrm{ggT}(a_0, ..., a_n) \in R$ jedoch eine Einheit, und f damit nicht notwendigerweise reduzibel. Deswegen ist es nützlich, Polynome in $R[x]$ mit teilerfremden Koeffizienten zu betrachten.

Definition 2.6.1: Sei R ein faktorieller Ring. Ein Polynom $0 \neq f = a_0 + a_1x + ... + a_nx^n \in R[x]$ heißt **primitiv**, wenn $\mathrm{ggT}(a_0, ..., a_n) = R^\times$

Eine wichtige Eigenschaft primitiver Polynome ist, dass ihr Produkt wieder primitiv ist. Damit können wir systematisch Ringelemente aus den Koeffizienten eines Polynoms abfaktorisieren und jedes Polynom in ein primitives Polynom und ein konstantes Polynom zerlegen.

Lemma 2.6.2 (Lemma von Gauß): Sei R ein faktorieller Ring und $f, g \in R[x]$ primitiv. Dann ist auch das Produkt fg primitiv.

Beweis:
Angenommen, fg ist nicht primitiv. Dann gibt es ein Primelement $p \in R$ mit $fg \in pR[x]$. Da $p \in R$ ein Primelement ist, ist nach Satz 2.4.16 der Ring R/pR ein Integritätsbereich und nach Lemma 2.4.13 damit auch der Polynomring $(R/pR)[x]$. Nach der universellen Eigenschaft des Polynomrings aus Satz 2.1.18 induzieren die kanonische Surjektion $\pi_p : R \to R/pR$ und die kanonische Inklusion $\iota : R/pR \to (R/pR)[x]$ einen surjektiven unitalen Ringhomomorphismus $\pi : R[x] \to (R/pR)[x]$ mit $\pi|_R = \iota \circ \pi_p$ und $\pi(x) = x$, nämlich

$$\pi := \pi_p[x] : R[x] \to (R/pR)[x], \quad \Sigma_{n=0}^{\infty} a_n x^n \mapsto \Sigma_{n=0}^{\infty}(a_n + pR)x^n.$$

Da $fg \in pR[x]$, gilt $\pi(fg) = \pi(f) \cdot \pi(g) = 0$. Da f, g primitiv sind, ist aber $\pi(f), \pi(g) \neq 0$, im Widerspruch zur Nullteilerfreiheit von $(R/pR)[x]$. Also muss auch fg primitiv sein. □

Wir bringen nun für einen faktoriellen Ring R mit Quotientenkörper $Q(R)$ die Polynome in $R[x]$ und in $Q(R)[x]$ mit Hilfe primitiver Polynome in Verbindung. Dazu faktorisieren wir für Polynome in $R[x]$ den größten gemeinsame Teiler der Koeffizienten ab, um sie primitiv zu machen. Analog können wir für Polynome in $Q(R)[x]$ den größten gemeinsame Teiler der Zähler und das kleinste gemeinsame Vielfache der Nenner aller Koeffizienten abspalten. Denn nach Satz 2.5.11 hat für jedes Repräsentantensystem P der Primelemente in R jedes Element $0 \neq q \in Q(R)$ eine eindeutige Darstellung

$$q = \varepsilon(q) \prod_{p \in P} p^{v_p(q)} \qquad \text{mit} \qquad \varepsilon(q) \in R^\times,\ v_p(q) \in \mathbb{Z}.$$

Indem wir die Primpotenzen aufsammeln, die im Zähler und Nenner jedes Koeffizienten auftreten, erhalten wir den sogenannten *Inhalt* eines Polynoms. Das Lemma von Gauß garantiert, dass der Inhalt ein gutes Verhalten unter der Bildung von Produkten zeigt und damit hilfreich für die Untersuchung von Teilbarkeitsfragen ist.

Definition 2.6.3: Sei R ein faktorieller Ring, $\mathbb{K} = Q(R)$ sein Quotientenkörper und P ein Repräsentantensystem der Primelemente in R. Für ein Polynom $f = a_0 + a_1 x + \ldots + a_n x^n$ in $\mathbb{K}[x] \setminus \{0\}$ ist der **Inhalt** $c(f)$ von f definiert als

$$c(f) := \prod_{p \in P} p^{m_p(f)} \quad \text{mit } m_p(f) := \min\{v_p(a_n), \ldots, v_p(a_0)\} \in \mathbb{Z}$$

Satz 2.6.4: Sei R ein faktorieller Ring und $\mathbb{K} = Q(R)$ sein Quotientenkörper. Dann definiert der Inhalt eine Abbildung $c : \mathbb{K}[x] \setminus \{0\} \to \mathbb{K} \setminus \{0\}$, $f \mapsto c(f)$ mit den folgenden Eigenschaften:

1. Für alle $f \in \mathbb{K}[x] \setminus \{0\}$ ist $f/c(f) \in R[x]$ primitiv.
2. Für alle primitiven $f \in R[x]$ gilt $c(f) = 1$.
3. Für $f \in \mathbb{K}[x] \setminus \{0\}$ gilt $f \in R[x] \Leftrightarrow c(f) \in R$.
4. Für alle $f, g \in \mathbb{K}[x] \setminus \{0\}$ gilt $c(fg) = c(f)c(g)$.

Beweis:
1. Sei $f(x) = a_n x^n + \ldots + a_0$ mit $a_i \in \mathbb{K}$. Per Definition des Inhalts gilt dann $v_p(a_i) - v_p(c(f)) \geq 0$ und damit $a_i/c(f) \in R$ für alle $i = 0, ..., n$ nach Satz 2.5.11. Daraus folgt $f/c(f) \in R[x]$. Weiter ist $f/c(f)$ primitiv, weil $v_p(a_i) = v_p(c(f))$ für mindestens ein $i = 0, ..., n$ gilt.

2. Ist f primitiv, so ist $m_p = 0$ für alle $p \in P$ und damit $c(f) = 1$.

3. Ist $f \in R[x] \setminus \{0\}$, so $c(f) \in R$. Ist umgekehrt $c(f) \in R$, so folgt $f = c(f) \cdot f/c(f) \in R[x]$, da $f/c(f) \in R[x]$ nach 1.

4. Per Definition des Inhalts gilt (*) $c(q \cdot f) = c(q) \cdot c(f)$ für alle $q \in \mathbb{K}$ und $f \in \mathbb{K}[x]$. Sind $f, g \in \mathbb{K}[x]$, so sind $f/c(f)$ und $g/c(g)$ primitiv nach 1, und nach dem Lemma von Gauß 2.6.2 damit auch ihr Produkt. Daraus ergibt sich

$$c(fg) \overset{*}{=} c(f)c(g)c(fg/c(f)c(g)) \overset{2.}{=} c(f)c(g). \qquad \square$$

Mit Hilfe des Inhalts können wir nun die Teiler eines Polynoms $f \in R[x]$ in den Ringen $R[x]$ und $Q(R)[x]$ vergleichen und auch seine Irreduzibilität in beiden Ringen untersuchen. Es stellt sich heraus, dass Irreduzibilität in $R[x]$ bereits die Irreduzibilität in $Q(R)[x]$ impliziert.

Korollar 2.6.5: Sei R ein faktorieller Ring, sei $\mathbb{K} = Q(R)$ und sei $g \in R[x]$ primitiv.

1. Ist $gh \in R[x]$ für ein $h \in \mathbb{K}[x]$, so ist auch $h \in R[x]$.
2. Ist g ein Teiler von $f \in R[x]$ im Ring $\mathbb{K}[x]$, so ist g auch ein Teiler von f im Ring $R[x]$.

Beweis:
1. Für $h = 0$ ist die Aussage trivial. Sei also $h \neq 0$. Dann gilt $c(g) = 1$ und $c(h) = c(g)c(h) = c(gh) \in R$ nach Satz 2.6.4 und damit $h \in R[x]$.

2. Angenommen g teilt f in $\mathbb{K}[x]$. Dann gibt es ein $h \in \mathbb{K}[x]$ mit $f = gh$. Also ist $gh \in R[x]$ und damit $h \in R[x]$ nach 1. und g teilt f in $R[x]$. $\square$

Korollar 2.6.6 (Satz von Gauß): Sei R ein faktorieller Ring, $\mathbb{K} = Q(R)$ sein Quotientenkörper und sei $0 \neq f \in R[x]$. Dann ist f genau dann irreduzibel in $\mathbb{K}[x]$, wenn f in $R[x]$ nicht das Produkt von zwei Polynomen positiven Grades ist.

Beweis:
Ist f in irreduzibel in $\mathbb{K}[x]$, so ist f nicht das Produkt zweier Polynome positiven Grades in $\mathbb{K}[x]$ und damit auch nicht in $R[x]$. Ist f dagegen reduzibel in $\mathbb{K}[x]$, so gibt es Polynome $g, h \in \mathbb{K}[x]$ positiven Grades mit $f = gh$. Dann ist $f = (g/c(g)) \cdot (c(g)h)$, das Polynom $g/c(g) \in R[x]$ ist nach Satz 2.6.4 primitiv, und damit ist nach Korollar 2.6.5 auch $c(g)h \in R[x]$. $\square$

Für ein Polynom $f \in R[x]$ können nach dem Satz von Gauß also drei Fälle auftreten:
(i) das Polynom f ist irreduzibel in $R[x]$ und in $\mathbb{K}[x]$, (ii) f ist reduzibel in $R[x]$ und in $\mathbb{K}[x]$, (iii) f ist irreduzibel in $\mathbb{K}[x]$, aber zerfällt in $R[x]$ als $f = c(f) \cdot (f/c(f))$ mit $c(f) \notin R^\times$. Fall (iii) kann offensichtlich nicht auftreten, wenn das betrachtete Polynom f primitiv ist, insbesondere also nicht für normierte Polynome.

Mit diesen Ergebnissen zur Teilbarkeit und Irreduzibilität in $R[x]$ und $\mathbb{K}[x]$ können wir die erste zentrale Aussage in diesem Abschnitt beweisen, nämlich dass der Polynomring über einem

faktoriellen Ring R wieder faktoriell ist. Dazu nutzen wir aus, dass der Polynomring $\mathbb{K}[x]$ über seinem Quotientenkörper als Hauptidealring faktoriell ist und wandeln irreduzible Polynome in $\mathbb{K}[x]$ in Primelemente in $R[x]$ um, indem wir sie durch ihren Inhalt teilen.

Satz 2.6.7: Ist R ein faktorieller Ring, so ist auch $R[x]$ faktoriell.

Beweis:
1. Wir zeigen, dass jedes Element $0 \neq f \in R[x]$ ein Produkt einer Einheit und von Primelementen in $R[x]$ ist. Dazu betrachten wir f als Element des Polynomrings $\mathbb{K}[x]$ über dem Quotientenkörper $\mathbb{K} = Q(R)$. Dieser ist als Polynomring über einem Körper nach Satz 2.5.31 ein Hauptidealring und damit faktoriell nach Satz 2.5.21. Wir können also f in $\mathbb{K}[x]$ als Produkt $f = uf_1 \cdots f_n$ einer Einheit $u \in \mathbb{K}^\times$ und nicht-konstanter, in $\mathbb{K}[x]$ irreduzibler Polynome $f_1, ..., f_n \in \mathbb{K}[x]$ schreiben. Die zugehörigen Polynome $f_i' = f_i/c(f_i) \in R[x]$ sind primitiv nach Satz 2.6.4 und ebenfalls irreduzibel in $\mathbb{K}[x]$ mit $f = u'f_1' \cdots f_n'$ und $u' = uc(f_1) \cdots c(f_n) \in \mathbb{K}[x]$. Da $f \in R[x]$ und $f_1', ..., f_n' \in R[x]$ primitiv sind, folgt $c(f) = c(u') \in R$ nach Satz 2.6.4 und damit $u' \in R$. Da R faktoriell ist, ist $u' = vp_1 \cdots p_m$ ein Produkt einer Einheit $v \in R^\times$ und von Primelementen $p_1, ..., p_m \in R$. Damit haben wir f als Produkt $f = vp_1 \cdots p_m f_1' \cdots f_n'$ geschrieben mit einer Einheit $v \in R^\times = R[x]^\times$, nicht-konstanten Polynomen $f_i' \in R[x]$, die irreduzibel in $\mathbb{K}[x]$ sind, und Primelementen $p_1, ..., p_m \in R$.

2. Es reicht nun, zu zeigen, dass $f_1', ..., f_n'$ und $p_1, ..., p_m$ auch Primelemente in $R[x]$ sind.
Für jedes $p_i \in R$ ist R/p_iR nach Satz 2.4.16 ein Integritätsbereich und damit nach Lemma 2.4.13 auch der Ring $R[x]/p_iR[x] \cong (R/p_iR)[x]$. Also ist p_i nach Satz 2.4.16 prim in $R[x]$.

Da f_i' irreduzibel und damit nach Satz 2.5.21 prim in $\mathbb{K}[x]$ ist, folgt aus $f_i'|gh$ für $g, h \in R[x]$, dass f_i' in $\mathbb{K}[x]$ einen der Faktoren teilt, also etwa $f_i'|g$ in $\mathbb{K}[x]$. Damit ist f_i' nach Korollar 2.6.5 auch ein Teiler von g in $R[x]$, und es ist gezeigt, dass f_i' ein Primelement in $R[x]$ ist. □

Daraus ergibt sich induktiv, dass auch Polynomringe in mehreren Variablen über einem faktoriellen Ring R immer faktoriell sind. Denn nach Beispiel 2.1.15, 10. ist der Polynomring $R[x_1, ..., x_m]$ isomorph zum Polynomring $R[x_1, ..., x_{m-1}][x_m]$.

Korollar 2.6.8: Sei R ein faktorieller Ring. Dann ist auch der Polynomring $R[x_1, \ldots, x_n]$ faktoriell für alle $n \in \mathbb{N}$.

Nachdem der Zusammenhang zwischen Irreduzibilität in den Polynomringen $R[x]$ und $\mathbb{K}[x]$ geklärt ist, können wir ihn ausnutzen, um einfache Kriterien für die Irreduzibilität von Polynomen in $\mathbb{K}[x]$ zu entwickeln. Dazu wandeln wir ein gegebenes Polynom in $\mathbb{K}[x]$ zunächst in ein primitives Polynom in $R[x]$ um, indem wir es durch einen Inhalt dividieren. Dann untersuchen wir die Irreduzibilität des resultierenden Polynoms in $R[x]$.

Unser erstes Irreduzibilitätskriterium ist hilfreich, um die Irreduzibilität von Polynomen vom Grad 2 und 3 zu untersuchen. Denn ein reduzibles Polynom vom Grad 2 oder 3 ist aus Gradgründen immer durch ein lineares Polynom teilbar. Die Teilbarkeit durch lineare Polynome können wir untersuchen, indem wir seine Nullstellen betrachten.

Satz 2.6.9 (Rationale Nullstellen): Sei R ein faktorieller Ring, $\mathbb{K} = Q(R)$ sein Quotientenkörper und $f = a_n x^n + \cdots + a_0 \in R[x]$. Dann gilt:

1. Ist $a = r/s \in \mathbb{K}$ mit teilerfremden $r, s \in R$ ein Nullstelle von f, so gilt $s \mid a_n$ und $r \mid a_0$.

2. Ist f normiert, so liegt jede Nullstelle von f in $Q(R)$ auch in R.

Beweis:
Ist $a = r/s$ eine Nullstelle von f, so ist $g = sx - r$ ein primitiver Teiler von f in $\mathbb{K}[x]$. Nach Korollar 2.6.5 gibt es ein $h = b_{n-1}x^{n-1} + \cdots + b_0 \in R[x]$ mit $f = gh$. Es folgt $a_n = sb_{n-1}$, $a_0 = -rb_0$. □

Beispiel 2.6.10. Das Polynom $f = x^3 - \frac{1}{2}x + 1 \in \mathbb{Q}[x]$ ist irreduzibel.

Denn $f/c(f) = 2x^3 - x + 2 \in \mathbb{Z}[x]$. Nach Satz 2.6.9 wären $\pm\frac{1}{2}, \pm 1, \pm 2$ die einzig möglichen Nullstellen von $f/c(f)$ und f. Man rechnet nach, dass das keine Nullstellen sind. Wäre f reduzibel in $\mathbb{Q}[x]$, gäbe es $g, h \in \mathbb{Q}[x]$ mit $0 < \deg(g), \deg(h) \leq 2$ und $f = hg$. Damit müsste g oder h ein Linearfaktor sein, und f hätte damit eine Nullstelle in $\mathbb{Q}$.

Man beachte, dass sich die Argumentation aus diesem Beispiel nicht ohne Weiteres auf Polynome vom Grad > 3 übertragen lässt. Beispielsweise kann ein Polynom vom Grad 4 in $R[x]$ auch in zwei Faktoren vom Grad 2 zerfallen, die beide keine Nullstellen in $Q(R)$ besitzen müssen. Ein Beispiel ist das Polynom $f = x^4 + 2x^2 + 1 = (x^2+1)\cdot(x^2+1) \in \mathbb{Z}[x]$, das offensichtlich reduzibel ist, aber keine Nullstellen in $\mathbb{Q}$ besitzt.

Man kann den Satz über rationale Nullstellen auch dazu benutzen, zu zeigen, dass ein Ring nicht faktoriell ist. Dazu reicht es aus, ein Polynom $p \in R[x]$ zu finden, dass eine Nullstelle im Quotientenkörper $Q(R)$ hat, aber nicht in R.

Beispiel 2.6.11. Der Ring $R = \mathbb{Z}[\mathrm{i}\sqrt{3}]$ ist nicht faktoriell.

Denn $c = e^{2\pi\mathrm{i}/3} = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3} \in Q(R)$ ist eine Nullstelle des Polynoms $f = x^2 + x + 1 \in R[x]$ in $Q(R) = \mathbb{Q} + \mathrm{i}\sqrt{3}\mathbb{Q}$, die nicht in R liegt.

Eine weitere nützliche Methode, um die Irreduzibilität von Polynomen über dem Quotientenkörper $\mathbb{K} = Q(R)$ eines faktoriellen Rings R zu untersuchen, ist vom Quotientenkörper $\mathbb{K} = Q(R)$ zu dem Quotientenkörper $\mathbb{K}_p = Q(R/(p))$ für ein Primelement $p \in R$ überzugehen. Ist R nicht nur faktoriell, sondern sogar ein Hauptidealring, so wird das noch einfacher, da dann $R/(p)$ bereits ein Körper ist und damit $\mathbb{K}_p = Q(R/(p)) = R/(p)$. Der Vorteil dabei ist, dass es in $\mathbb{K}_p$ viel weniger Polynome gibt als in $\mathbb{K}$ und man durch Probieren der verschiedenen Möglichkeiten leicht herausbekommt, welche davon reduzibel sind.

Um Polynome in $\mathbb{K}[x]$ und $\mathbb{K}_p[x]$ zu vergleichen, nutzt man aus, dass die Inklusionsabildungen $\iota : R \to \mathbb{K}$ und $\iota_p : R/(p) \to \mathbb{K}_p$ und die kanonische Surjektion $\pi_p : R \to R/(p)$ Ringhomomorphismen sind. Nach der universellen Eigenschaft des Polynomrings aus Satz 2.1.18 induzieren sie damit Ringhomomorphismen $\iota' : R[x] \to \mathbb{K}[x]$ und $\pi'_p : R[x] \to \mathbb{K}_p[x]$.

Satz 2.6.12 (Reduktion mod p):
Sei R ein faktorieller Ring mit Quotientenkörper $\mathbb{K} = Q(R)$ und $f \in R[x]$. Gibt es ein Primelement $p \in R$, so dass

(i) der Leitkoeffizient von f nicht durch p teilbar ist,

(ii) $\pi'_p(f) \in \mathbb{K}_p[x]$ irreduzibel ist,

so ist f irreduzibel in $\mathbb{K}[x]$.

Beweis:
Angenommen f ist reduzibel in $\mathbb{K}[x]$. Nach Korollar 2.6.6 gibt es dann Polynome $g, h \in R[x]$ positiven Grades mit $f = gh$. Seien $f_p = \pi'_p(f)$, $g_p = \pi'_p(g)$ und $h_p = \pi'_p(h)$ die Bilder von f, g, h in $\mathbb{K}_p[x]$. Da π'_p ein Ringhomomorphismus ist, gilt $f_p = g_p h_p$. Da der Leitkoeffizient von f nicht durch p teilbar ist und das Produkt der Leitkoeffizienten von g und h ist, sind die Leitkoeffizienten von g und h ebenfalls nicht durch p teilbar. Daraus folgt $\deg(g_p) = \deg(g) > 0$ und $\deg(h_p) = \deg(h) > 0$, ein Widerspruch zur Irreduzibilität von f_p. □

Beispiel 2.6.13.

