Algebraische Strukturen

Thomas Markwig
Fachbereich Mathematik
Technische Universität Kaiserslautern

Vorlesungsskript

Oktober 2008

Inhaltsverzeichnis

Einleitung

Die Studienpläne der verschiedenen Studiengänge mit Hauptfach Mathematik an unserer Universität bedingen, daß die Hörerschaft der Vorlesung *Algebraische Strukturen* recht inhomogen ist. Für einige ist dies neben der Vorlesung *Grundlagen der Mathematik I* die erste Mathematikvorlesung, die sie besuchen, andere haben bereits ein oder zwei Semester lang Mathematik studiert. Dementsprechend sind die Voraussetzungen der einzelnen Teilnehmer sehr unterschiedlich – sowohl inhaltlicher Art, als auch was die Vertrautheit mit der mathematischen Sprache betrifft. Ich verzichte darauf, die Vorlesung mit einem Überblick über grundlegende Elemente der mathematischen Sprache und der Logik zu beginnen. Stattdessen werden sie in der Vorlesung einfach dann, wenn sie erstmals verwendet werden, kurz erläutert. Für eine ausführlichere Besprechung verweise ich die Hörer der Vorlesung auf die Vorlesung *Grundlagen der Mathematik I* und die Leser des Skriptes auf den Anhang. Insbesondere setze ich voraus, daß die Hörer und Leser mit dem Begriff der *Menge* und einfachen Mengenoperationen wie etwa *Schnitt* oder *Vereinigung* vertraut sind, und daß auch der Begriff einer *Abbildung* zwischen zwei Mengen sowie einfache Eigenschaften derselben wie etwa *Invertierbarkeit* bekannt sind. Die Begriffe können aber auch im Anhang nachgeschlagen werden. Zudem gehe ich davon aus, daß die Mengen der *natürlichen Zahlen* $\mathbb{N}$, der *ganzen Zahlen* $\mathbb{Z}$, der *rationalen Zahlen* $\mathbb{Q}$ und der *reellen Zahlen* $\mathbb{R}$ sowie die grundlegenden Rechenoperationen für diese Zahlbereiche bekannt sind.

Ich möchte auch nicht versäumen, darauf hinzuweisen, daß die Vorlesung selbst sich im Stil vom vorliegenden Vorlesungsskript fundamental unterscheidet. Sie wird in ihrer Darstellung wesentlich knapper, weniger textlastig und dafür *graphischer* gestaltet sein. Zudem werden etliche Aussagen und Bemerkungen des Skriptes in der Vorlesung nur in mündlicher Form auftauchen oder evt. auch ganz wegfallen. In gewisser Weise ergänzen sich die Vorlesung und das Skript auf diese Weise.

Wie der Name der Vorlesung nahe legt, werden grundlegende Strukturen der Algebra eingeführt und untersucht – *Gruppen*, *Ringe* und *Körper* sowie Abbildungen, die die jeweilige Struktur respektieren. Wir werden viel Zeit damit verbringen wichtige Beispiele für die jeweiligen Strukturen kennenzulernen und dabei hoffentlich auch deren Nutzen erkennen. Um letzterem Vorschub zu leisten, möchte ich die Einleitung mit der Beschreibung einiger Probleme abschließen, zu deren Lösung die im Verlauf der Vorlesung eingeführten Strukturen und der erzielten Ergebnisse einen wesentlichen Beitrag leisten. [1] Dabei werden einige Begriffe auftauchen, die erst in

[1] Die Strichcodes werden in Kapitel 5 näher betrachtet. Der chinesische Restsatz ist Bestandteil von Kapitel 7. Seine Anwendung im RSA-Verfahren wird allerdings erst in der Vorlesung Elementare Zahlentheorie betrachtet werden können. Wer nicht so lange warten möchte, dem sei das Buch [Beu94] empfohlen. Die zyklischen Codes sprengen den Rahmen der Vorlesung gänzlich, auch wenn die dafür erforderliche Struktur des Polynomrings $\mathsf{K}[t]$ und seiner Ideale ausführlich behandelt werden. Für die zyklischen Codes verweise ich auf [Sch91].

den späteren Kapiteln mit Leben gefüllt werden – dem Leser sei empfohlen, zunächst einfach so zu tun, als hätten sie eine Bedeutung, und den entsprechenden Abschnitt später noch mal zu lesen!