1. Für $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ sind die irreduziblen Polynome in $\mathbb{F}_2[x]$ vom Grad ≤ 4:

$$\begin{aligned} d = 1: &\quad x,\ x+1 \\ d = 2: &\quad x^2 + x + 1 \\ d = 3: &\quad x^3 + x + 1,\ x^3 + x^2 + 1 \\ d = 4: &\quad x^4 + x + 1,\ x^4 + x^3 + 1,\ x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

   Also ist $f = 7x^4 + 6x^3 + 4x^2 + 3x + 1 \in \mathbb{Q}[x]$ mit $\pi'_2(f) = x^4 + x + 1 \in \mathbb{F}_2[x]$ irreduzibel.

2. Das Polynom $x - 1$ ist irreduzibel in $\mathbb{R}[x]$. Das Polynom $x_1^2 + x_2^2 \in \mathbb{R}[x_1, x_2]$ ist damit irreduzibel in $\mathbb{R}[x_1, x_2]$, denn seine Reduktion mod $x_2 - 1$ ist das irreduzible Polynom $x_1^2 + 1 \in \mathbb{R}[x_1, x_2]/(x_2) \cong \mathbb{R}[x_1]$.

3. Das Kriterium greift nicht immer. Man kann zeigen, dass $f = x^4 + 3x^2 + 1 \in \mathbb{Q}[x]$ irreduzibel ist, aber f_p ist reduzibel in $\mathbb{F}_p[x]$ für jede Primzahl $p \in \mathbb{N}$.

4. Das Polynom $f = (2x+1)(x+1) = 2x^2 + 3x + 1 \in \mathbb{Z}[x]$ ist offensichtlich nicht irreduzibel in $\mathbb{Q}[x]$. Das Polynom $f_2 = \pi'_2(f) = x + 1 \in \mathbb{F}_2[x]$ ist aber irreduzibel. Die Voraussetzung, dass der Leitkoeffizient nicht durch p teilbar ist, ist also notwendig.

In Satz 2.6.12 garantiert die Voraussetzung, dass p den Leitkoeffizienten des Polynoms $f \in R[x]$ nicht teilt, dass jede Faktorisierung $f = gh$ in zwei Polynome g, h positiven Grades auch eine Faktorisierung seines Bilds $f_p \in \mathbb{K}_p[x]$ definiert. Denn sie garantiert, dass die Leitkoeffizienten von g_p und h_p nicht verschwinden. Eine noch stärkere Aussage erhält man, wenn man zusätzlich fordert, dass p alle anderen Koeffizienten von f teilt. In diesem Fall ist nämlich $f_p \in \mathbb{K}_p[x]$ ein Monom, dessen Teiler leicht zu untersuchen sind. Setzt man zusätzlich voraus, dass p^2 den konstanten Term von f nicht teilt, so kann man direkt die Irreduzibilität von f folgern.

Satz 2.6.14 (Eisensteinkriterium):
Sei R ein faktorieller Ring mit Quotientenkörper $\mathbb{K}$ und $f = a_n x^n + \cdots + a_0 \in R[x]$. Gibt es ein Primelement $p \in R$ mit $p \nmid a_n$, mit $p \mid a_{n-1}, ..., a_0$ und mit $p^2 \nmid a_0$, so ist f irreduzibel in $\mathbb{K}[x]$. Sind die Bedingungen erfüllt, so nennt man f **eisensteinsch** oder ein **Eisensteinpolynom**.

Beweis:
Ist f reduzibel in $\mathbb{K}[x]$, so gibt es nach Korollar 2.6.6 Polynome $g, h \in R[x]$ positiven Grades mit $f = gh$. Seien f_p, g_p, h_p die Bilder von f, g, h in $\mathbb{K}_p[x]$. Dann gilt $f_p = g_p h_p$. Wegen $p \nmid a_n$ gilt $\deg(f_p) = \deg(f) = n > 0$, $\deg(g_p) = \deg(g) > 0$ und $\deg(h_p) = \deg(h) > 0$. Wegen $p \mid a_0, ..., a_{n-1}$ ist damit $f_p(x) = \alpha x^n$, mit $\alpha = \pi_p(a_n) \neq 0$. Alle Teiler von f_p sind damit von der Form βx^k mit $0 \neq \beta \in \mathbb{K}_p$ und $0 \leq k \leq n$. Also verschwinden die konstanten Terme von g_p und h_p, und p teilt die konstanten Terme von g und h. Daraus folgt aber $p^2 \mid a_0$. □

Beispiel 2.6.15.

1. Die Polynome $f = 3x^7 - 8x + 6 \in \mathbb{Z}[x]$ und $g = x^5 - 2x^4 + 4x + 2 \in \mathbb{Z}[x]$ sind eisensteinsch mit $p = 2$ und damit irreduzibel in $\mathbb{Q}[x]$.

2. Das Polynom $x - 1 \in \mathbb{C}[x]$ ist ein Primelement, da $\mathbb{C}[x]/(x-1) \cong \mathbb{C}$ ein Körper ist. Das Polynom $x_1^2 + x_2^2 - 1 = x_1^2 + (x_2+1)(x_2-1) \in \mathbb{C}[x_1, x_2] \cong \mathbb{C}[x_2][x_1]$ ist (x_2-1)-eisensteinsch und damit irreduzibel.

3. Für eine Primzahl $p \in \mathbb{N}$ betrachten wir das Polynom $\Phi_p = x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x]$, das nicht eisensteinsch ist. Wir bezeichnen mit Φ_p' das Polynom, das entsteht, indem wir die Variable x in f durch $x + 1$ ersetzen. Wäre $\Phi_p = gh$ reduzibel, so wäre auch $\Phi_p' = g'h'$ reduzibel, und damit reicht es, die Irreduzibilität von Φ_p' nachzuweisen. Da $x^p - 1 = (x-1)\Phi_p$ ergibt sich

$$\Phi_p' = \frac{1}{x}\left((x+1)^p - 1\right) = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}.$$

Damit ist Φ_p' ein p-Eisensteinpolynom, und damit irreduzibel. Die Voraussetzung, dass p eine Primzahl ist, ist für die Irreduzibilität von Φ_p notwendig. Es handelt sich nämlich um ein sogenanntes **Kreisteilungspolynom**. In der Vorlesung *Körpertheorie* wird gezeigt, dass Φ_p genau dann irreduzibel ist, wenn p eine Primzahl ist.

Kapitel 3

Elementare Zahlentheorie

Zum Begriff: Das Wort *elementar* ist im Kontext der Zahlentheorie nicht immer gleichbedeutend mit *einfach*. Zahlentheoretische Methoden werden auch elementar genannt, wenn sie keine Funktionentheorie benutzen. Beispielsweise ist die Riemannsche Zeta-Funktion in diesem Sinn kein Untersuchungsobjekt der *elementaren* Zahlentheorie.

3.1 Die Eulersche φ–Funktion

In diesem Abschnitt befassen wir uns systematisch mit der Einheitengruppe des Rings $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{N}$ oder, dazu äquivalent, mit den Erzeugern endlicher zyklischer Gruppen. Denn jede zyklische Gruppe der Ordnung n ist nach Korollar 1.7.1 isomorph zu einer Gruppe $\mathbb{Z}/n\mathbb{Z}$. Die Erzeuger dieser zyklischen Gruppe sind genau die Restklassen der zu n teilerfremden Zahlen.

Satz 3.1.1: Sei $n \in \mathbb{N}$. Für $a \in \mathbb{Z}$ sind äquivalent:

(i) a und n sind teilerfremd.

(ii) Die Restklasse $\bar{a} = a + n\mathbb{Z}$ ist eine Einheit in $\mathbb{Z}/n\mathbb{Z}$.

(iii) $\bar{a} = a + n\mathbb{Z}$ erzeugt $\mathbb{Z}/n\mathbb{Z}$ als additive Gruppe.

Beweis:
Die Äquivalenz von (i) und (ii) ist Korollar 2.5.20. Die Bedingung (iii) ist äquivalent zu $o(\bar{a}) = n$, also zu $\bar{a} + ... + \bar{a} = k\bar{a} = \bar{k} \cdot \bar{a} \neq 0$ für $0 < k < n$ und damit zu (i). □

Für kleine $n \in \mathbb{N}$ lassen sich die Erzeuger der zyklischen Gruppe $\mathbb{Z}/n\mathbb{Z}$ und damit die Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ explizit bestimmen, indem man überprüft, welche Zahlen in $\{1, ..., n-1\}$ zu n teilerfremd sind. Für die Elemente $\bar{1}$ und $\overline{n-1} = -\bar{1}$ ist dies immer erfüllt.

Beispiel 3.1.2. Es gilt

- $(\mathbb{Z}/30\mathbb{Z})^\times = \{\bar{1}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}\}$.
- $(\mathbb{Z}/21\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{8}, \overline{10}, \overline{11}, \overline{13}, \overline{16}, \overline{17}, \overline{19}, \overline{20}\}$.
- $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\}$ für jede Primzahl $p \in \mathbb{N}$.

Um systematisch zu untersuchen, wie viele Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ existieren und wieviele Erzeuger die Gruppe $\mathbb{Z}/n\mathbb{Z}$ besitzt, definieren wir eine entsprechende Funktion, die einer natürlichen Zahl $n \in \mathbb{N}$ die Ordnung der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ zuordnet.

Definition 3.1.3: Die **Eulersche φ-Funktion** ist die Abbildung

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad n \mapsto |\{a \in \mathbb{Z} \mid 1 \leq a < n, \mathrm{ggT}(a,n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

Satz 3.1.4: Für die Eulersche φ-Funktion gilt

1. $\varphi(mn) = \varphi(m)\varphi(n)$ für alle $n, m \in \mathbb{N}$ mit $\mathrm{ggT}(n,m) = 1$,
2. $\varphi(p^n) = (p-1)p^{n-1}$ für alle $p, n \in \mathbb{N}$ mit p prim.
3. $\varphi(n) = (p_1 - 1)p_1^{\nu_1 - 1} \cdot \ldots \cdot (p_s - 1)p_s^{\nu_s - 1}$ für $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{\nu_1} \cdots p_s^{\nu_s}$.

Beweis:
1. Sind $m, n \in \mathbb{N}$ teilerfremd, so ist nach dem chinesischen Restsatz 2.5.23 der Ring $\mathbb{Z}/mn\mathbb{Z}$ isomorph zu dem Ring $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Daraus ergibt sich für die Einheitengruppen

$$\begin{aligned} & (\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \\ \Rightarrow \quad & \varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m)\varphi(n). \end{aligned}$$

2. Sind $n, p \in \mathbb{N}$ mit p prim, so ist eine Zahl $a \in \mathbb{Z}$ teilerfremd zu p^n genau dann, wenn $p \nmid a$ gilt. Die Menge der Vielfachen von p in $\{1, 2, ..., p^n\}$ ist $\{p, 2p, 3p, ..., (p^{n-1} - 1)p\}$. Sie hat p^{n-1} Elemente, und daraus ergibt sich

$$\varphi(p^n) = |\{1, 2, \ldots, p^n - 1\}| - |\{p, 2p, \ldots, (p^{n-1} - 1)p\}| = p^n - 1 - (p^{n-1} - 1) = (p-1)p^{n-1}.$$

3. Folgt direkt aus 1. und 2. □

Beispiel 3.1.5. Es gilt

- $\varphi(3072) = \varphi(2^{10} \cdot 3) = (2-1) \cdot 2^9 \cdot 2 = 2^{10} = 1024$.
- $\varphi(169) = \varphi(13^2) = 12 \cdot 13 = 156$.

Aus der Primfaktorzerlegung einer Zahl $n \in \mathbb{N}$ lässt sich also direkt die Anzahl der Einheiten im Ring $\mathbb{Z}/n\mathbb{Z}$ und die Zahl der Erzeuger der Gruppe $\mathbb{Z}/n\mathbb{Z}$ berechnen. Weitere interessante Ergebnisse zur Eulerschen φ-Funktion ergeben sich direkt aus bekannten Aussagen über Gruppen. Da die Ordnung jedes Elements $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ nach dem Satz von Lagrange die Gruppenordnung $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ teilt, ist $\bar{a}^{\varphi(n)} = \bar{1}$, und damit $a^{\varphi(n)} \equiv 1 \bmod n$ für alle zu n teilerfremden $a \in \mathbb{Z}$. Für Primzahlen p lässt sich das noch expliziter machen, da dann $\varphi(p) = p - 1$ gilt.

Korollar 3.1.6 (Satz von Euler): Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd zu n. Dann ist

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Korollar 3.1.7 (Kleiner Satz von Fermat): Für jede Primzahl $p \in \mathbb{N}$ gilt

$$a^p \equiv a \bmod p \; \forall a \in \mathbb{Z} \qquad \text{und} \quad a^{p-1} \equiv 1 \bmod p \;\; \text{falls } a \in \mathbb{Z} \text{ mit } p \nmid a.$$

Beweis:
Da p eine Primzahl ist, sind offenbar alle Zahlen $1, \ldots, p-1$ teilerfremd zu p und damit $\varphi(p) = p-1$. Mit dem Satz von Euler folgt die zweite Aussage und durch Multiplikation mit a dann die erste Aussage für $p \nmid a$. Für $p \mid a$ gilt $a^p \equiv 0 \equiv a \bmod p$. □

Der kleine Satz von Fermat besitzt eine interessante Anwendung, nämlich einen *Primzahltest*. Kann man eine Zahl $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ und $a^{n-1} \not\equiv 1 \mod n$ finden, so ist n nach dem kleinen Satz von Fermat keine Primzahl. In der Praxis kann man dazu zunächst kleine Zahlen $a \in \mathbb{N}$ wählen und probieren, ob $a^{n-1} \equiv 1 \bmod n$. Dabei ist es allerdings wegen des Aufwands nicht sinnvoll a^{n-1} explizit zu berechnen. Stattdessen arbeitet man mit der sogenannten *binären Exponentiation*.

Anwendung 3.1.8 (**Fermat-Primzahltest** mit der **binären Exponentiation**):

Die binäre Exponentiation beruht auf der Rekursion

$$a^m = \begin{cases} \left(a^{\frac{m}{2}}\right)^2 & \text{für } m \text{ gerade,} \\ a \cdot a^{m-1} & \text{für } m \text{ ungerade.} \end{cases}$$

Um $a^m \bmod s$ zu berechnen kann man daher wie folgt vorgehen:

- Man setzt $k_0 = m$ und $k_{n+1} = k_n/2$ falls k_n gerade und $k_{n+1} = k_n - 1$ falls k_n ungerade ist, bis man die Zahl $k_r = 0$ erreicht.
- Man setzt $m_r = 1 \bmod s$, und für $0 \le n \le r-1$ setzt man $m_n = a \cdot m_{n+1} \bmod s$ falls k_n ungerade ist, und $m_n = m_{n+1}^2 \bmod s$ falls k_n gerade ist.
- Dann gilt: $a^m \bmod s = m_0 \bmod s$.

Dieses Verfahren ist deutlich effizienter als die direkte Berechnung von a^m, die m Multiplikationen benötigt. Man benötigt dabei nämlich nur etwa $\log_2 m \ll m$ Multiplikationen und die Reduktion mod s nach jeder Multiplikation hält die Zahlen klein.

Beispiel 3.1.9.
Wir berechnen mit der binären Exponentiation $2^{38} \equiv 4 \bmod 39$. Damit ist 39 keine Primzahl.

	k_n	Operation	m_n
n=0	38	:2	$11^2 = 121 \equiv 4 \bmod 39$
n=1	19	-1	$2 \cdot 25 = 50 \equiv 11 \bmod 39$
n=2	18	:2	$5^2 \equiv 25 \bmod 39$
n=3	9	-1	$2 \cdot 22 = 44 \equiv 5 \bmod 39$
n=4	8	:2	$16^2 = 256 \equiv 22 \bmod 39$
n=5	4	:2	$4^2 \equiv 16 \bmod 39$
n=6	2	:2	$2^2 \equiv 4 \bmod 39$
n=7	1	-1	$2 \bmod 39$
n=8	0		$1 \bmod 39$

Bemerkung 3.1.10. Der Primzahltest mit dem Satz von Fermat liefert eine *notwendige* Bedingung dafür, dass eine Zahl $n \in \mathbb{N}$ eine Primzahl ist, aber keine hinreichende. Es gibt Zahlen $n \in \mathbb{N}$ mit $a^{n-1} \equiv 1 \bmod n$ für alle zu n teilerfremden $a \in \mathbb{Z}$, obwohl n nicht prim ist. Solche Zahlen heißen **Carmichaelzahlen**. Seit 1994 ist bekannt, dass es unendlich viele Carmichaelzahlen gibt. Die Carmichaelzahlen < 100000 sind

Carmichaelzahl	Primfaktorzerlegung	Carmichaelzahl	Primfaktorzerlegung
561	$3 \cdot 11 \cdot 17$	15841	$7 \cdot 31 \cdot 73$
1105	$5 \cdot 13 \cdot 17$	29341	$13 \cdot 37 \cdot 61$
1729	$7 \cdot 13 \cdot 19$	41041	$7 \cdot 11 \cdot 13 \cdot 41$
2465	$5 \cdot 17 \cdot 29$	46657	$13 \cdot 37 \cdot 97$
2821	$7 \cdot 13 \cdot 31$	52633	$7 \cdot 73 \cdot 103$
6601	$7 \cdot 23 \cdot 41$	62745	$3 \cdot 5 \cdot 47 \cdot 89$
8911	$7 \cdot 19 \cdot 67$	63973	$7 \cdot 13 \cdot 19 \cdot 37$
10585	$5 \cdot 29 \cdot 73$	75361	$11 \cdot 13 \cdot 17 \cdot 31$

Eine weitere wichtige Anwendung des kleinen Satzes von Fermat und des Satzes von Euler ist die sogenannte *RSA-Verschlüsselung*[1]. Dies ist ein asymmetrisches Verschlüsselungsverfahren, das oft zum Übertragen von Schlüsseln für andere Verfahren benutzt wird. Es wird beispielsweise in *X.509-Zertifikaten*, in den Übertragungs-Protokollen *IPsec*, *TLS*, *SSH*, *WASTE*, der Email-Verschlüsselung durch *OpenPGP* und *S/MIME*, im RFID Chip auf dem deutschen Reisepass und im Online-Banking Verfahren *HBCI* eingesetzt. Der Vorteil eines asymmetrischen Verschlüsselungsverfahrens ist, dass der private Schlüssel, der zum Entschlüsseln einer Botschaft benutzt wird, nie weitergegeben werden muss und damit auch nicht abgefangen werden kann. Weitergegeben wird nur der öffentliche Schlüssel, der zum Verschlüsseln der Botschaften benutzt wird, aber nicht zum Entschlüsseln ausreicht.

Anwendung 3.1.11 (RSA-Verschlüsselung):

1. Man wählt zwei große Primzahlen p und q, die nicht zu nahe beieinander liegen (optimal ist $0,1 < |\log_2 p - \log_2 q| < 30$). Diese können beispielsweise mit Varianten des Fermatschen Primzahltests 3.1.8 bestimmt werden. Sie sind der **private Schlüssel**, der an niemanden übermittelt wird.

2. Man berechnet $n := pq$ und $m := \varphi(n) = (p-1)(q-1)$ und wählt eine zu m teilerfremde Zahl[2] $d \in \mathbb{N}$. Die Zahlen n und d sind der **öffentliche Schlüssel** oder **public key** und können bekannt gegeben werden an alle, die einem Botschaften schicken wollen.

3. Die an den Empfänger zu vermittelnde Botschaft wird durch eine Restklasse $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ repräsentiert[3]. Sie wird verschlüsselt, indem man aus $\bar{a}$, n und d die Zahl $b = a^d \bmod$ n berechnet, und diese Zahl übermittelt.

4. Der Empfänger, der p, q, d, m kennt, berechnet mit Hilfe des euklidischen Algorithmus wie in Korollar 2.5.39 und Beispiel 2.5.40 ein Inverses $e = d^{-1} \bmod m$ sowie $b^d \bmod n$.

[1] Benannt nach Ronald L. Rivest, Adi Shamir und Leonard Adleman.

[2] Diese Bedingung kann gelockert werden. Es ist eigentlich nur notwendig, dass m teilerfremd zu $\lambda(n)$ ist, wobei λ die sogenannte Carmichaelfunktion ist mit $\lambda(n) \mid \varphi(n)$ für alle $n \in \mathbb{N}$.

[3] Diese Bedingung kann gelockert werden. Es reicht, dass $a \not\equiv 0 \bmod n$ gilt

5. Da $ed = 1 + km$ für ein $k \in \mathbb{Z}$ und $a^m \equiv 1 \bmod n$ nach dem Satz von Euler 3.1.6, folgt

$$b^e = (a^d)^e = a^{de} = a^{1+km} = a \cdot (a^m)^k \equiv a \bmod n$$

und der Empfänger kann somit die Botschaft entschlüsseln.

Diese Methode funktioniert (noch?), da bisher kein effizienter Algorithmus zur Berechnung der Primfaktorzerlegung bekannt ist, und daher die Zahlen m und e aus n und d nicht bestimmt werden können. Es gibt allerdings auch keinen Beweis, dass ein effizienter Algorithmus zur Primfaktorzerlegung nicht existiert. In der Praxis muss die RSA-Verschlüsselung für maximale Sicherheit auch noch mit anderen Verfahren kombiniert werden.

3.2 Primzahlen: Die Sätze von Euklid und Wilson

Wir beschäftigen uns nun noch etwas systematischer mit Primzahlen. Seit der Antike ist bekannt, dass es unendlich viele Primzahlen gibt. Die ist der berühmte Satz von Euklid, den wir auf zwei verschiedene Weisen beweisen werden.

Satz 3.2.1 (**Satz von Euklid**)**:** Es gibt unendlich viele Primzahlen.

Beweis von Euklid:
Angenommen es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_t > 1$. Da 2 prim ist, ist dann $t \geq 1$. Damit ist $n := 1 + p_1 \ldots p_t > 1$, und n hat einen Primteiler p. Da $n \equiv 1 \bmod p_i$ gilt aber $p \neq p_i$ für $i = 1, ..., t$, ein Widerspruch. □

Beweis von Euler: Angenommen es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_t$. Dann hätte jede natürliche Zahl $n \in \mathbb{Z}_{>0}$ eine eindeutige Primzahlzerlegung

$$n = p_1^{\nu_1} \ldots p_t^{\nu_t} \text{ mit } \nu_1, \ldots, \nu_t \geq 0. \tag{3.1}$$

Dann können wir die harmonische Reihe faktorisieren, um zu einem Widerspruch zu gelangen

$$\infty = \sum_{n=1}^{\infty} \frac{1}{n} = \sum_{\nu_1,\ldots,\nu_t \geq 0} \frac{1}{p_1^{\nu_1}} \cdots \frac{1}{p_t^{\nu_t}} = \prod_{i=1}^{t} (1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots) = \prod_{i=1}^{t} \frac{1}{1 - \frac{1}{p_i}} < \infty, \tag{3.2}$$

wobei benutzt wurde, dass die Reihen $\Sigma_{k=0}^{\infty} 1/p_i^k$ für $p_i > 1$ absolut konvergieren, und damit nach dem Cauchyschen Produktsatz ausmultipliziert werden können. □

Euklids Beweis ist konstruktiv, kann also zur Konstruktion von Primzahlen benutzt werden. Multipliziert man nämlich alle Primzahlen $p_1, ..., p_t$ in einem Intervall $[1, p_t]$ und addiert Eins hinzu, so erhält man eine Zahl $p = p_1 \cdots p_t + 1$, die nicht durch $p_1, ..., p_t$ teilbar ist. Ihre Primfaktorzerlegung liefert also neue Primzahlen. Eulers Beweis besitzt dafür Anwendungen in der Zahlentheorie und liefert Erkenntnisse über die Verteilung von Primzahlen. So folgt aus der Divergenz des Produkts auf der rechten Seite in (3.2) insbesondere, dass $\sum_{p \text{ prim}} 1/p = \infty$. Betrachtet man statt der harmonischen Reihe $\Sigma_{n=1}^{\infty} 1/n$ die Reihe $\Sigma_{n=1}^{\infty} 1/n^s$ für $s > 1$, die strikt konvergiert, so erhält man eine Identität für die **Riemannsche Zetafunktion**

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prim}} \frac{1}{1 - \frac{1}{p^s}} \qquad \text{für} \qquad s > 1.$$

Der Satz von Euklid liefert zwar die Existenz beliebig vieler Primzahlen, aber kein notwendiges und hinreichendes Kriterium dafür, dass eine gegebene Zahl $n \in \mathbb{N}$ eine Primzahl ist. Gängige Primzahltests wie der Primzahltest mit Hilfe des kleinen Satzes von Fermat, liefern oft nur notwendige, aber keine hinreichenden Bedingungen. Andere in der Praxis genutzte Primzahltests liefern nur Wahrscheinlichkeiten dafür, dass es sich bei einer gegebenen Zahl um eine Primzahl handelt. Dennoch gibt es notwendige und hinreichende Primzahlkriterien. Das Problem ist nur, dass diese rechnerisch nicht effizient sind. Ein Beispiel dafür ist der Satz von Wilson.

Satz 3.2.2 (Satz von Wilson): Sei $2 \leq n \in \mathbb{N}$. Dann ist n genau dann eine Primzahl, wenn

$$(n-1)! \equiv -1 \bmod n.$$

Beweis:
Angenommen n ist keine Primzahl. Dann gibt es $m \in \mathbb{Z}$ mit $1 < m < n$ und $m \mid n$. Wegen $\mathrm{ggT}(m,n) = m > 1$ ist dann $\overline{m}$ in $\mathbb{Z}/n\mathbb{Z}$ keine Einheit nach Satz 3.1.1. In $\mathbb{Z}/n\mathbb{Z}$ gilt

$$\overline{(n-1)!} = \bar{1} \cdot \bar{2} \cdots \overline{m-1} \cdot \overline{m} \cdot \overline{m+1} \cdots \overline{n-1} \tag{3.3}$$

Damit ist $\overline{(n-1)!}$ keine Einheit und insbesondere $\overline{(n-1)!} \neq -\bar{1}$.

Ist $n \in \mathbb{N}$ eine Primzahl, so ist $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$ ein Körper und $\overline{(n-1)!}$ ist das Produkt aller Einheiten in $\mathbb{F}_n$. Für $n = 2$ erhält man $1! = -1 \bmod 2$. Ansonsten ist n ungerade, und damit $|\mathbb{F}_n^\times| = n-1$ gerade. Alle Einheiten $a \in \mathbb{F}_n^\times$ mit $a \neq a^{-1}$ bilden Paare, und die zugehörigen Faktoren in (3.3) multiplizieren sich zu $a \cdot a^{-1} = \bar{1}$. Die Einheiten mit $a = a^{-1}$ erfüllen $a^2 - \bar{1} = 0$. Wegen der Nullteilerfreiheit von $\mathbb{F}_n$ hat die Gleichung $x^2 - \bar{1} = (x+\bar{1})(x-\bar{1}) = 0$ genau die zwei Lösungen $x = \bar{1}$ und $x = -\bar{1}$, und damit folgt $\overline{(n-1)!} = \bar{1} \cdot (-\bar{1}) = -\bar{1}$. □

Der Satz von Wilson liefert zwar keinen in der Praxis relevanten Primzahltest. Er kann aber dazu genutzt werden, Fakultäten von Zahlen in endlichen Zahlkörpern $\mathbb{F}_p$ zu berechnen und die Irreduzibilität gewisser Polynome in $\mathbb{F}_p[x]$ zu beweisen.

Korollar 3.2.3: Sei $p = 2q+1$ eine ungerade Primzahl. Dann ist

$$(q!)^2 \equiv (-1)^{q+1} \bmod p$$

Beweis:
Nach dem Satz von Wilson gilt $(p-1)! = (2q)! = -1 \bmod p$. Daraus ergibt sich

$$\begin{aligned} -1 \bmod p &\equiv (2q)! \bmod p \equiv q! \cdot (q+1) \cdot (q+2) \cdots (p-1) \bmod p \\ &\equiv q! \cdot (p-q) \cdot (p-q+1) \cdots (p-1) \bmod p \equiv q! \cdot (-q) \cdot (-q+1) \cdots (-1) \bmod p \\ &\equiv (-1)^q (q!)^2 \bmod p. \end{aligned}$$

□

Korollar 3.2.4: Sei p eine Primzahl mit $p \equiv 1 \bmod 4$. Dann ist $x^2 + \bar{1} \in \mathbb{F}_p[x]$ reduzibel.

Beweis:
Ist $p = 2q+1 \equiv 1 \bmod 4$, so ist q gerade, und damit ergibt sich aus Korollar 3.2.3 dass $(q!)^2 = (-1)^{q+1} \bmod p = -1 \bmod p$. Damit ist $q!$ eine Nullstelle des quadratischen Polynoms $x^2 + \bar{1} \in \mathbb{F}_p[x]$ und $x^2 + \bar{1}$ ist reduzibel. □

3.3 Die Gaußschen Zahlen

Mit den Resultaten zu Primzahlen im letzten Abschnitt haben wir nun das nötige Handwerkszeug, um den Ring der Gaußschen Zahlen systematisch zu untersuchen. Wir werden nun zeigen, dass es sich dabei um einen euklidischen Ring handelt und die Primelemente in $\mathbb{Z}[\mathrm{i}]$ bestimmen. Der Ring der Gaußschen Zahlen wurde in Beispiel 2.2.3, 8 eingeführt als der Ring

$$\mathbb{Z}[\mathrm{i}] := \mathbb{Z} + \mathrm{i}\mathbb{Z} = \{a + \mathrm{i}b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}.$$

Es handelt sich offensichtlich um einen unitalen Unterring von $\mathbb{C}$ und damit nach Beispiel 2.4.12, 3. um einen Integritätsbereich. In Beispiel 2.3.14 wurde gezeigt, dass dieser Ring isomorph zum Faktorring $\mathbb{Z}[x]/(x^2+1)$ ist, wobei $(x^2+1) \subseteq \mathbb{Z}[x]$ das von dem Polynom x^2+1 erzeugte Hauptideal bezeichnet. Dieser Isomorphismus wird von dem unitalen Ringhomomorphismus

$$\mathrm{ev}_{\mathrm{i}} : \mathbb{Z}[x] \to \mathbb{Z}[\mathrm{i}], \quad \Sigma_{k=0}^{\infty} a_k x^k \mapsto \Sigma_{k=0}^{\infty} a_k \mathrm{i}^k$$

mit Kern $\ker(\mathrm{ev}_{\mathrm{i}}) = (x^2+1)$ induziert (vgl. Satz 2.3.2 und Beispiel 2.3.14). Wir bestimmen nun die Einheiten im Ring $\mathbb{Z}[\mathrm{i}]$ und zeigen anschließend, dass $\mathbb{Z}[\mathrm{i}]$ euklidisch ist.

Satz 3.3.1: Der Ring $\mathbb{Z}[\mathrm{i}] = \mathbb{Z} + \mathrm{i}\mathbb{Z}$ hat die folgenden Eigenschaften:

1. Er hat genau zwei unitale Ringautomorphismen, nämlich die Identitätsabbildung und die komplexe Konjugation $^-$: $a + \mathrm{i}b \mapsto a - \mathrm{i}b$.
2. Die **Normabbildung** $N : \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$, $a + \mathrm{i}b \mapsto |a + \mathrm{i}b|^2 = a^2 + b^2$ ist multiplikativ: $N(uv) = N(u)N(v)$ für alle $u, v \in \mathbb{Z}[\mathrm{i}]$.
3. Seine Einheitengruppe ist $\mathbb{Z}[\mathrm{i}]^\times = \{u \in \mathbb{Z}[\mathrm{i}] \mid N(u) = 1\} = \{1, \mathrm{i}, -1, -\mathrm{i}\}$.
4. Jedes Element aus $\mathbb{Z}[\mathrm{i}]$ ist assoziiert zu genau einem Element der Menge

$$\{a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}] \mid -a < b \leq a\} \cup \{0\}.$$

Beweis:
1. Ist $\varphi : \mathbb{Z}[\mathrm{i}] \to \mathbb{Z}[\mathrm{i}]$ ein unitaler Ringautomorphismus, so ist per Definition $\varphi(1) = 1$. Da φ ein Gruppenhomomorphismus ist, folgt $\varphi(a) = a$ für alle $a \in \mathbb{Z}$, und daraus ergibt sich $\varphi(a + \mathrm{i}b) = \varphi(a) + \varphi(\mathrm{i})\varphi(b) = a + \varphi(\mathrm{i})b$ für alle $a, b \in \mathbb{Z}$. Damit ist φ durch $\varphi(\mathrm{i})$ eindeutig bestimmt, und es gilt $\varphi(\mathrm{i})^2 = \varphi(\mathrm{i}^2) = \varphi(-1) = -1$, also $\varphi(\mathrm{i}) \in \{\pm\mathrm{i}\}$. Für $\varphi(\mathrm{i}) = \mathrm{i}$ erhält man $\varphi = \mathrm{id}$, und für $\varphi(\mathrm{i}) = -\mathrm{i}$ die komplexe Konjugation.

2. Folgt aus der Identität $|z \cdot w| = |z| \cdot |w|$ für alle $z, w \in \mathbb{C}$.

3. Ist $u = a + ib \in \mathbb{Z}[\mathrm{i}]$ eine Einheit, so folgt $1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1})$, und damit muss $N(u)$ eine Einheit in $\mathbb{Z}$ sein, also $N(u) \in \{\pm 1\}$. Da $N(u) = a^2 + b^2 > 0$ folgt $N(u) = 1$ und damit $u = a + \mathrm{i}b \in \{\pm 1, \pm\mathrm{i}\}$.

4. Multiplikation mit Einheiten entspricht Drehungen der komplexen Ebene um Vielfache von $90°$. Damit kann jedes $z \in \mathbb{C}\backslash\{0\}$ in genau eine Zahl $x+\mathrm{i}y$ mit $-x < y \leq x$ überführt werden. □

Satz 3.3.2: Der Ring $\mathbb{Z}[\mathrm{i}]$ ist euklidisch mit Höhenfunktion $N : \mathbb{Z}[\mathrm{i}]\backslash\{0\} \to \mathbb{N}_0$, $a+\mathrm{i}b \mapsto a^2+b^2$.

Beweis:
Als unitaler Unterring des Körpers $\mathbb{C}$ ist $\mathbb{Z}[\mathrm{i}]$ ein Integritätsbereich. Wir zeigen, dass es zu Elementen $u, v \in \mathbb{Z}[\mathrm{i}]$ mit $v \neq 0$ Elemente $m, r \in \mathbb{Z}[\mathrm{i}]$ gibt mit $u = mv + r$ und $N(r) < N(v)$. Sei dazu $u/v = \alpha + i\beta \in \mathbb{C}$ mit $\alpha, \beta \in \mathbb{R}$. Dann gibt es zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $|\alpha - a| \leq \frac{1}{2}$ und $|\beta - b| \leq \frac{1}{2}$. Für $m := a + ib \in \mathbb{Z}[\mathrm{i}]$ und $r := u - mv \in \mathbb{Z}[\mathrm{i}]$ gilt dann

$$\frac{N(r)}{N(v)} = \frac{|r|^2}{|v|^2} = \left|\frac{u}{v} - m\right|^2 = (\alpha - a)^2 + (\beta - b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1 \quad \Rightarrow \quad N(r) < N(v). \qquad \square$$

Da $\mathbb{Z}[\mathrm{i}]$ ein euklidischer Ring ist, ist $\mathbb{Z}[\mathrm{i}]$ nach Satz 2.5.28 ein Hauptidealring und damit nach Satz 2.5.21 auch ein faktorieller Ring. Mit Hilfe der Ergebnisse über Primzahlen aus dem letzten Abschnitt können wir nun die Primelemente in $\mathbb{Z}[\mathrm{i}]$ explizit bestimmen. Wir beginnen dabei mit Elementen des unitalen Unterrings $\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}]$. Ist $n \in \mathbb{Z}$ kein Primelement in $\mathbb{Z}$, so ist n auch kein Primelement in $\mathbb{Z}[\mathrm{i}]$, denn jeder echte Teiler von n in $\mathbb{Z}$ ist auch ein echter Teiler von n in $\mathbb{Z}[\mathrm{i}]$. Allerdings kann es passieren, dass Primzahlen in $\mathbb{Z}$ keine Primelemente in $\mathbb{Z}[\mathrm{i}]$ sind. In diesem Fall liefert uns deren Primfaktorzerlegung in $\mathbb{Z}[\mathrm{i}]$ neue Primelemente, die nicht in $\mathbb{Z}$ enthalten sind. Die Frage ist, für welche Primzahlen in $\mathbb{Z}$ dies eintritt, und ob wir auf diese Weise alle Primelemente in $\mathbb{Z}[\mathrm{i}]$ erhalten. Zur Klärung der ersten Frage, benötigen wir die Aussagen über die Irreduzibilität des Polynoms $x^2 + \bar{1}$ in $\mathbb{F}_p[x]$ aus Korollar 3.2.4.

Satz 3.3.3: Für eine Primzahl $p \in \mathbb{N}$ sind äquivalent:

(i) p ist nicht prim in $\mathbb{Z}[\mathrm{i}]$.

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

(iii) $p = 2$ oder $p \equiv 1 \bmod 4$.

(iv) Das Polynom $x^2 + \bar{1}$ ist reduzibel in $\mathbb{F}_p[x]$.

Beweis:
(i) $\Rightarrow$ (ii): Ist $p \in \mathbb{Z}$ eine Primzahl in $\mathbb{Z}$, aber nicht prim in $\mathbb{Z}[\mathrm{i}]$, so ist p keine Einheit, denn $\mathbb{Z}[\mathrm{i}]^\times \cap \mathbb{Z} = \{\pm 1\}$. Da $\mathbb{Z}[\mathrm{i}]$ faktoriell ist, ist dann p reduzibel in $\mathbb{Z}[\mathrm{i}]$, und es gibt $u, v \in \mathbb{Z}[\mathrm{i}] \setminus \mathbb{Z}[\mathrm{i}]^\times$ mit $p = uv$. Da die Normabbildung multiplikativ ist, folgt $p^2 = N(p) = N(uv) = N(u)N(v)$. Da $u, v \notin \mathbb{Z}[\mathrm{i}]^\times$ gilt $N(u), N(v) > 1$, und es folgt $N(u) = N(v) = p$. Da $u \in \mathbb{Z}[\mathrm{i}]$ gibt es $a, b \in \mathbb{Z}$ mit $u = a + ib$, und daraus folgt $p = N(u) = a^2 + b^2$.

(ii) $\Rightarrow$ (iii) Sei $p = a^2 + b^2 \neq 2$ eine Primzahl. Dann ist p ungerade, und damit genau eine der Zahlen $a, b \in \mathbb{Z}$ gerade und die andere ungerade. Sei o. B. d. A. die Zahl a gerade. Dann gibt es $a', b' \in \mathbb{Z}$ mit $a = 2a'$, $b = 2b' + 1$, und es folgt

$$p = (2a')^2 + (2b' + 1)^2 = 4a'^2 + 4b'^2 + 4b' + 1 \equiv 1 \bmod 4.$$

(iii) $\Rightarrow$ (iv) Für $p = 2$ ist $x^2 + \bar{1} = (x + \bar{1})^2 \in \mathbb{F}_2[x]$ nicht irreduzibel. Für $p \equiv 1 \bmod 4$ ist $x^2 + \bar{1} \in \mathbb{F}_p[x]$ nach Korollar 3.2.4 reduzibel.

(iv) $\Rightarrow$ (i) Sei $x^2 + \bar{1}$ reduzibel in $\mathbb{F}_p[x]$. Dann ist $(x^2 + \bar{1})$ kein Primideal in $\mathbb{F}_p[x]$ und $\mathbb{F}_p[x]/(x^2 + \bar{1})$ kein Integritätsbereich nach Satz 2.4.16. Da $\mathbb{Z}[\mathrm{i}] \cong \mathbb{Z}[x]/(x^2 + 1)$ nach Beispiel 2.3.14, folgt

$$\mathbb{Z}[\mathrm{i}]/(p) \cong \mathbb{Z}[x]/(p, x^2 + 1) \cong \mathbb{F}_p[x]/(x^2 + \bar{1}).$$

Damit ist auch $\mathbb{Z}[\mathrm{i}]/(p)$ kein Integritätsbereich und p nicht prim in $\mathbb{Z}[\mathrm{i}]$ nach Satz 2.4.16. $\square$

Satz 3.3.3 liefert nicht nur Aussagen über die Primelemente in $\mathbb{Z}[\mathrm{i}]$, sondern auch einen interessanten Zusammenhang zwischen der Darstellbarkeit einer Primzahl als Summe zweier Quadrate ganzer Zahlen und ihrem Rest bei Division durch vier. Dieser lässt sich zu einer Aussage über beliebige natürliche Zahlen verallgemeinern. Die Darstellbarkeit einer natürlichen Zahl n als Summe zweier Quadrate ganzer Zahlen hängt nur von den Multiplizitäten der Primzahlen $p \equiv -1 \bmod 4$ ab, die in ihrer Primfaktorzerlegung auftreten.

Satz 3.3.4 (Fermat)**:**
Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{p \in \mathbb{N} \text{ prim}} p^{v_p(n)}$. Dann sind äquivalent:

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

(ii) Für jede Primzahl $p \in \mathbb{N}$ mit $p \equiv -1 \bmod 4$ ist $v_p(n)$ gerade.

Beweis:
(i) $\Rightarrow$ (ii): Induktion über n. Für $n = 1$ gilt $v_p(n) = 0$ für alle Primzahlen p, und damit ist die Aussage wahr. Sei nun $n = a^2 + b^2 > 1$ mit $a, b \in \mathbb{Z}$ und $p \in \mathbb{N}$ prim mit $p \equiv -1 \mod 4$. Dann ist p auch prim in $\mathbb{Z}[\mathrm{i}]$ nach Satz 3.3.3, und aus $p \mid n = a^2 + b^2 = (a + \mathrm{i}b)(a - \mathrm{i}b)$ folgt $p \mid a + \mathrm{i}b$ oder $p \mid a - \mathrm{i}b$. Da $p \mid a + \mathrm{i}b \Leftrightarrow p \mid a$ und $p \mid b \Leftrightarrow p \mid a - \mathrm{i}b$, gilt $p^2 \mid n$. Damit gibt es $n', a', b' \in \mathbb{Z}$ mit $n = n'p^2$, $a = a'p$, $b = b'p$ und $n' = a'^2 + b'^2$. Nach Induktionsvoraussetzung ist $v_p(n')$ gerade und damit auch $v_p(n) = v_p(n') + 2$.

(ii)$\Rightarrow$(i): Nach Voraussetzung treten alle Primzahlen p mit $p \equiv -1 \mod 4$ mit geradzahligen Vielfachheiten $v_p(n)$ in n auf. Indem wir die Potenzen von Primzahlen p mit $p \equiv -1 \mod 4$ aus der Primfaktorzerlegung von n abspalten, erhalten wir eine Faktorisierung $n = m^2 \cdot p_1 \cdots p_t$ mit $m \in \mathbb{Z}$ und Primzahlen p_j mit $p_j = 2$ oder $p_j \equiv 1 \bmod 4$ für $j \in \{1, ..., t\}$. Nach Satz 3.3.3 gibt es $a_j, b_j \in \mathbb{Z}$ mit $p_j = a_j^2 + b_j^2 = N(a_j + \mathrm{i}b_j)$. Setzen wir $u_j := a_j + \mathrm{i}b_j$ und $u = a + \mathrm{i}b := mu_1 \dots u_t \in \mathbb{Z}[\mathrm{i}]$, so folgt aus der Multiplikativität der Normabbildung

$$n = m^2 p_1 \dots p_t = N(m)N(u_1) \dots N(u_t) = N(mu_1 \dots u_t) = N(u) = a^2 + b^2.$$

□

Mit Hilfe von Satz 3.3.1 und Satz 3.3.3 können wir nun die Primelemente im Ring $\mathbb{Z}[\mathrm{i}]$ vollständig bestimmen. Dazu nutzen wir aus, dass nach Satz 3.3.1, 4. jedes Primelement in $\mathbb{Z}[\mathrm{i}]$ assoziiert ist zu genau einem Primelement $a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]$ mit $-a < b \leq a$. Damit ist die Menge $P_{\mathbb{Z}[\mathrm{i}]} = \{a + \mathrm{i}b \mid a + \mathrm{i}b \text{ prim in } \mathbb{Z}[\mathrm{i}], -a < b \leq a\}$ ein Repräsentantensystem der Primelemente in $\mathbb{Z}[\mathrm{i}]$. Indem wir zeigen, dass jedes Element in diesem Repräsentantensystem genau eine Primzahl in $\mathbb{N}$ teilt, können wir dann die Primelemente in $\mathbb{Z}[\mathrm{i}]$ explizit bestimmen.

Satz 3.3.5: Sei $P_{\mathbb{Z}[\mathrm{i}]} = \{a + \mathrm{i}b \mid a + \mathrm{i}b \text{ prim in } \mathbb{Z}[\mathrm{i}], -a < b \leq a\}$ und $P_{\mathbb{Z}}$ die Menge aller positiven Primzahlen in $\mathbb{Z}$. Dann gilt:

1. Jedes Element $u \in P_{\mathbb{Z}[\mathrm{i}]}$ teilt genau eine Primzahl $p \in \mathbb{N}$. Dies definiert eine surjektive Abbildung $\pi : P_{\mathbb{Z}[\mathrm{i}]} \to P_{\mathbb{Z}}$.
2. Das Urbild $\pi^{-1}(p)$ und die Zerlegung von p in Primelemente in $P_{\mathbb{Z}[\mathrm{i}]}$ sind gegeben durch:
   - $\pi^{-1}(2) = \{1 + \mathrm{i}\}$ und $2 = (-\mathrm{i})(1 + \mathrm{i})^2$.
   - $\pi^{-1}(p) = \{p\}$ und $p = p$ für $p \equiv -1 \bmod 4$.
   - $\pi^{-1}(p) = \{a \pm \mathrm{i}b\}$ und $p = (a + \mathrm{i}b)(a - \mathrm{i}b)$ mit eindeutigen $0 < b < a$ für $p \equiv 1 \bmod 4$.

Beweis:
1. Sei $u \in P_{\mathbb{Z}[\mathrm{i}]}$. Da $\mathbb{Z}[\mathrm{i}]$ ein Hauptidealring ist und u ein Primelement, ist $\mathbb{Z}[\mathrm{i}]/(u)$ ein Körper nach Satz 2.5.22. Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}[\mathrm{i}]/(u)$, $z \mapsto z + (u)$ ist ein unitaler Ringhomomorphismus mit $\ker(f) = \mathbb{Z} \cap (u)$. Nach dem Homomorphiesatz 2.3.11 induziert f damit einen injektiven unitalen Ringhomomorphismus $f' : \mathbb{Z}/(\mathbb{Z} \cap (u)) \to \mathbb{Z}[i]/(u)$, $z + \ker(f) \mapsto z + (u)$. Damit ist $\mathbb{Z}/(\mathbb{Z} \cap (u))$ isomorph zu dem unitalen Unterring $f'(\mathbb{Z}/(\mathbb{Z} \cap (u)))$ des Körpers $\mathbb{Z}[\mathrm{i}]/(u)$, also zu einem Integritätsbereich. Nach Satz 2.4.16 ist $\mathbb{Z} \cap (u)$ damit ein Primideal in $\mathbb{Z}$, also von der Form $\mathbb{Z} \cap (u) = p\mathbb{Z}$ mit einer Primzahl $p \in \mathbb{N}$. Wegen $p \in \mathbb{Z} \cap (u) \subseteq (u)$ gilt $u \mid p$. Ist $q \in \mathbb{N}$ eine weitere Primzahl mit $u \mid q$, so folgt $q \in \mathbb{Z} \cap (u) = p\mathbb{Z}$ und damit $p \mid q$, also $q = p$.

2. Wir zeigen, dass jedes Element $u = a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]$ mit $N(u) \in \mathbb{N}$ prim ein Primelement ist: Aus $N(u) \in \mathbb{N}$ prim, folgt $N(u) \neq 1$ und damit $u \notin \mathbb{Z}[\mathrm{i}]^\times$. Ist $u = v \cdot w$ mit $v, w \in \mathbb{Z}[\mathrm{i}]$, so folgt aus der Multiplikativität der Normabbildung $N(u) = N(v) \cdot N(w)$. Da $N(u)$ prim ist, folgt $N(v) = 1$ und $N(w) = N(u)$ oder $N(w) = 1$ und $N(v) = N(u)$. Im ersten Fall ist v eine Einheit, im zweiten Fall w. Damit ist u ein Primelement.

Wir betrachten nun die drei Fälle getrennt.

• $p = 2$: Es gilt $2 = 1+1 = (1+\mathrm{i})(1-\mathrm{i}) = (-\mathrm{i})(1+\mathrm{i})^2$. Es ist $-\mathrm{i} \in \mathbb{Z}[\mathrm{i}]^\times$, und das Element $1+\mathrm{i}$ ist wegen $N(1+\mathrm{i}) = 2$ ein Primelement. Damit ist $2 = (-\mathrm{i})(1+\mathrm{i})^2$ die Primfaktorzerlegung von 2 in $\mathbb{Z}[\mathrm{i}]$, und wegen der Eindeutigkeit der Primfaktorzerlegung hat 2 keine weiteren Primteiler. Damit ist $\pi^{-1}(2) = \{1 + \mathrm{i}\}$.

• $p \equiv -1 \bmod 4$: In diesem Fall ist p auch ein Primelement in $\mathbb{Z}[\mathrm{i}]$ nach Satz 3.3.3, also $p \in P_{\mathbb{Z}[\mathrm{i}]}$, und die Primfaktorzerlegung ist $p = p$. Wegen der Eindeutigkeit der Primfaktorzerlegung hat p keine weiteren Primteiler und $\pi^{-1}(p) = \{p\}$.

• $p \equiv 1 \bmod 4$: Nach Satz 3.3.3 gibt es dann $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2 = (a + \mathrm{i}b) \cdot (a - \mathrm{i}b)$. Durch Vertauschen von a und b und Vorzeichenwechsel kann man $0 \leq b \leq a$ erreichen. Da p prim ist, muss $b \neq 0$ gelten, und da $2 \neq p$ prim ist, gilt auch $b \neq a$, also $0 < b < a$. Die Elemente $a \pm \mathrm{i}b$ sind wegen $N(a \pm \mathrm{i}b) = a^2 + b^2 = p$ Primelemente, und wegen $0 < b < a$ folgt $a \pm \mathrm{i}b \in P_{\mathbb{Z}[\mathrm{i}]}$. Damit ist $p = (a + \mathrm{i}b) \cdot (a - \mathrm{i}b)$, wegen der Eindeutigkeit der Primfaktorzerlegung hat p keine weiteren Primteiler, und es folgt $\pi^{-1}(p) = \{a + \mathrm{i}b, a - \mathrm{i}b\}$. □

Es gibt also genau drei verschiedene Typen von Primzahlen in $\mathbb{N}$:

- Primzahlen $p \in \mathbb{N}$, die prim in $\mathbb{Z}[\mathrm{i}]$ bleiben, heißen **träge**.
- Primzahlen $p \in \mathbb{N}$, die in $\mathbb{Z}[\mathrm{i}]$ zwei verschiedene Primfaktoren haben, heißen **zerfallend**.
- Primzahlen $p \in \mathbb{N}$, die in $\mathbb{Z}[\mathrm{i}]$ einen Primfaktor mit Vielfachheit 2 haben, heißen **verzweigt**.

Beispiel 3.3.6. Ordnet man die Primelemente $u \in P_{\mathbb{Z}[i]}$ aufsteigend in $\pi(u) \in P_{\mathbb{Z}}$, so erhält man

$$P_{\mathbb{Z}[\mathrm{i}]} = \{1 + \mathrm{i}, 3, 2 + \mathrm{i}, 2 - \mathrm{i}, 7, 11, 3 + 2\mathrm{i}, 3 - 2\mathrm{i}, 4 + \mathrm{i}, 4 - \mathrm{i}, 19, \ldots\}$$

Abbildung 3.1 zeigt alle Primelemente $u \in P_{\mathbb{Z}[i]} \in P$ mit $N(u) \leq 50^2$.

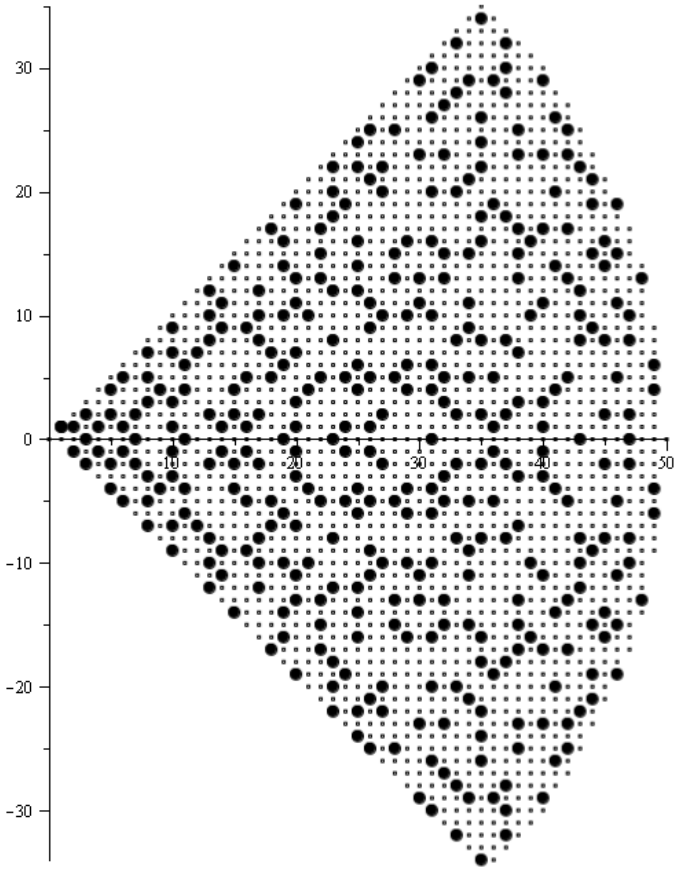


Abbildung 3.1: Die Primelemente $u \in P_{\mathbb{Z}[i]}$ mit Norm $N(u) \leq 50^2$.

3.4 Das quadratische Reziprozitätsgesetz

In diesem Abschnitt befassen wir uns mit den sogenannten *quadratischen Resten*, Zahlen in den Körpern $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{N}$, die sich als Quadrate $\overline{m}^2$ eines Elements $\overline{m} \in \mathbb{F}_p$ schreiben lassen. Quadratische Reste spielen eine wichtige Rolle in der Zahlentheorie, beispielsweise in der Untersuchung der p-adischen Zahlen und in diskreten Fouriertransformierten. Sie treten auch in der Kryptographie auf und liefern außerdem Primzahltests. Wir können diese Anwendungen in dieser Vorlesung nicht behandeln. Wir werden aber aus quadratischen Resten Aussagen über die Anzahl der Lösungen von quadratischen Gleichungen und von Ungleichungssystemen in den Körpern $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gewinnen. Damit lässt sich unter anderem die Irreduzibilität quadratischer Polynome in $\mathbb{F}_p[x]$ und die Verteilung von Primzahlen untersuchen.

Ausgangspunkt sind normierte quadratische Polynome $q = x^2 - \bar{b}x + \bar{c}$ im Körper $\mathbb{F}_p$ für Primzahlen $p \in \mathbb{N}$ und $\bar{b}, \bar{c} \in \mathbb{F}_p$. Der Fall $p = 2$ spielt dabei eine Sonderrolle und lässt sich leicht durch Ausprobieren behandeln. Ist $p \neq 2$, so gibt es ein multiplikatives Inverses $\bar{2}^{-1} \in \mathbb{F}_p$, und durch quadratische Ergänzung erhält man $q = x^2 - \bar{b}x + \bar{c} = (x - \bar{2}^{-1}\bar{b})^2 + \bar{c} - \bar{2}^{-2}\bar{b}^2$. Es reicht also, Polynome der Form $q = x^2 - \bar{a}$ mit $\bar{a} \in \mathbb{F}_p$ zu untersuchen. Im Fall $\bar{a} = \bar{0}$ gibt es wegen der Nullteilerfreiheit von $\mathbb{F}_p$ genau eine Nullstelle, nämlich $x = \bar{0}$. Wir können uns also auf die Restklassen zu p teilerfremder Zahlen beschränken. Die Bezeichnung quadratischer Rest wird dabei sowohl für die Restklassen selbst als auch für ihre Repräsentanten in $\mathbb{Z}$ benutzt.

Definition 3.4.1: Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Dann heißen eine ganze Zahl $a \in \mathbb{Z}$ mit $p \nmid a$ und ihre Restklasse $\bar{a} \in \mathbb{F}_p$ **quadratischer Rest** modulo p wenn es ein $x \in \mathbb{Z}$ gibt mit $x^2 \equiv a \bmod p$. Ansonsten nennt man a und $\bar{a}$ **quadratische Nichtreste** modulo p.

Beispiel 3.4.2.

1. Vielfache von p und $\bar{0} \in \mathbb{F}_p$ sind weder quadratische Reste noch Nichtreste modulo p.
2. Die Zahl $\bar{1} \in \mathbb{F}_p$ und damit alle $n \in \mathbb{Z}$ mit $n \equiv 1 \bmod p$ sind immer quadratische Reste, denn es gilt $\bar{1} \cdot \bar{1} = \bar{1}$.
3. In $\mathbb{F}_3$ gilt $\bar{1}^2 = \bar{2}^2 = \bar{1}$. Also ist $a \in \mathbb{Z}$ genau dann ein quadratischer Rest modulo 3, wenn $a \equiv 1 \bmod 3$ ist.
4. Die quadratischen Reste modulo 11 sind die Restklassen $\{\bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\}$.
   Denn es gilt $\bar{1}^2 = \overline{10}^2 = \bar{1}$, $\bar{2}^2 = \bar{9}^2 = \bar{4}$, $\bar{3}^2 = \bar{8}^2 = \bar{9}$, $\bar{4}^2 = \bar{7}^2 = \bar{5}$ und $\bar{5}^2 = \bar{6}^2 = \bar{3}$.

Indem wir das Quadrieren von Einheiten in $\mathbb{F}_p^\times$ als Gruppenendomorphismus $q : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ der Einheitengruppe $\mathbb{F}_p^\times$ auffassen, erkennen wir, dass die quadratischen Reste eine Untergruppe der Einheitengruppe bilden. Ebenso erkennt man, dass es immer genauso viele quadratische Reste in $\mathbb{F}_p^\times$ wie quadratische Nichtreste gibt.

Satz 3.4.3: Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Dann bilden die quadratischen Reste modulo p eine Untergruppe $Q_p \subseteq \mathbb{F}_p^\times$ vom Index 2. Insbesondere enthält $\mathbb{F}_p^\times$ genau $\frac{1}{2}(p-1)$ quadratische Reste und $\frac{1}{2}(p-1)$ Nichtreste.

Beweis:
Die Abbildung $\varphi_2 : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $a \mapsto a^2$ ist ein Gruppenhomomorphismus mit Bild Q_p und Kern $\ker(\varphi_2) = \{a \in \mathbb{F}_p \mid a^2 = \bar{1}\} = \{\pm\bar{1}\}$. Denn wegen der Nullteilerfreiheit von $\mathbb{F}_p$ hat die Gleichung $a^2 - \bar{1} = (a + \bar{1})(a - \bar{1}) = \bar{0}$ genau die Lösungen $\pm\bar{1}$. Damit ist $|Q_p| = |\mathbb{F}_p^\times|/|\ker(q)| = \frac{1}{2}(p-1)$ und $[\mathbb{F}_p^\times : Q_p] = |\mathbb{F}_p^\times|/|Q_p| = 2$. □

Um Aussagen darüber machen zu können, ob eine gegebene Zahl ein quadratischer Rest modulo einer Primzahl p ist, führen wir eine Abbildung von $\mathbb{Z}$ in die Menge $\{0, \pm 1\}$ ein, die eine ähnliche Rolle spielen wird, wie das Signum einer Permutation in der symmetrischen Gruppe. Dies ist das sogenannte *Legendresymbol*.

Definition 3.4.4: Sei $p \in \mathbb{N}$ eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann ist das **Legendresymbol** definiert durch:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist,} \\ 0 & \text{falls } p \mid a \end{cases}$$

Beispiel 3.4.5. Für $p = 11$ ist die Wertetabelle des Legendresymbols:

a	0	1	2	3	4	5	6	7	8	9	10
$\left(\frac{a}{p}\right)$	0	1	-1	1	1	1	-1	-1	-1	1	-1

Da eine Zahl $a \in \mathbb{Z}$ genau dann ein quadratischer Rest modulo p ist, wenn $\bar{a} \in \mathbb{F}_p^\times$ ein quadratischer Rest ist, und $\bar{a} = 0$ genau dann, wenn $p \mid a$, hängt das Legendresymbol nur von der Restklasse von a in $\mathbb{F}_p$ ab. Statt als eine Abbildung $\mathbb{Z} \to \{0, 1, -1\}$ können wir das Legendresymbol also auch als eine Abbildung $\mathbb{F}_p^\times \to C_2$ in die multiplikative Gruppe $C_2 = \{\pm 1\}$ auffassen. Diese Abbildung ist sogar ein Gruppenhomomorphismus.

Satz 3.4.6: Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Dann gilt:

1. Sind $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod p$, so ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ für alle $a, b \in \mathbb{Z}$.
3. Das Legendresymbol definiert einen Gruppenhomomorphismus $L : \mathbb{F}_p^\times \to C_2$, $\bar{a} \mapsto \left(\frac{a}{p}\right)$.

Beweis:
Die 1. Aussage ist offensichtlich und ebenso 2. für $p \mid a$ oder $p \mid b$. Da Q_p eine Untergruppe vom Index 2 in $\mathbb{F}_p^\times$ ist, ist Q_p ein Normalteiler und $F_p^\times / Q_p \cong C_2 = \{\pm 1\}$. Die kanonische Surjektion definiert dann einen surjektiven Gruppenhomomorphismus $L : \mathbb{F}_p^\times \to C_2$, der quadratische Reste auf das neutrale Element $1 \in C_2$ und quadratische Nichtreste auf -1 abbildet. Dieser stimmt offensichtlich für alle $a \in \mathbb{Z}$ mit $p \nmid a$ mit dem Legendresymbol überein. Damit folgt auch die 2. Aussage für $p \nmid a, b$. □

Ähnlich wie das Quadrieren einer Einheit einen Gruppenhomomorphismus von $\mathbb{F}_p^\times$ in die Untergruppe $Q_p \subseteq \mathbb{F}_p^\times$ der quadratischen Reste definiert, ist für jedes $q \in \mathbb{N}$ auch die Abbildung $\varphi_q : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $a \mapsto a^q$ ein Gruppenhomomorphismus. Der Kern und das Bild dieses Gruppenhomomorphismus lassen sich aber im allgemeinen weniger leicht bestimmen. Da $\mathbb{F}_p^\times$ nur die Restklassen von zu p teilerfremden Zahlen in $\mathbb{Z}$ enthält und es sich bei p um eine ungerade Primzahl handelt, können wir aus dem Satz von Euler (Korollar 3.1.6) und dem kleinen Satz von Fermat (Korollar 3.1.7) zumindest Aussagen über die Fälle $q = p - 1$ und $q = \frac{1}{2}(p-1)$ gewinnen. Dies liefert eine Verallgemeinerung des kleinen Satzes von Fermat.

Satz 3.4.7 (Eulerkriterium): Sei $p \in \mathbb{N}$ eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Beweis:
Für $p \mid a$ ist die Aussage offensichtlich. Für $p \nmid a$ ist $\varphi_q : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $a \mapsto a^q$ mit $q = \frac{1}{2}(p-1)$ ein Gruppenhomomorphismus. Da $\varphi_q(a)^2 = a^{2q} = a^{p-1} = \bar{1}$ nach Korollar 3.1.6, folgt auch $\varphi_q(\mathbb{F}_p^\times) \subseteq \{\pm\bar{1}\}$. Wäre $\varphi_q(\mathbb{F}_p^\times) \subsetneq \{\pm\bar{1}\}$, so müsste $\varphi_q(a) = \bar{1}$ für alle $a \in \mathbb{F}_p^\times$ gelten, da $\varphi_q(\mathbb{F}_p^\times) \subseteq \mathbb{F}_p^\times$ eine Untergruppe ist. Damit hätte das Polynom $x^q - \bar{1}$ genau $p-1 > q$ Nullstellen, ein Widerspruch zu Korollar 2.5.32. Also gilt $\varphi_q(\mathbb{F}_p^\times) = \{\pm\bar{1}\}$. Mit dem Homomorphiesatz folgt $|\ker(\varphi_q)| = |\mathbb{F}_p^\times|/|\varphi_q(\mathbb{F}_p^\times)| = |\mathbb{F}_p^\times|/2 = q$. Ist $a \in Q_p$, so gibt es ein $b \in \mathbb{F}_p^\times$ mit $a = b^2$, und mit Korollar 3.1.6 folgt wieder $\varphi_q(a) = b^{p-1} = \bar{1}$. Damit gilt $Q_p \subseteq \ker(\varphi_q)$ und wegen $|\ker(\varphi_q)| = |Q_p| = q$ folgt $Q_p = \ker(\varphi_q)$ und damit die Behauptung. □

Mit dem Eulerkriterium lässt sich eine Lösung der Gleichung $x^2 \equiv a \bmod p$ explizit angeben, wenn eine Lösung existiert, also wenn a ein quadratischer Rest ist. Ebenso lässt sich damit klären, für welche ungeraden Primzahlen p das Element $-\bar{1} \in \mathbb{F}_p^\times$ ein quadratischer Rest ist.

Korollar 3.4.8: Sei $p \equiv -1 \bmod 4$ eine Primzahl und $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$. Dann ist $x = a^{\frac{p+1}{4}}$ eine Lösung der Gleichung $x^2 \equiv a \bmod p$.

Beweis:
Nach Satz 3.4.7 ist $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) = 1 \bmod p$. Daraus folgt $x^2 = a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} \equiv a \bmod p$. □

Korollar 3.4.9 (Erster Ergänzungssatz): Für jede ungerade Primzahl $p \in \mathbb{N}$ gilt

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv \ \ 1 \bmod 4 \\ -1 & \text{falls } p \equiv -1 \bmod 4. \end{cases}$$

Damit ist -1 ein quadratischer Rest modulo p genau dann, wenn $p \equiv 1 \bmod 4$.

Um Legendresymbole effizient berechnen zu können, müssen wir uns zunächst genauer mit der Struktur der quadratischen Reste modulo p befassen. Diese können wir nach Satz 3.4.6 auch mit den Nebenklassen der Untergruppe $C_2 = \{\bar{1}, -\bar{1}\} \subseteq \mathbb{F}_p^\times$ identifizieren. Jede solche Nebenklasse ist von der Form $\{\bar{a}, -\bar{a}\}$ mit $\bar{a} \in \mathbb{F}_p^\times$. Für manche Anwendungen bietet es sich an, aus jeder Nebenklasse einen Repräsentanten zu wählen. Ein solches Repräsentantensystem der C_2-Nebenklassen bezeichnet man auch als *Halbsystem*.

Definition 3.4.10: Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Ein **Halbsystem modulo** p ist ein Repräsentantensystem der Nebenklassen in $\mathbb{F}_p^\times/C_2$, also eine Teilmenge $S \subseteq \mathbb{F}_p^\times$, die genau ein Element aus jeder C_2-Nebenklasse $\{\bar{a}, -\bar{a}\}$ enthält.

Da es in $\mathbb{F}_p^\times$ genau $\frac{1}{2}(p-1)$ C_2-Nebenklassen gibt, gibt es $2^{\frac{p-1}{2}}$ Halbsysteme. Ist S ein Halbsystem modulo p ist, so ist offensichtlich auch das Komplement $-S := \{-\bar{b} \mid \bar{b} \in S\}$ von S in $\mathbb{F}_p^\times$ wieder ein Halbsystem. Das Legendresymbol einer Zahl $a \in \mathbb{Z}$ modulo p lässt sich dann aus dem Schnitt der Halbsysteme $-S$ und $\bar{a}S$ bestimmen.

Satz 3.4.11 (Lemma von Gauß): Sei $p \in \mathbb{N}$ eine ungerade Primzahl und $S \subseteq \mathbb{F}_p^\times$ ein Halbsystem. Dann ist für jedes $a \in \mathbb{Z}$ mit $p \nmid a$ auch $\bar{a}S := \{\overline{ab} \in \mathbb{F}_p^\times \mid \bar{b} \in S\}$ wieder ein Halbsystem und

$$\left(\frac{a}{p}\right) = (-1)^h \quad \text{mit} \quad h = |(-S) \cap (\bar{a}S)|.$$

Beweis:
Da $p \nmid a$ ist $\bar{a} \in \mathbb{F}_p^\times$, und damit besteht $\bar{a}S$ für jedes Halbsystem S ebenfalls aus $\frac{p-1}{2}$ Elementen. Weiterhin gilt $\bar{a}S \cap (-\bar{a}S) = \varnothing$, und damit enthält $\bar{a}S$ maximal ein Element aus jeder Nebenklasse $\{\bar{b}, -\bar{b}\}$. Da $|\bar{a}S| = \frac{p-1}{2}$, enthält $\bar{a}S$ genau ein Element aus jeder C_2 Nebenklasse $\{\bar{b}, -\bar{b}\}$ und ist ein Halbsystem.

Für ein Halbsystem S bezeichnen wir mit $\pi(S) := \Pi_{\bar{x} \in S}\, \bar{x}$ das Produkt aller Elemente in S. Da $\bar{a}S = (S \cap \bar{a}S) \dot\cup ((-S) \cap \bar{a}S)$, gilt $\pi(\bar{a}S) = (-1)^{|(-S)\cap(\bar{a}S)|}\pi(S)$. Aus dem Eulerkriterium folgt

$$(-1)^{|(-S)\cap(\bar{a}S)|}\pi(S) = \pi(\bar{a}S) = \prod_{\bar{x}\in S} \overline{ax} = \bar{a}^{\frac{p-1}{2}} \prod_{\bar{x}\in S} \bar{x} \overset{3.4.7}{=} \left(\frac{a}{p}\right)\pi(S). \qquad \square$$

Korollar 3.4.12 (Zweiter Ergänzungssatz): Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Dann gilt

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \mod 8 \\ -1 & \text{falls } p \equiv \pm 3 \mod 8 \end{cases}$$

Beweis:
Für das Halbsystem $S = \{\bar{1}, \bar{2}, \ldots, \overline{\frac{p-1}{2}}\}$ gilt $\bar{2}S = \{\bar{2}, \bar{4}, \ldots, \overline{p-1}\}$. Damit ist $h = |(-S) \cap \bar{2}S|$ die Anzahl aller $x \in \mathbb{Z}$ mit $\frac{p+1}{2} \le 2x \le p-1$. Daraus folgt

$$|(-S) \cap 2S| = \left|\left\{x \in \mathbb{Z} \mid \frac{p}{4} < x < \frac{p}{2}\right\}\right| = \begin{cases} \frac{p-1}{4} & p \equiv 1 \mod 4 \\ \frac{p+1}{4} & p \equiv -1 \mod 4 \end{cases} = \begin{cases} \text{gerade} & p \equiv \pm 1 \mod 8 \\ \text{ungerade} & p \equiv \pm 3 \mod 8, \end{cases}$$

und mit Satz 3.4.11 folgt die Behauptung. $\square$

Das Argument aus dem Beweis des zweiten Ergänzungssatzes lässt sich auch auf andere zu p teilerfremde Primzahlen q anwenden. Auch in diesem Fall ist nach Satz 3.4.11 das Legendresymbol durch die Kardinalität der Menge $(-S) \cap (\bar{q}S)$ gegeben, und diese lässt sich durch Lösungen gewisser Ungleichungen charakterisieren. Diese Ungleichungen werden jedoch deutlich komplizierter als im Fall $q = 2$. Dennoch liefern sie eine interessante geometrische Interpretation des Legendresymbols und anschließend einen Satz, mit dem wir Legendresymbole effizient berechnen können.

Lemma 3.4.13: Sei $p = 2q + 1 \in \mathbb{N}$ eine ungerade Primzahl und $r \in \mathbb{N}$ mit $p \nmid r$. Dann ist $\left(\frac{r}{p}\right) = (-1)^h$, wobei h die Anzahl der Lösungen $(x, y) \in \mathbb{Z}^2$ folgender Ungleichungen ist:

$$0 < x < \frac{p+1}{2}, \qquad 0 < y < \frac{r+1}{2}, \qquad -\frac{p}{2} < rx - py < 0. \tag{3.4}$$

Beweis:
Wir betrachten das Halbsystem $S = \{\bar{1}, \ldots, \bar{q}\} \subseteq \mathbb{F}_p^\times$. Nach Satz 3.4.11 ist $\left(\frac{r}{p}\right) = (-1)^h$, wobei

$$\begin{aligned} h &= |(-S) \cap (\bar{r}S)| = |\{\bar{x} \in S \mid \overline{rx} \in -S\}| = |\{\bar{x} \in S \mid \overline{rx} \in \{\overline{q+1}, \ldots, \overline{p-1}\}\}| \\ &= |\{x \in \{1, \ldots, q\} \mid \overline{rx} \in \{\overline{q+1}, \ldots, \overline{p-1}\}\}| \end{aligned}$$

Nun gilt $x \in \{1, ..., q\}$ genau dann, wenn $x \in \mathbb{Z}$ mit

$$0 < x < \tfrac{1}{2}(p+1). \tag{3.5}$$

Ferner gilt $\overline{rx} \in \{\overline{q+1}, ..., \overline{p-1}\}$ genau dann, wenn es $a, y \in \mathbb{Z}$ gibt mit $1 \leq a \leq q$ und $rx = q + a + (y-1)p$. Auflösen der letzten Gleichung nach a und einsetzen in die Ungleichung für a liefert dann die Ungleichungen

$$-q \leq rx - py \leq -1. \tag{3.6}$$

Da es zu jedem x höchstens ein $y \in \mathbb{Z}$ gibt, das die Ungleichung (3.6) erfüllt, ist h die Anzahl der Paare $(x, y) \in \mathbb{Z}^2$, die die Ungleichungen (3.5) und (3.6) erfüllen. Umformen von (3.6) ergibt

$$rx + 1 \leq py \leq rx + q, \tag{3.7}$$

und mit (3.5) folgt dann aus (3.7)

$$0 < r + 1 \leq py \leq rq + q \leq (r+1)q < (r+1)\frac{p}{2} \quad \Leftrightarrow \quad 0 < y < \frac{r+1}{2}. \tag{3.8}$$

Die Ungleichungen (3.5), (3.7) und (3.8) sind dann wegen $rx - py \in \mathbb{Z}$ äquivalent zu (3.4). □

Aus diesem eher technischen Ergebnis zu Lösungen von Ungleichungen, ergibt sich ein Satz, der sehr hilfreich zur Berechnung des Legendresymbols ist, das sogenannte quadratische Reziprozitätsgesetz, das es erlaubt Zähler und Nenner im Legendresymbol zu vertauschen, sofern sie verschieden und beide ungerade sind.

Satz 3.4.14 (quadratisches Reziprozitätsgesetz):
Seien $p, q \in \mathbb{N}$ zwei verschiedene ungerade Primzahlen. Dann gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv q \equiv -1 \bmod 4. \end{cases}$$

Beweis:
Nach Lemma 3.4.13 ist $\left(\frac{q}{p}\right) = (-1)^{|X_p|}$ mit

$$X_p = \{(x, y) \in \mathbb{Z}^2 \mid 0 < x < \tfrac{p+1}{2},\ 0 < y < \tfrac{q+1}{2},\ -\tfrac{p}{2} < qx - py < 0\}.$$

Vertauschen wir p und q sowie Variablen x und y, so erhalten wir analog $\left(\frac{p}{q}\right) = (-1)^{|X_q|}$ mit

$$X_q = \{(x, y) \in \mathbb{Z}^2 \mid 0 < y < \tfrac{q+1}{2},\ 0 < x < \tfrac{p+1}{2},\ -\tfrac{q}{2} < py - qx < 0\}.$$

Da $-\frac{q}{2} < py - qx < 0$ äquivalent ist zu $0 < qx - qy < \frac{q}{2}$, gilt $X_p \cap X_q = \emptyset$. Außerdem folgt aus $x, y \in \mathbb{Z}$ mit $qx - py = 0$, dass $p \mid x$ und $q \mid y$, was den Ungleichungen $0 < y < \frac{q+1}{2}$ und $0 < x < \frac{p+1}{2}$ widerspricht. Damit ist dieser Fall schon durch die Ungleichungen $0 < y < \frac{q+1}{2}$ und $0 < x < \frac{p+1}{2}$ ausgeschlossen, und es ergibt sich

$$X := X_p \cup X_q = \{(x, y) \in \mathbb{Z}^2 \mid 0 < x < \tfrac{p+1}{2},\ 0 < y < \tfrac{q+1}{2},\ -\tfrac{p}{2} < qx - py < \tfrac{q}{2}\} \tag{3.9}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{|X_q|}(-1)^{|X_p|} = (-1)^{|X|}.$$

Zu untersuchen ist also, ob die Menge $X = X_p \cup X_q$ geradzahlig oder ungeradzahlig viele Elemente enthält. Dazu betrachten wir die Punktspiegelung von $\mathbb{R}^2$ im Punkt $P := (\frac{p+1}{4}, \frac{q+1}{4})$

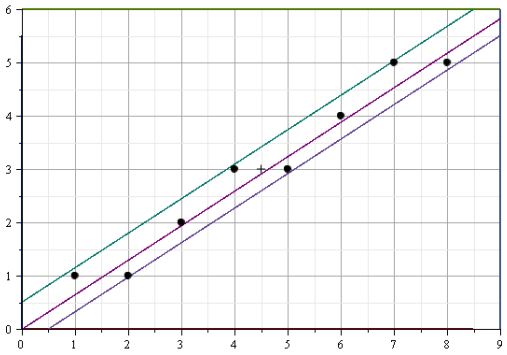
$$\varphi : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x, y) \mapsto \left(\tfrac{p+1}{2} - x, \tfrac{q+1}{2} - y\right).$$

Sie bildet die Menge X auf sich selbst ab, denn wegen p, q ungerade gilt $\varphi(x, y) \in \mathbb{Z}^2$ genau dann, wenn $(x, y) \in \mathbb{Z}^2$. Die ersten zwei Ungleichungen in (3.9) sind offensichtlich invariant unter φ und für die letzte ergibt sich

$$\begin{aligned} & -\tfrac{p}{2} < q(\tfrac{p+1}{2} - x) - p(\tfrac{q+1}{2} - y) < \tfrac{q}{2} \quad \Leftrightarrow \quad -\tfrac{p}{2} < -qx + py + \tfrac{q}{2} - \tfrac{p}{2} < \tfrac{q}{2} \\ \Leftrightarrow \quad & -\tfrac{q}{2} < -qx + py < \tfrac{p}{2} \quad \Leftrightarrow \quad -\tfrac{p}{2} < qx - py < \tfrac{q}{2} \end{aligned}$$

Da $\varphi(X) = X$, $\varphi^2 = \mathrm{id}$ und P der einzige Fixpunkt von φ ist, ist $|X|$ genau dann ungerade, wenn $P \in X$. Da P die Ungleichungen in (3.9) erfüllt, gilt dies genau dann, wenn $P \in \mathbb{Z}^2$. Dies ist offenbar genau dann der Fall, wenn $p \equiv -1 \bmod 4$ und $q \equiv -1 \bmod 4$ gilt. □

Beispiel 3.4.15.
Die Menge X für $p = 17$ und $q = 11$ und der Punkt P sind in der folgenden Grafik dargestellt



Man beachte die Linie $qx - py = 0$, die die Mengen X_p und X_q voneinander trennt. Nur die Vereinigung $X = X_p \cup X_q$ ist invariant unter einer Punktspiegelung an P.

Das quadratische Reziprozitätsgesetz kann gut zur Berechnung des Legendresymbols und damit zur Klärung der Frage verwendet werden, ob eine vorgegebene Zahl ein quadratischer Rest ist

Beispiel 3.4.16. Wir untersuchen, ob

$$x^2 \equiv 7 \bmod 19 \tag{3.10}$$

eine Lösung $x \in \mathbb{Z}$ hat. Dies ist genau dann der Fall, wenn $\bar{7}$ ein quadratischer Rest modulo 19 ist, also genau dann, wenn $\left(\frac{7}{19}\right) = 1$ gilt. Um das Legendresymbol zu berechnen, nutzt man das quadratische Reziprozitätsgesetz und Satz 3.4.6, 1. um die Argumente im Legendresymbol schrittweise durch kleinere Zahlen zu ersetzen, bis man den ersten oder zweiten Ergänzungssatz (Korollare 3.4.9 und 3.4.12) anwenden kann.

$$\left(\frac{7}{19}\right) \overset{3.4.14}{=} -\left(\frac{19}{7}\right) \overset{3.4.6,1.}{=} -\left(\frac{5}{7}\right) \overset{3.4.14}{=} -\left(\frac{7}{5}\right) \overset{3.4.6,1.}{=} -\left(\frac{2}{5}\right) \overset{3.4.12}{=} 1.$$

Damit hat (3.10) eine Lösung. Durch Ausprobieren sieht man, dass $x = 8$ eine Lösung ist.

Beispiel 3.4.16 ist von einer besonders einfachen Form, da bei der Berechnung im Zähler und Nenner jeweils nur Primzahlen auftauchen. Im allgemeinen kann der Zähler des Legendresymbols aber auch nicht-Primzahlen enthalten, und das quadratischen Reziprozitätsgesetz kann dann erst angewendet werden, nachdem man den Zähler in seine Primfaktoren faktorisiert und das Produkt der entsprechenden Legendresymbole gebildet hat. Um diese rechnerisch aufwändige Primfaktorzerlegung im Zähler zu vermeiden, bietet es sich an, die Definition des Legendresymbols zu erweitern, so dass im Nenner auch Nicht-Primzahlen auftreten können. Damit das quadratische Reziprozitätsgesetz seine Gültigkeit behalten kann und aus Symmetriegründen muss man dabei fordern, dass das resultierende Symbol auch im Nenner multiplikativ ist.

Definition 3.4.17: Seien $a, n \in \mathbb{Z}$ mit $n \geq 1$ ungerade und $n = p_1^{v_1} \dots p_s^{v_s}$ die Primfaktorzerlegung von n. Dann ist das **Jacobisymbol** definiert als

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{v_1} \dots \left(\frac{a}{p_s}\right)^{v_s}.$$

Beispiel 3.4.18.

1. Es gilt $\left(\frac{a}{1}\right) = 1$ für alle $a \in \mathbb{Z}$, denn in diesem Fall gilt $v_1 = ... = v_s = 0$ und $z^0 = 1$ für alle $z \in \mathbb{Z} \setminus \{0\}$.
2. Aus der Definition des Jacobisymbols erhält man mit dem zweiten Ergänzungssatz 3.4.12 $\left(\frac{2}{21}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{7}\right) = (-1)(1) = -1$.

Wir zeigen nun, dass auch das Jacobisymbol das quadratische Reziprozitätsgesetz erfüllt, sowie die meisten anderen bekannten Identitäten für das Legendresymbol. Bis auf die Ergänzungssätze und das quadratische Reziprozitätsgesetz ergibt sich das direkt aus der Definition.

Satz 3.4.19 (Eigenschaften des Jacobisymbols):

Seien $a, b, m, n \in \mathbb{Z}$ und $m, n \geq 1$ ungerade. Dann gilt

1. Wertebereich: $\left(\frac{a}{n}\right) \in \{0, 1, -1\}$.
2. Trivialität: $\left(\frac{a}{n}\right) = 0$ genau dann, wenn $\mathrm{ggT}(a, n) \neq 1$.
3. Periodizität im Zähler: Aus $a \equiv b \bmod n$ folgt $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
4. Multiplikativität im Zähler: $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
5. Multiplikativität im Nenner: $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
6. Erster Ergänzungssatz: $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
7. Zweiter Ergänzungssatz: $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.
8. Quadratisches Reziprozitätsgesetz: $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$.
9. Quadratische Reste: Wenn n **prim** ist und $n \nmid a$, dann ist a genau dann ein quadratischer Rest modulo n, wenn $\left(\frac{a}{n}\right) = 1$ ist.

Beweis:
Aussagen 1. -5. und 9. folgen direkt aus der Definition 3.4.17 und den entsprechenden Aussagen für das Legendresymbol (vgl. Definition 3.4.4 und Satz 3.4.6)

Für Aussagen 6.-8. betrachten wir die Gruppenhomomorphismen

$$\varepsilon_4 : (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\},\ \bar{n} \mapsto (-1)^{\frac{n-1}{2}}$$
$$\varepsilon_8 : (\mathbb{Z}/8\mathbb{Z})^\times \to \{\pm 1\},\ \bar{n} \mapsto (-1)^{\frac{n^2-1}{8}}.$$

Aus $n \equiv m \bmod 4$ folgt $2 \mid \frac{1}{2}(n-m)$, und aus $n \equiv m \bmod 8$ folgt $2 \mid \frac{1}{8}(n^2-m^2)$. Damit sind diese Abbildungen wohldefiniert. Durch direktes Nachrechnen ergibt sich, dass es sich um Gruppenhomomorphismen handelt.

Wir beweisen die Aussagen 6.-8. durch Induktion über n.
Für $n = 1$ folgen sie direkt aus Beispiel 3.4.18, 1. und aus Definition des Legendresymbols, denn

$$\left(\frac{-1}{1}\right) = \left(\frac{2}{1}\right) = \left(\frac{1}{m}\right) = 1 = (-1)^0.$$

Sei nun $n > 1$. Da n nach Voraussetzung ungerade ist, hat dann n einen ungeraden Primfaktor p. Wir setzen $q = n/p$. Dann folgt aus den Ergänzungssätzen und der Induktionsvoraussetzung

6. $$\left(\frac{-1}{n}\right) = \left(\frac{-1}{pq}\right) \overset{5.}{=} \left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right) \overset{IV}{=} \varepsilon_4(p)\varepsilon_4(q) = \varepsilon_4(pq) = \varepsilon_4(n) = (-1)^{\frac{n-1}{2}}.$$

7. $$\left(\frac{2}{n}\right) = \left(\frac{2}{pq}\right) \overset{5.}{=} \left(\frac{2}{p}\right)\left(\frac{2}{q}\right) \overset{IV}{=} \varepsilon_8(p)\varepsilon_8(q) = \varepsilon_8(pq) = \varepsilon_8(n) = (-1)^{\frac{n^2-1}{8}}.$$

Ist $\mathrm{ggT}(m,n) \neq 1$, so ist 8. trivialerweise erfüllt, denn dann gilt nach 2. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 0$. Sind m, n beide prim, so gilt 8. nach dem quadratischen Reziprozitätsgesetz. Ist $m = 2m' + 1$ prim mit $\mathrm{ggT}(m,n) = 1$ und p ein nichttrivialer Primteiler von n mit $n = pq$, so folgt

$$\begin{aligned}\left(\frac{m}{n}\right) = \left(\frac{m}{pq}\right) &\overset{5.}{=} \left(\frac{m}{p}\right)\left(\frac{m}{q}\right) \overset{IV}{=} \varepsilon_4(p)^{m'}\left(\frac{p}{m}\right)\varepsilon_4(q)^{m'}\left(\frac{q}{m}\right) \overset{4.}{=} (\varepsilon_4(p)\cdot\varepsilon_4(q))^{m'}\left(\frac{n}{m}\right) \qquad (3.11)\\ &= \varepsilon_4(n)^{m'}\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right).\end{aligned}$$

Damit ist 8. für beliebige $n \geq 1$ ungerade und Primzahlen m bewiesen. Analog folgt es auch für Primzahlen n und beliebige $m \geq 1$ ungerade. Durch Faktorisieren der Zähler und Nenner der Jacobisymbole ergibt sich dann (3.11) für beliebige $n \geq 1$ ungerade, und 8. ist bewiesen. □

Das Jacobisymbol und damit auch das Legendresymbol lässt sich nun schnell durch einen Algorithmus berechnen, der dem Euklidischen Algorithmus ähnelt. Dazu wendet man abwechselnd das quadratische Reziprozitätsgesetz und die Periodizität des Jacobi-Symbols im Zähler an. Erhält man dabei ein Jacobi-Symbol, dessen Zähler oder Nenner durch zwei teilbar ist, so muss man vor Anwendung des quadratischen Reziprozitätsgesetzes die Zweierpotenzen im Zähler oder Nenner abspalten und das entsprechende Jacobisymbol mit den zweiten Ergänzungssatz berechnen. Am Ende der Rechnung ergibt sich dann der Wert mit dem ersten oder zweiten Ergänzungssatz.

Beispiel 3.4.20. Es gilt:

$$\begin{aligned}&\left(\frac{397}{1009}\right) \overset{8.}{=} \left(\frac{1009}{397}\right) \overset{3.}{=} \left(\frac{215}{397}\right) \overset{8.}{=} \left(\frac{397}{215}\right) \overset{3.}{=} \left(\frac{182}{215}\right) \overset{4.}{=} \left(\frac{2}{215}\right)\left(\frac{91}{215}\right)\\ &\overset{7.}{=} \left(\frac{91}{215}\right) \overset{8.}{=} -\left(\frac{215}{91}\right) \overset{3.}{=} -\left(\frac{33}{91}\right) \overset{8.}{=} -\left(\frac{91}{33}\right) \overset{3.}{=} -\left(\frac{25}{33}\right) \overset{8.}{=} -\left(\frac{33}{25}\right)\\ &\overset{3.}{=} -\left(\frac{8}{25}\right) \overset{4.}{=} -\left(\frac{2}{25}\right)\left(\frac{2}{25}\right)\left(\frac{2}{25}\right) \overset{1.}{=} -\left(\frac{2}{25}\right) \overset{4.}{=} -\left(\frac{2}{5}\right)\left(\frac{2}{5}\right) \overset{1.}{=} -1,\end{aligned}$$

wobei in 7. die Identität $215^2 - 1 = (215+1)(215-1) = 216 \cdot 214 \equiv 0 \bmod 16$ benutzt wurde.

Eine interessante Konsequenz des quadratischen Reziprozitätsgesetzes ist die Periodizität des Jacobisymbols im *Nenner*, die ebenfalls in konkreten Rechnungen hilfreich sein kann. Diese nimmt im Fall $a \equiv 1 \bmod 4$ eine besonders einfache Form an.

Satz 3.4.21: Seien $m, n \in \mathbb{N}$ ungerade. Dann gilt für alle $a \in \mathbb{Z}$:

1. Aus $m \equiv n \bmod 4a$ folgt $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$.
2. Ist $a \equiv 1 \bmod 4$, so folgt $\left(\frac{a}{m}\right) = \left(\frac{m}{|a|}\right)$.

Beweis:
1. Für $a = 0$ ist die Aussage trivial. Sind $a \neq 0$ und m nicht teilerfremd, so gibt es eine ungerade Primzahl p, die m und a teilt, und wegen $m \equiv n \bmod a$ teilt p dann auch n. Damit gilt $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right) = 0$. Sind m und n teilerfremd zu a, so können wir a faktorisieren als $a = (-1)^e \cdot 2^\mu \cdot b$ mit $e \in \{0, 1\}$, $\mu \geq 0$ und $b > 0$ ungerade. Nach dem quadratischen Reziprozitätsgesetz und den Ergänzungssätzen gilt dann

$$\left(\frac{a}{m}\right) \overset{3.4.19,\,4}{=} \left(\frac{-1}{m}\right)^e \left(\frac{2}{m}\right)^\mu \left(\frac{b}{m}\right) \overset{3.4.19,\,6,7,8}{=} (-1)^{e\frac{m-1}{2}} (-1)^{\mu\frac{m^2-1}{8}} (-1)^{\frac{m-1}{2}\frac{b-1}{2}} \left(\frac{m}{b}\right) = (-1)^{N(m)} \left(\frac{m}{b}\right)$$

$$N(m) = \tfrac{1}{4}(m-1)\left(2e + (b-1)\right) + \tfrac{\mu}{8}(m^2-1). \tag{3.12}$$

Ist $m \equiv n \bmod 4a$, so folgt $m \equiv n \bmod b$ und damit $\left(\frac{m}{b}\right) = \left(\frac{n}{b}\right)$ nach Satz 3.4.19, 3. Für ungerades a ist $\mu = 0$ und $m \equiv n \bmod 4$. Daraus folgt $N(m) \equiv N(n) \bmod 2$ und damit die Behauptung. Ist a gerade, so gilt $8 \mid 4a$ und damit $m \equiv n \bmod 8$. Daraus folgt wieder

$$N(m) - N(n) = \tfrac{1}{4}(m-n)(2e + b - 1) + \tfrac{\mu}{8}(m^2 - n^2) \equiv 0 \bmod 2.$$

2. Ist $a \equiv 1 \bmod 4$, so ist a ungerade, und wir können a faktorisieren als $a = (-1)^e \cdot b$ mit $b = |a| > 0$ ungerade. Aus $a = 1 \bmod 4$ folgt dann $b \equiv (-1)^e \bmod 4$ und

$$\tfrac{1}{2}(b-1) \equiv \tfrac{1}{2}((-1)^e - 1) \equiv e \bmod 2.$$

Also ist $e + \frac{b-1}{2}$ und damit auch $N(m)$ aus (3.12) gerade, und aus (3.12) folgt die Behauptung. □

Eine wichtige Anwendung des Legendre- und Jacobisymbols ist die Untersuchung der Frage, ob ein quadratisches Polynom $q = x^2 - bx + c$ in $\mathbb{F}_p[x]$ eine Nullstelle besitzt. Ist $p = 2$, so lässt sich das am einfachsten durch Probieren ermitteln. Ansonsten kann man das Problem mit Hilfe der Legendresymbole und mit quadratischer Ergänzung lösen. Denn dann besitzt $\bar{2} \in \mathbb{F}_p$ ein multiplikatives Inverses d, und es gilt $q = x^2 - bx + c = (x - db)^2 + c - d^2b^2$. Alternativ kann man auch die Mitternachtsformel benutzen, die für $p \neq 2$ ihre Gültigkeit behält und besagt, dass ein Polynom $q = ax^2 + bx + c$ genau dann eine Nullstelle in $\mathbb{F}_p$ hat, wenn $b^2 - 4ac$ ein quadratischer Rest in $\mathbb{F}_p$ ist.

Beispiel 3.4.22.

1. Die Zahl $a = -6$ ist genau dann quadratischer Rest modulo einer Primzahl p, wenn $p \equiv 1, 5, 7, 11 \bmod 24$ ist. Das Polynom $f(x) = x^2 + 6$ ist also genau dann irreduzibel modulo p, wenn $p \equiv 13, 17, 19, 23 \bmod 24$ ist.

   Denn es gilt $\mathrm{ggT}(p, 24) > 1$ genau dann, wenn $\mathrm{ggT}(p, 6) > 1$. Ansonsten ist $p \equiv q \bmod 24$ für ein $q \in \{1, 5, 7, 11, 13, 17, 19, 23\}$, und es folgt

$$\left(\frac{-6}{p}\right) \overset{3.4.21}{=} \left(\frac{-6}{q}\right) \overset{3.4.19,\,4}{=} \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)\left(\frac{3}{q}\right) \overset{3.4.19,\,6,7}{=} (-1)^{\frac{q-1}{2}} (-1)^{\frac{q^2-1}{8}} \left(\frac{3}{q}\right) \overset{3.4.19,\,8}{=} (-1)^{\frac{q^2-1}{8}} \left(\frac{q}{3}\right)$$

$$= \begin{cases} (-1)^{\frac{q^2-1}{8}} & q \equiv 1 \bmod 3 \\ (-1)^{\frac{q^2-1}{8}+1} & q = -1 \bmod 3. \end{cases}$$

2. Das Polynom x^2-5 ist genau dann in $\mathbb{F}_p[x]$ irreduzibel, wenn $p \neq 2$ und $p \equiv \pm 2 \bmod 5$ gilt. Für $p=2$ ist offensichtlich $x^2-5 = x^2-1$ reduzibel, da $x=1$ eine Nullstelle ist, und für $p=5$ ist $\bar{0}$ eine Nullstelle. Ist $p \notin \{2,5\}$, so ist $p = q \bmod 5$ für ein $q \in \{1,2,3,4\}$. Da $5 \equiv 1 \bmod 4$ folgt dann

$$\left(\frac{5}{p}\right) \overset{3.4.19,8.}{=} \left(\frac{p}{5}\right) \overset{3.4.19,3}{=} \left(\frac{q}{5}\right) = \begin{cases} 1 & q = 1,4 \\ -1 & q = 2,3 \end{cases}.$$

3. Das Polynom $f = x^2 - 7x + 11$ ist irreduzibel in $\mathbb{F}_p[x]$ genau dann, wenn $p \equiv \pm 2 \bmod 5$ gilt. Denn es gilt $b^2 - 4ac = 49 - 44 = 5$, und nach 2. ist 5 kein Quadrat in $\mathbb{F}_p$ genau dann, wenn $p = \pm 2 \bmod 5$ ist. Für $p=2$ ist $f = x^2 - x + 1$ und hat keine Nullstelle in $\mathbb{F}_2$.

Eine weitere wichtige Anwendung von Legendre- und Jacobisymbolen ist, dass sie es einem erlauben, Aussagen über die Verteilung von Primzahlen zu machen. So kann man mit Hilfe der Legendresymbole zeigen, dass in bestimmten Restklassen jeweils unendlich viele Primzahlen enthalten sind. Wir zeigen dies für die Restklassen modulo 8.

Satz 3.4.23: In jeder der Mengen $8\mathbb{Z}+1$, $8\mathbb{Z}+3$, $8\mathbb{Z}+5$ und $8\mathbb{Z}+7$ sind unendlich viele Primzahlen enthalten.

Beweis:
1. Angenommen, die Aussage ist falsch. Dann gibt es ein $k \in \{1,3,5,7\}$ und ein $B \in \mathbb{N}$, so dass $p \leq B$ für alle Primzahlen $p \in 8\mathbb{Z}+k$. Wir setzen

$$U := \prod_{\substack{m \in \mathbb{N}, m \leq B \\ m \text{ ungerade}}} m \qquad N := \begin{cases} (2U)^4 + 1 & \text{für } k = 1, \\ U^2 + 2 & \text{für } k = 3, \\ U^2 + 4 & \text{für } k = 5, \\ 8U^2 - 1 & \text{für } k = 7 \end{cases}$$

und zeigen, dass $N \equiv k \bmod 8$ ist. Als Produkt von ungeraden Zahlen ist U ungerade, also von der Form $U = 2n+1$ mit $n \in \mathbb{N}$. Es folgt $U^2 = (2n+1)^2 = 4n^2+4n+1 = 4n(n+1)+1 \equiv 1 \bmod 8$, denn entweder n oder $n+1$ ist gerade und damit ist $4n(n+1)$ durch 8 teilbar. Daraus folgt:

$$N \equiv \begin{cases} (2 \cdot 1)^4 + 1 \equiv 1 \bmod 8 & \text{für } k = 1, \\ 1^2 + 2 \equiv 3 \bmod 8 & \text{für } k = 3, \\ 1^2 + 4 \equiv 5 \bmod 8 & \text{für } k = 5, \\ 8 \cdot 1^2 - 1 \equiv 7 \bmod 8 & \text{für } k = 7. \end{cases}$$

2. Wir zeigen, dass für jeden Primteiler p von N gilt $p > B$: Da N ungerade ist, muss jeder Primteiler p von N ungerade sein. Wäre nun p ein Primteiler von N mit $p \leq B$, so würde p im Produkt U auftauchen. daraus ergäbe sich $U = 0 \bmod p$ und im Widerspruch zu $p \mid N$

$$N \equiv \begin{cases} 1 \bmod p & \text{für } k = 1, \\ 2 \bmod p & \text{für } k = 3, \\ 4 \bmod p & \text{für } k = 5, \\ -1 \bmod p & \text{für } k = 7. \end{cases}$$

3. Es reicht nun, zu zeigen, dass N einen Primteiler p mit $p \equiv k \bmod 8$ besitzt. Aus 2. folgt dann $p > B$, und wir erhalten einen Widerspruch zur Annahme, dass alle Primzahlen $q \in 8\mathbb{Z}+k$ die Bedingung $q \leq B$ erfüllen. Die Existenz eines solchen Primteilers p zeigen wir für die vier Fälle $k = 1, 3, 5, 7$ separat:

• $k = 1$: Für jeden Primteiler p von $N = (2U)^4 + 1$ gilt $(2U)^4 \equiv -1 \bmod p$. Damit hat die Restklasse von $2U$ Ordnung 8 in $\mathbb{F}_p^\times$. Nach dem Satz von Lagrange muss 8 also die Gruppenordnung $|\mathbb{F}_p^\times| = p - 1$ teilen. Es folgt $p \equiv 1 \bmod 8$.

• $k = 3$: Für jeden Primteiler p von $N = U^2 + 2$ gilt $U^2 \equiv -2 \bmod p$, und damit ist -2 ein quadratischer Rest modulo p. Mit den Ergänzungssätzen folgt für das Legendresymbol

$$1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \overset{3.4.19,\,6,7}{=} (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p^2+4p-5}{8}}$$

Nach Korollar 3.4.9 und 3.4.12 muss damit $p \equiv 1 \bmod 4$ und $p \equiv \pm 1 \bmod 8$, also $p \equiv 1 \bmod 8$ gelten, oder $p \equiv -1 \bmod 4$ und $p \equiv \pm 3 \bmod 8$ und damit $p \equiv 3 \bmod 8$. Wäre $p \equiv 1 \bmod 8$ für alle Primteiler von N, so wäre auch $N \equiv 1 \bmod 8$, im Widerspruch zu $N \equiv k = 3 \bmod 8$. Also existiert mindestens ein Primteiler p von N mit $p \equiv 3 \bmod 8$.

• $k = 5$: Für jeden Primteiler p von $N = U^2 + 4$ gilt $U^2 \equiv -4 \bmod p$, und damit ist -4 ein quadratischer Rest modulo p. Für das Legendresymbol folgt:

$$1 = \left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2 = \left(\frac{-1}{p}\right) \overset{3.4.19,\,6}{=} (-1)^{\frac{p-1}{2}}.$$

Mit dem ersten Ergänzungssatz (Korollar 3.4.9) folgt $p \equiv 1 \bmod 4$, also $p \equiv 1 \bmod 8$ oder $p \equiv 5 \bmod 8$. Wäre $p \equiv 1 \bmod 8$ für alle Primteiler von N, so wäre auch $N \equiv 1 \bmod 8$, im Widerspruch zu $N \equiv k = 5 \bmod 8$. Also existiert mindestens ein Primteiler p von N mit $p \equiv 5 \bmod 8$.

• $k = 7$: Für jeden Primteiler p von $N = 8U^2 - 1$ gilt $8U^2 \equiv 1 \bmod p$, und daraus folgt $16U^2 = (4U)^2 \equiv 2 \bmod p$. Also ist 2 ein quadratischer Rest modulo p und $\left(\frac{2}{p}\right) = 1$. Der zweite Ergänzungssatz 3.4.12 liefert $p \equiv 1 \bmod 8$ oder $p \equiv 7 \bmod 8$. Wäre $p \equiv 1 \bmod 8$ für alle Primteiler von N, so wäre auch $N \equiv 1 \bmod 8$, im Widerspruch zu $N \equiv k = 7 \bmod 8$. Also existiert mindestens ein Primteiler p von N mit $p \equiv 7 \bmod 8$. □

Eine weitere wichtige Anwendung des Jacobisymbols ist ein nützlicher Primzahltest, der *Solovay-Strassen-Primzahltest*. Er beruht auf der Beobachtung, dass sich das Eulerkriterium

$$a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \mod n \qquad \text{für } n \in \mathbb{N} \text{ prim} \tag{3.13}$$

nicht auf die Jacobisymbole von Nicht-Primzahlen $n \in \mathbb{N}$ verallgemeinert. Solovay und Strassen haben bewiesen, dass das Eulerkriterium für eine Nichtprimzahl $n > 1$ mindestens für die Hälfte aller Restklassen $a \in \mathbb{Z}/n\mathbb{Z}$ nicht erfüllt ist. Indem man für zufällig gewählt Zahlen $a \in \{1, ..., n-1\}$ zunächst $\mathrm{ggT}(a, n)$ und für $\mathrm{ggT}(a, n) = 1$ auch die Jacobisymbole $\left(\frac{a}{n}\right)$ und $a^{\frac{n-1}{2}}$ modulo n berechnet, findet man so entweder (i) eine Zahl mit $\mathrm{ggT}(a, n) > 1$, woraus man schließen kann, dass n keine Primzahl ist, (ii) eine Zahl a die (3.13) nicht erfüllt, woraus man ebenfalls schließen kann, dass n keine Primzahl ist, oder (iii) für alle getesteten a gilt $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$. Nachdem man N zufällig gewählte Zahlen aus $\{1, ..., n-1\}$ getestet hat,

weiss man dann, dass die Wahrscheinlichkeit, dass n eine Primzahl ist, mindestens $1 - 2^{-N}$ ist. Der Test ist halb-probabilistisch, weil er eine definitive Aussage darüber liefert, dass n keine Primzahl ist, aber nur Wahrscheinlichkeiten dafür, dass n eine Primzahl ist.

Anwendung 3.4.24 (**Solovay-Strassen-Primzahltest**)**:**

1. Wähle zufällig eine Restklasse $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.
2. Berechne $d := \mathrm{ggT}(a, n)$. Wenn $d \neq 1$, ist n nicht prim. Stop.
3. Berechne beide Seiten von (3.13). Beides ist effektiv möglich. Wenn sie nicht gleich sind, ist n nicht prim. Stop.
4. Wiederhole die ersten drei Schritte N mal.
5. Bricht der Test nicht ab, so ist n prim mit einer Wahrscheinlichkeit von $\geq 1 - 2^{-N}$.

Anhang A

A.1 Die komplexen Zahlen

In diesem Appendix versammeln wir ohne Beweis einige wichtige Definitionen, Sätze und Rechenregeln für komplexe Zahlen. Die komplexen Zahlen werden eingeführt, indem wir auf dem reellen Vektorraum $\mathbb{R}^2$ eine Multiplikation definieren, die ihm die Struktur eines Körpers verleiht. Dass dies tatsächlich einen Körper liefert, ergibt sich durch direktes Nachrechnen der Körperaxiome.

Satz A.1.1: Die Menge $\mathbb{R}^2$ mit den Verknüpfungen $+, \cdot : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$,

$$(a,b)+(c,d) := (a+c, b+d) \qquad (a,b)\cdot(c,d) := (ac-bd, ad+bc) \qquad \forall a,b,c,d \in \mathbb{R}$$

ist ein Körper. Er wird als der Körper der **komplexen Zahlen** und mit $\mathbb{C}$ bezeichnet. Er enthält den Körper $\mathbb{R}$ der reellen Zahlen als Teilkörper $\mathbb{R} \times \{0\} \subseteq \mathbb{C}$.

Die Notation (a,b) für komplexe Zahlen ist sperrig und unübersichtlich. Man schreibt komplexe Zahlen als reelle Linearkombinationen der Basisvektoren $1 := (1,0)$ und $\mathrm{i} := (0,1)$ als $a + \mathrm{i}b := a \cdot (1,0) + b \cdot (0,1) = (a,b)$ für $a, b \in \mathbb{R}$. Damit erhält man $1^2 = (1,0)^2 = 1$ und $\mathrm{i}^2 = (0,1)\cdot(0,1) = -1$, und die Addition und Multiplikation in $\mathbb{C}$ bekommen die Form

$$\begin{aligned}(a+\mathrm{i}b)+(c+\mathrm{i}d) &= (a+c)+\mathrm{i}(b+d)\\ (a+\mathrm{i}b)(c+\mathrm{i}d) &= ac+\mathrm{i}(bc+ad)+\mathrm{i}^2bd = (ac-bd)+\mathrm{i}(ad+bc).\end{aligned} \tag{A.1}$$

Wir fassen die wichtigsten Bezeichnungen für komplexe Zahlen in einer Definition zusammen.

Definition A.1.2: Im Körper $\mathbb{C}$ der komplexen Zahlen benutzt man die Bezeichnung $x + \mathrm{i}y$ für (x,y) und Formel (A.1) für die Verknüpfungen. Das Element $\mathrm{i} := (0,1)$ mit $\mathrm{i}^2 = -1$ heißt **imaginäre Einheit**, und eine Zahl der Form $\mathrm{i}y$, $y \in \mathbb{R}$ heißt **imaginär**. Für $z = x + \mathrm{i}y \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ definiert man

- den **Realteil** $\mathrm{Re}(z) := x \in \mathbb{R}$,
- den **Imaginärteil** $\mathrm{Im}(z) := y \in \mathbb{R}$,
- die zu z **komplex konjugierte** Zahl $\overline{z} := x - \mathrm{i}y \in \mathbb{C}$,
- den **Betrag** $|z| := \sqrt{x^2+y^2} = \sqrt{z\overline{z}} \in \mathbb{R}$,

- das **Argument** $\arg(z) \in [0, 2\pi)$ von $z = x + \mathrm{i}y \in \mathbb{C} \setminus \{0\}$ als den eindeutigen Winkel mit

$$\cos(\arg(z)) = \frac{\mathrm{Re}(z)}{|z|} = \frac{x}{\sqrt{x^2+y^2}} \qquad \sin(\arg(z)) = \frac{\mathrm{Im}(z)}{|z|} = \frac{y}{\sqrt{x^2+y^2}}.$$

Lemma A.1.3:

1. Die komplexe Konjugation erfüllt die Bedingungen:

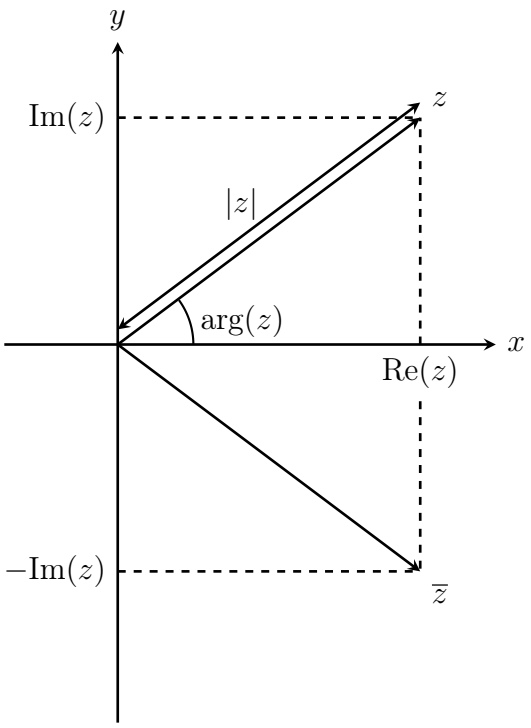
$$\overline{z+w} = \overline{z} + \overline{w}, \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}, \quad \overline{x} = x, \quad \overline{\mathrm{i}x} = -\mathrm{i}x, \quad \overline{\overline{z}} = z \qquad \forall z, w \in \mathbb{C}, x \in \mathbb{R}$$

2. Für alle $z \in \mathbb{C}$ gilt:

$$\mathrm{Re}(z) = \tfrac{1}{2}(z + \overline{z}), \quad \mathrm{Im}(z) = \tfrac{\mathrm{i}}{2}(\overline{z} - z), \quad z \cdot \overline{z} = |z|^2.$$

Beispiel A.1.4. Wir bestimmen $\mathrm{Re}(1/z)$ und $\mathrm{Im}(1/z)$ für $z = 1 + 2\mathrm{i}$. Dazu erweitern wir den Bruch mit dem komplex Konjugierten des Nenners:

$$\frac{1}{z} = \frac{1}{1+2\mathrm{i}} = \frac{1-2\mathrm{i}}{(1-2\mathrm{i})(1+2\mathrm{i})} = \frac{1-2\mathrm{i}}{1-4\mathrm{i}^2} = \frac{1-2\mathrm{i}}{5} \quad \Rightarrow \quad \mathrm{Re}(1/z) = \tfrac{1}{5}, \mathrm{Im}(1/z) = -\tfrac{2}{5}.$$

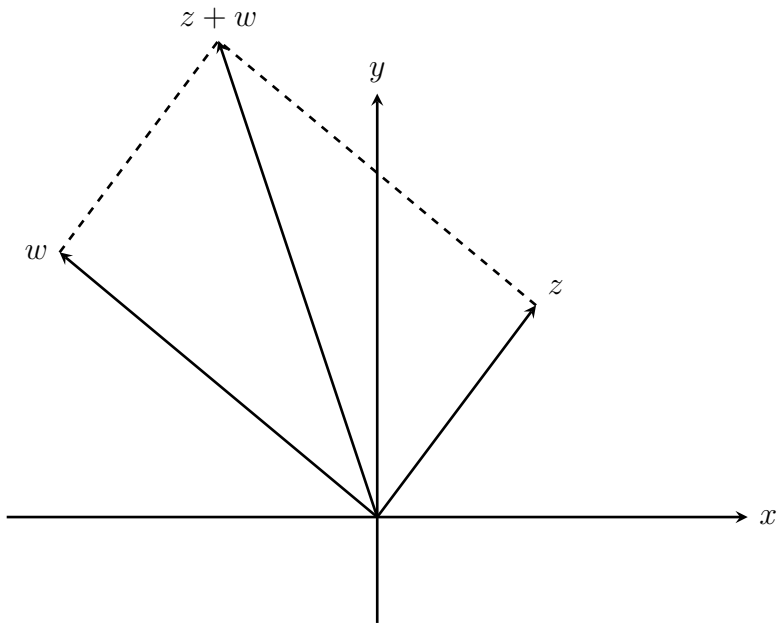


Das Argument einer komplexen Zahl $z \in \mathbb{C}$ ist per Definition der Winkel, den der zugehörige Vektor mit der positiven x-Achse einschließt und der Betrag die euklidische Norm dieses Vektors. Die Addition in $\mathbb{C}$ stimmt offensichtlich mit der Vektoraddition im $\mathbb{R}^2$ überein und lässt sich mittels der Parallelogrammregel visualisieren. Bei der Multiplikation komplexer Zahlen multiplizieren sich ihre Beträge und addieren sich ihre Argumente, denn aus den Additionsformeln

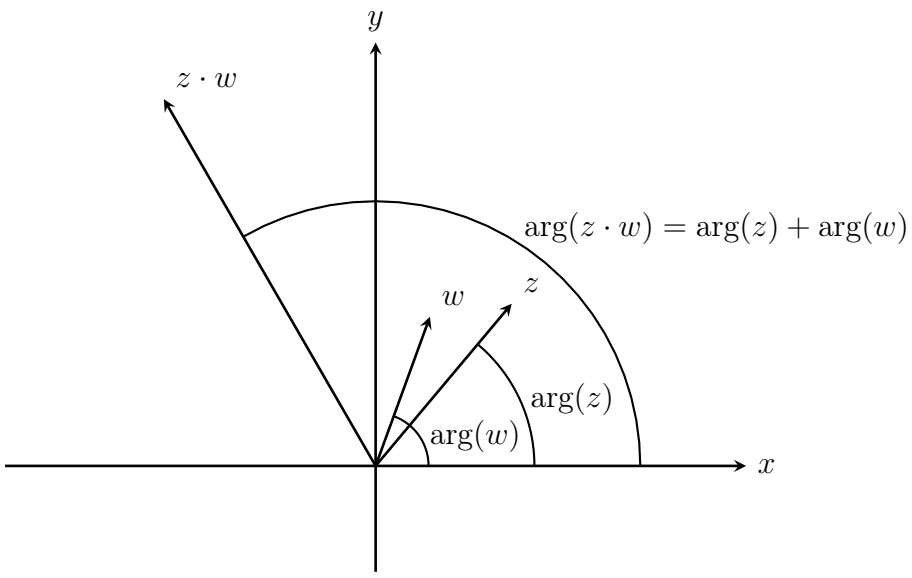
für Sinus und Kosinus ergibt sich für zwei komplexe Zahlen $z = |z|(\cos\arg(z) + \mathrm{i}\sin\arg(z))$ und $w = |w|(\cos\arg(w) + \mathrm{i}\sin\arg(w))$

$$\begin{aligned} z \cdot w &= |z|(\cos\arg(z) + \mathrm{i}\sin\arg(z)) \cdot |w|(\cos\arg(w) + \mathrm{i}\sin\arg(w)) \\ &= |z||w|(\cos\arg(z)\cos\arg(w) - \sin\arg(z)\sin\arg(w)) \\ &+ \mathrm{i}|z||w|(\sin\arg(z)\cos\arg(w) + \sin\arg(w)\cos\arg(z))) \\ &= |z||w|(\cos(\arg(z) + \arg(w)) + \mathrm{i}\sin(\arg(z) + \arg(w))). \end{aligned}$$

Also gilt $|z \cdot w| = |z| \cdot |w|$ und $\arg(z \cdot w) = \arg(z) + \arg(w)$.



Die Addition komplexer Zahlen



Die Multiplikation komplexer Zahlen

Wir können die Multiplikation und Addition komplexer Zahlen auch mit Hilfe der komplexen Exponentialfunktion beschreiben. Dies ist die Abbildung $\exp : \mathbb{C} \to \mathbb{C}$, $z \mapsto e^z$ definiert durch

$$\exp(x + \mathrm{i}y) = \exp(x) \cdot \exp(\mathrm{i}y) = e^x(\cos(y) + \mathrm{i}\sin(y)) \qquad \forall x, y \in \mathbb{R}, \tag{A.2}$$

wobei e^x für $x \in \mathbb{R}$ das reelle Exponential von x bezeichnet. Aus dieser Definition erhält man direkt die Funktionalgleichung der Exponentialfunktion

$$\begin{aligned} &\exp(x + \mathrm{i}y) \cdot \exp(x' + \mathrm{i}y') = e^x(\cos(y) + \mathrm{i}\sin(y)) \cdot e^{x'}(\cos(y') + \mathrm{i}\sin(y')) \\ &= e^{x+x'}(\cos(y)\cos(y') - \sin(y)\sin(y')) + \mathrm{i}e^{x+x'}(\cos(y)\sin(y') + \sin(y)\cos(y')) \\ &= e^{e+x'}(\cos(y + y') + \mathrm{i}\sin(y + y')) = \exp((x + x') + \mathrm{i}(y + y')). \end{aligned} \tag{A.3}$$

In der Tat kann man die komplexe Exponentialfunktion durch eine auf ganz $\mathbb{C}$ absolut konvergente Potenzreihe definieren

$$\exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!}.$$

Die Funktionalgleichung ergibt sich dann wie für die reelle Exponentialfunktion mit der Cauchyschen Produktformel. Mit Hilfe der komplexen Exponentialabbildung erhält man dann die sogenannte Polardarstellung einer komplexen Zahl.

Korollar A.1.5:

1. Jede komplexe Zahl $z \in \mathbb{C} \setminus \{0\}$ lässt sich eindeutig schreiben als

   $$z = re^{\mathrm{i}\varphi} = r(\cos\varphi + \mathrm{i}\sin\varphi) \qquad \text{mit} \quad r = |z| \in \mathbb{R}^+, \varphi = \arg(z) \in [0, 2\pi).$$

   Diese heißt **Polardarstellung** und $z = x + \mathrm{i}y$ heißt **kartesische Darstellung** von z.

2. Für $z = re^{\mathrm{i}\varphi}$ und $w = se^{\mathrm{i}\psi}$ mit $r, s \in \mathbb{R}$ und $\varphi, \psi \in \mathbb{R}$ gilt $z \cdot w = rse^{\mathrm{i}(\varphi+\psi)}$.

3. Es gilt die **de Moivresche Formel**

   $$(\cos\varphi + \mathrm{i}\sin\varphi)^n = e^{\mathrm{i}n\varphi} = \cos(n\varphi) + \mathrm{i}\sin(n\varphi) \qquad \forall n \in \mathrm{Z}, \varphi \in [0, 2\pi)$$

Beispiel A.1.6. Wir bestimmen die Polardarstellung der komplexen Zahl $z = 1 - \mathrm{i}$ und die kartesische Darstellung der komplexen Zahl $w = 3e^{\mathrm{i}\pi/3}$.

Für $z = 1 - \mathrm{i}$ gilt $|z| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$ und damit auch

$$1/\sqrt{2} = \mathrm{Re}(z)/|z| = \cos(\arg(z)) = -\mathrm{Im(z)}/|z| = -\sin(\arg(z)) \quad \Rightarrow \quad \arg(z) = 7\pi/4.$$

Daraus folgt $z = \sqrt{2}e^{7\pi\mathrm{i}/4}$. Für w ergibt sich aus den Identitäten $\cos(\pi/3) = 1/2$ und $\sin(\pi/3) = \sqrt{3}/2$ die kartesische Darstellung $w = 3(\cos(\pi/3) + \mathrm{i}\sin(\pi/3)) = \frac{3}{2}(1 + \sqrt{3}\mathrm{i})$.

Eine wichtige Motivation für die Betrachtung der komplexen Zahlen ist der Fundamentalsatz der Algebra. Er besagt, dass jedes nicht-konstante Polynom mit Koeffizienten in $\mathbb{C}$ über $\mathbb{C}$ vollständig in Linearfaktoren zerfällt.

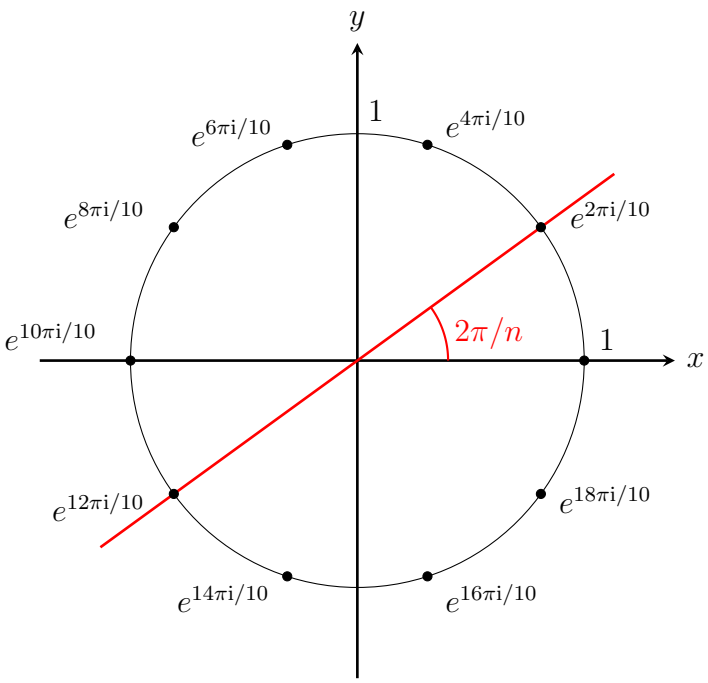
Satz A.1.7 (**Fundamentalsatz der Algebra**)**:**
Jedes nicht-konstante Polynom mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle in $\mathbb{C}$ und zerfällt deshalb über $\mathbb{C}$ in **Linearfaktoren**: zu $p = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ mit $a_n, ..., a_0 \in \mathbb{C}$, $a_n \neq 0$ und $n \in \mathbb{N}$ existieren $z_1, ..., z_n \in \mathbb{C}$ mit $p = a_n(x - z_1) \cdot (x - z_2) \cdots (x - z_n)$. Die Zahlen $z_1, ..., z_n \in \mathbb{C}$ sind genau die Nullstellen von p in $\mathbb{C}$.

Offensichtlich gilt diese Aussage nicht für reelle Zahlen, denn das Polynom x^2+1 hat keine reelle Nullstellen. Über $\mathbb{C}$ zerfällt es in Linearfaktoren, denn $(x+\mathrm{i})(x-\mathrm{i}) = x^2-\mathrm{i}^2 = x^2-(-1) = x^2+1$. Es besitzt also genau die komplexen Nullstellen $\pm\mathrm{i}$. Als Spezialfall nicht-konstanter Polynome mit *komplexen* Koeffizienten lässt sich also insbesondere jedes nicht-konstante Polynom mit *reellen* Koeffizienten als Produkt von Linearfaktoren $(x - z_1) \cdots (x - z_n)$ mit $z_j \in \mathbb{C}$ schreiben. Die folgenden zwei Spezialfälle dieser Aussage sind besonders relevant.

Lemma A.1.8:

1. Ist $p = a_n x^n + ... + a_1 x + a_0$ ein Polynom mit reellen Koeffizienten $a_n, ..., a_0 \in \mathbb{R}$, so ist $z \in \mathbb{C}$ eine Nullstelle von p genau dann, wenn $\overline{z} \in \mathbb{C}$ eine Nullstelle von p ist.
2. Die Nullstellen des Polynoms $x^n - 1$ mit $n \in \mathbb{N}$ sind die komplexen Zahlen $z_k = e^{2\pi\mathrm{i}k/n}$ mit $k \in \{0, 1, ..., n-1\}$. Man nennt sie die $n$ten **Einheitswurzeln**.

Die $n$ten Einheitswurzeln bilden die Ecken eines in den Einheitskreis $S^1 = \{z \in \mathbb{C} \,|\, |z| = 1\}$ einbeschriebenen regulären n-Ecks, dessen erste Ecke auf der Zahl 1 liegt.



Die $n$ten Einheitswurzeln für $n = 10$.

Allgemeiner erhält man für eine komplexe Zahl w eine Lösung der Gleichung $z^n = w$, indem man einen Kreis mit Radius $r = \sqrt[n]{|w|}$ um den Ursprung zeichnet, den Winkel φ zwischen w und der positiven x-Achse in n gleiche Teile teilt und den Punkt auf dem Kreis mit Radius r markiert, der mit der positiven x-Achse den Winkel φ/n einschließt. Die n Lösungen der

Gleichung $z^n = w$ sind dann genau die Ecken eines in den Kreis einbeschriebenen regulären n-Ecks, dessen erste Ecke auf diesem Punkt liegt. (Übung).

Bemerkung A.1.9. Das sichere Rechnen mit trigonometrischen Funktionen und komplexen Zahlen wird im Studium und auch im Staatsexamen vorausgesetzt. Dazu gehört es, dass man die wichtigsten Werte von Sinus und Kosinus ohne Hilfsmittel jederzeit reproduzieren kann.

Füllen Sie dazu die folgende Tabelle aus prägen Sie sich diese Werte des Sinus und Kosinus ein. Zeichnen Sie dann die zugehörigen Punkte $e^{\mathrm{i}\alpha} = \cos(\alpha) + \mathrm{i}\sin(\alpha)$ in der komplexen Ebene.

α	0	$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{3\pi}{4}$	π	$\frac{5\pi}{4}$	$\frac{3\pi}{2}$	$\frac{7\pi}{4}$	2π	$\frac{\pi}{6}$	$\frac{\pi}{3}$	$\frac{2\pi}{3}$	$\frac{5\pi}{6}$	$\frac{7\pi}{6}$	$\frac{4\pi}{3}$	$\frac{5\pi}{3}$	$\frac{11\pi}{6}$
$\sin(\alpha)$																	
$\cos(\alpha)$																	

Sie sollten auch wissen, dass $\sin(\alpha)^2 + \cos(\alpha)^2 = 1$ für alle $\alpha \in \mathbb{R}$ gilt, und die Additionsformeln für Sinus und Kosinus kennen:

$$\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta) \qquad \cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta).$$

Es ist eine hilfreiche Übung, sich daraus entsprechende Additionsformeln für den Tangens und Kotangens herzuleiten.

A.2 Wichtige Beispiele von kommutativen Ringen

Körper $\Rightarrow$ euklidischer Ring $\Rightarrow$ Hauptidealring $\Rightarrow$ faktorieller Ring $\Rightarrow$ Integritätsbereich.

	Integritäts-bereich (IB)	**faktorieller Ring (FR)**	**Hauptideal-ring (HIR)**	**euklidischer Ring (ER)**	**Körper**
$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$	✓	✓	✓	✓ h beliebig	✓
$\mathbb{Z}/p\mathbb{Z}$, p prim	✓	✓	✓	✓ h beliebig	✓
$\mathbb{K}[x]/(f)$, f irred.	✓	✓	✓	✓ h beliebig	✓
$Q(R)$, R IB	✓	✓	✓	✓ h beliebig	✓
R/I I max	✓	✓	✓	✓ h beliebig	✓
$R/(p)$, p irred, R HIR	✓	✓	✓	✓ h beliebig	✓
R IB, endlich	✓	✓	✓	✓ h beliebig	✓
$\mathbb{Z}$	✓	✓	✓	✓, $h(z) = \|z\|$	×
$\mathbb{Z}[\mathrm{i}]$	✓	✓	✓	✓ $h(a+\mathrm{i}b)$ $= a^2+b^2$	×
$\mathbb{K}[x]$	✓	✓	✓	✓, $h(f) = \deg(f)$	×
$R[x]$, R FR	✓	✓	?	?	×
$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$	✓	✓	✓	×	×
$\mathbb{Z}[x]$	✓	✓	×	×	×
$\mathbb{K}[x,y]$	✓	✓	×	×	×
$\mathbb{Z}[x,y]$	✓	✓	×	×	×
R/I, I prim	✓	?	?	?	?
$\mathbb{Z}[\mathrm{i}\sqrt{5}]$	✓	×	×	×	×
$\mathbb{K}[x]/(f)$, $f \neq$ irred.	×	×	×	×	×
$\mathbb{Z}/n\mathbb{Z}$, $n \neq$ prim	×	×	×	×	×

Legende: $\mathbb{K}$=Körper, R=kommutativer Ring mit Eins.

Index

(M), 84
(m), 84
C_g, 10
C_n, 13
D_n, 18
G-Isomorphismus, 38
G-Menge, 38
G-äquivariant, 38
$N(H)$, 42
$Q(R)$, 92
$R[[x]]$, 76
$R[x]$, 75
$R[x_1, ..., x_n]$, 76
R^*, 77
$R^\times$, 77
R_d, 98
S^1, 13
S_M, 8
S_n, 8
$Z(G)$, 14
$Z(U)$, 14
$\mathbb{F}_p$, 88
$\mathbb{Z}/n\mathbb{Z}$, 27
$\mathbb{Z}[\mathrm{i}]$, 81
$\mathbb{Z}^m$, 55
$\mathbb{Z}^m/A\mathbb{Z}^n$, 58
$\deg(p)$, 75
$\varepsilon(r)$, 99
$\mathrm{ggT}(X)$, 96
$\mathrm{kgV}(X)$, 96
$\langle M \rangle$, 16
$\left(\frac{a}{p}\right)$, 128
$\mathrm{SL}(n, \mathbb{K})$, 14
$\mathrm{SO}(n, \mathbb{K})$, 16
$\mathrm{tors}(G)$, 62
$\preceq$, 89
$\rhd$, 38
$\rtimes$, 33, 36
$\rtimes_\varphi$, 33
$\mathrm{Aut}(G)$, 12
$\mathrm{Aut}(R)$, 78
$\mathrm{GL}(n, \mathbb{Z})$, 60
$\mathrm{GL}(n, \mathbb{K})$, 7
$\mathrm{GL}_{\mathbb{K}}(V)$, 7
$\mathrm{Hom}_{\mathbb{K}}(V, W)$, 7
$\mathrm{Inn}(G)$, 14
$\mathrm{Mat}(n \times m, \mathbb{K})$, 7
$\mathrm{O}(n, \mathbb{K})$, 14
O_η, 40
$\mathrm{U}(n)$, 14
$\mathrm{char}(R)$, 79
ev_r, 79
$\trianglelefteq$, 25
φ, 117
$c(f)$, 111
f_*, 79
$o(g)$, 20
p-Gruppe, 44
p-Untergruppe, 68
pqr-Satz, 72
$r \mid s$, 95
$v_p(r)$, 99
[G:H], 23
Äquivalenz
    elementare Operationen, 58
    Matrizen mit Einträgen in $\mathbb{Z}$, 58
öffentlicher Schlüssel, 120

abelsche Gruppe, 6
    freie, 62
additive Notation, 7
alternierende Gruppe, 48
Argument
    komplexe Zahl, 140
assoziiert, 95
Auflösen von Gleichungen
    Gruppen, 6
auflösbar, 65
Automorphismengruppe
    von (unitalem) Ring, 78
    von Gruppe, 12
Automorphismus
    von (unitalen)Ringen, 78

von Gruppen, 9

Bahn, 40
Bahnengleichung, 43
Betrag
komplexe Zahl, 139
Bild
Gruppenhomomorphismus, 10
Ringhomomorphismus, 81
binäre Exponentiation, 119

Carmichaelzahlen, 119
Charakteristik, 79
charakteristische Eigenschaft
Faktorring, 86
Faktorgruppe, 29
Quotientenkörper, 93
chinesischer Restsatz
abelsche Gruppen, 55
Hauptidealringe, 104

de Moivresche Formel, 142
Diagonalmatrix
positive, 61
Diedergruppe, 18
direktes Produkt
Gruppen, 8
Gruppen, äußeres, 8
Ringe, 74
disjunkt
Permutationen, 48
Distributivgesetz, 73

echte Untergruppe, 13
echtes Ideal, 83
Einbettung
von unitalen Ringen, 78
einfache Gruppe, 26
Einheit, 77
Einheitskreis, 13
Einheitswurzeln, 13, 143
Eins, 7
Einschränkung
Gruppenoperation, 39
Einselement, 7
Eisensteinkriterium, 115
Eisensteinpolynom, 115
eisensteinsch, 115
elementare Operationen, 58
elementare Transposition, 45
elementare Vertauschung, 45
Elementarmatrizen, 59
endlich erzeugt, 84
endlich erzeugte Gruppe, 17
endliche Gruppe, 6
Endomorphismenring, 74
Endomorphismus
von (unitalen) Ringen, 78
von Gruppen, 9
Epimorphismus
von (unitalen)Ringen, 78
von Gruppen, 9
Erster Ergänzungssatz, 129
erweiterter euklidischer Algorithmus, 107
euklidische Gruppe, 34
euklidischer Algorithmus, 108
euklidischer Ring, 105
Eulerkriterium, 129
Eulersche φ-Funktion, 117
Evaluationsabbildung, 79

Faktoren, 65
Faktorgruppe, 26
faktorieller Ring, 98
faktorisieren
Gruppenhomomorphismus, 30
Faktorring, 82
Fehlstandspaar, 46
Fermat-Primzahltest, 119
Fixpunkt, 41
formale Potenzreihe, 76
freie abelsche Gruppe, 62
Fundamentalsatz der Algebra, 143

Gaußsche Zahlen, 81
gebrochen rationale Funktionen, 94
gekürzter Bruch, 100
gerade Permutation, 46
größter gemeinsamer Teiler, 96
Grad
Polynom, 75
Gruppe, 5
abelsche, 6
einfache, 26
endlich erzeugte, 17
endliche, 6
triviale, 7
zyklische, 17
Gruppenautomorphismus, 9
Gruppenendomorphismus, 9
Gruppenhomomorphismus, 9

bijektiver, 9
injektiver, 9
surjektiver, 9
trivialer, 9
Gruppenisomorphismus, 9
Gruppenmultiplikation, 5
Gruppenoperation, 38
Gruppenordnung, 6
Gruppenwirkung, 38

Höhenfunktion, 105
Halbsystem modulo p, 129
Hauptideal, 84
Hauptidealring, 101
Homomorphiesatz, 30, 86
Ringe, 86
Homomorphismus
von Gruppen, 9
von G-Mengen, 38
von (unitalen) Ringen, 78

Ideal, 82
echtes, 83
endlich erzeugtes, 84
maximales, 88
nichttriviales, 83
von Teilmenge erzeugtes, 84
zweiseitiges, 82
Idealkorrespondenz, 85
imaginär, 139
imaginäre Einheit, 139
Imaginärteil, 139
Index, 23
Inhalt, 111
innere Automorphismen, 10
innere Automorphismengruppe, 14
Integritätsbereich, 90
Integritätsring, 90
invariant unter Gruppenoperation, 39
invariante Teilmenge, 39
Inverses, 5
Inversion, 39
irreduzibel, 96
Isomorphiesatz
erster, 32
zweiter, 32
Isomorphismus
von G-Mengen, 38
von (unitalen) Ringen, 78
von Gruppen, 9

Isotropiegruppe, 41

Jacobisymbol, 133
Eigenschaften, 133

Kürzungsregel, 6
kanonische Erzeuger, 55
kanonische Surjektion, 26, 82
kanonischer Ringhomomorphismus, 79
Kern
Gruppenhomomorphismus, 10
Ringhomomorphismus, 81
Kette, 89
Klassengleichung, 44
Kleiner Satz von Fermat, 118
Kleinsche Vierergruppe, 9, 64
kleinstes gemeinsames Vielfaches, 96
kommutativer Ring, 73
Kommutativgesetz, 73
komplexe Konjugation, 139
komplexe Zahlen, 139
Kompositionsfaktoren, 65
Kompositionsreihe, 65
kongruent modulo n, 24
Konjugationsabbildung, 10
Konjugationsklassen, 41
konjugiert
Gruppenelemente, 41
konstantes Polynom, 75
Kreisteilungspolynom, 116

Länge
Bahn, 40
Permutation, 46
Zykel, 45
Legendresymbol, 128
Leitkoeffizient, 75
Lemma von Bézout, 102
Lemma von Gauß, 110
Lemma von Gauß
über Halbsysteme, 130
Linearfaktoren, 143
Linksideal, 82
Linksnebenklasse, 22
Linksoperation, 38
Linkstranslation, 39
Linkswirkung, 38

maximales Element, 89
maximales Ideal, 88
Monomorphismus

von (unitalen)Ringen, 78
von Gruppen, 9
Multiplikationstafel, 8
multiplikative Notation, 7

neutrales Element, 5
nichttriviale Teiler, 95
nichttriviale Untergruppe, 13
nichttriviales Ideal, 83
Noetherscher Homomorphiesatz, 30
Noetherscher Isomorphiesatz
erster, 32
zweiter, 32
Normabbildung, 123
normale Untergruppe, 25
Normalisator, 42
Normalteiler, 25
normiert, 75
Null, 7
Nullelement, 7
Nullpolynom, 75
Nullring, 74
Nullteiler, 90
nullteilerfrei, 90

obere Schranke, 89
Operation, 38
transitive, 40
triviale, 39
Orbit, 40
Ordnung
Gruppe, 6
Gruppenelement, 20
orthogonale Gruppe, 14
für symmetrische Bilinearform, 40

paarweise teilerfremd, 96
partiell geordnete Menge, 89
partielle Ordnung, 89
Partition
Menge, 22
natürliche Zahl, 50
Permutation, 8
Permutationsmatrix, 10
Polardarstellung, 142
Polynom, 75
Polynomdivision, 106
Polynomgrad, 75
polynomiale Abbildung, 76
Polynomring, 75
positive Diagonalmatrix, 61
Präsentation
abelsche Gruppe, 58
Diedergruppe, 19
Primelement, 96
Primideal, 91
primitiv, 110
Primkörper, 94
Primzahl
träge, 126
verzweigte, 126
zerfallende, 126
private Schlüssel, 120
Produkt
Ringe, 74
public key, 120
Pullback, 39

quadratfrei, 98
quadratischer Nichtrest, 127
quadratischer Rest, 127
quadratisches Reziprozitätsgesetz, 131
Quadrik, 40
Quaternionengruppe, 37
Quaternionenring, 81
Quotientenkörper, 92
Quotientenring, 82

Rang, 63
rationale Nullstellen, 113
Realteil, 139
Rechenregeln
Ringe, 74
Rechenregeln für Inverse, 6
Rechtsideal, 82
Rechtsnebenklasse, 22
Rechtsoperation, 38
Rechtstranslation, 39
Rechtswirkung, 38
Reduktion mod p, 114
Restklassen, 24
Restklassenring, 74
Riemannsche Zetafunktion, 121
Ring, 73
euklidischer, 105
faktorieller, 98
kommutativer, 73
mit Eins, 73
unitärer, 73
unitaler, 73

Ring mit Eins, 73
Ringautomorphismus, 78
Ringendomorphismus, 78
Ringepimorphismus, 78
Ringhomomorphismus, 78
    kanonischer, 79
    unitaler, 78
Ringmonomorphismus, 78
Rotation, 19
RSA-Verschlüsselung, 120

Satz über rationale Nullstellen, 113
Satz von Burnside, 72
Satz von Cauchy, 71
Satz von Cayley, 45
Satz von Euklid, 121
Satz von Euler, 118
Satz von Feit-Thompson, 72
Satz von Gauß, 112
Satz von Jordan-Hölder, 65
Satz von Lagrange, 24
Satz von Sylow
    erster, 70
    zweiter, 69
Satz von Wilson, 121
Schiefkörper, 77
Schnitt
    Untergruppen, 16
semidirektes Produkt, 33, 36
    äußeres, 33
    inneres, 36
    triviales, 34
Signum, 46
Solovay-Strassen-Primzahltest, 138
spalten, 37
spezielle lineare Gruppe, 14
spezielle orthogonale Gruppe, 16
Sphären, 40
Spiegelung, 19
stabil unter Gruppenoperation, 39
Stabilisator, 41
Standgruppe, 41
Subnormalreihe, 65
Sylowgruppe, 68
Sylowscher Satz
    erster, 70
    zweiter, 69
Sylowuntergruppe, 68
Symmetriegruppe, 18
    n-eck, 18
    euklidischer Raum, 34
symmetrische Gruppe, 8

Teiler, 95
teilerfremd, 96
Teilring, 80
Torsion, 62
Torsionsuntergruppe, 62
total geordnet, 89
Träger, 48
transitiv, 40
Transposition, 45
triviale Gruppe, 7
triviale Teiler, 95
triviale Untergruppe, 13
trivialer Gruppenhomomorphismus, 9
triviales semidirektes Produkt, 34

ungerade Permutation, 46
unitäre Gruppe, 14
unitärer Ring, 73
unitaler Ring, 73
unitaler Teilring, 80
unitaler Unterring, 80
universelle Eigenschaft
    Faktorring, 86
    Polynomring, 80
Untergruppe, 12
    echte, 13
    nichttriviale, 13
    normale, 25
    triviale, 13
    von Teilmenge erzeugte, 16
Untergruppenkorrespondenz, 29
Unterring, 80
    echter, 81
    nichttrivaler, 81
unzerlegbar, 96

Verknüpfung, 5
Vertauschung, 45
Vielfaches, 95

Zentralisator, 14
Zentrum, 14, 81
Zornsches Lemma, 89
zueinander konjugiert
    Gruppenelemente, 41
    Untergruppen, 41
Zweiter Ergänzungssatz, 130

Zykel, 45
Zykelzerlegung, 48
zyklische Gruppe, 17