Strichcodes, ISBN-Nummern, Banknoten

Bezahlt man heutzutage in einem Geschäft seine Ware, so wird der Preis in aller Regel nicht per Hand eingegeben. Vielmehr wird der Strichcode, der sich an jedem Artikel befindet, eingescannt, und selbst wenn das aufgrund technischer Probleme nicht funktioniert, gibt der Kassierer nicht den Preis, sondern die zum Strichcode gehörende Ziffernfolge ein – üblicherweise aus 13 Ziffern bestehend. Der Preis wird

5 901234 123457

Abbildung 1. Ein EAN-13 Strichcode

dann aus einer vorhandenen Datenbank ermittelt, und in selbiger Datenbank wird vermerkt, daß das Geschäft nun einen Artikel dieses Codes weniger im Angebot hat. Wie gesagt, manchmal funktioniert das Einscannen nicht und eine solch lange Ziffernfolge abzutippen ist reichlich fehleranfällig. Im Falle eines Fehlers piepst die Kasse und der Kassierer gibt die Ziffernfolge noch mal ein. Wie kommt es, daß ein Fehler beim Eingeben immer auffällt?

Zunächst einmal bedeutet es nur, daß der falsche Code nicht in der Datenbank vorhanden ist. Das scheint auf den ersten Blick nicht zu verwundern, hat der Code doch 13 Ziffern und das Geschäft sicher nicht einmal 10000 verschiedene Artikel im Angebot. Würde man also jedem Artikel einen zufälligen Code aus 13 Ziffern geben, so könnte man ziemlich sicher sein, daß einzelne Fehler beim Abtippen auffallen würden. Nun werden diese Strichcodes aber nicht von den Geschäften vergeben, die die Ware verkaufen, sondern vom Hersteller – oder genauer gesagt, der Hersteller läßt sie bei einer zentralen Agentur eintragen. Letzteres ist sinnvoll, denn es sollen schließlich nicht zwei Hersteller den gleichen Code verwenden. Was das für ein Geschäft bedeuten würde, das Waren von beiden bezieht, liegt auf der Hand.

Der in Europa gängigste Typ des Strichcodes ist der **EAN-13**, was soviel wie *European Article Number* der Länge 13 bedeutet. Vergeben werden sie von mehreren Organisationen, und die ersten zwei bis drei Ziffern des Codes identifizieren (im wesentlichen) das Land in dem der Code ausgegeben wurde. Einige der folgenden Ziffern identifizieren den Hersteller, der wiederum weitere Ziffern zur Identifikation seines Produktes zur Verfügung hat.[2] Daraus ergibt sich aber, daß für verschiedene

[2] Das Bild des Strichcodes in Figur 1 stammt von der Web-Seite:

Produkte eines Herstellers ein großer Teil des Strichcodes identisch ist. Außerdem wird der Hersteller auch bei dem Teil, den er selbst bestimmen kann, kaum willkürliche Ziffern vergeben, sondern den Code weiter zur systematischen Produktklassifizierung nutzen wollen. Die Idee des *zufällig* gewählten Codes ist also hinfällig, und es kann durchaus sein, daß sich der Code für eine 100g-Tafel Schokolade sehr wenig von dem für eine 400g-Tafel unterscheidet – im Gegensatz zum Preis.

Wir brauchen also eine neue Idee, wie man Fehler bei der Eingabe mit hoher Wahrscheinlichkeit bemerken kann, und die Idee heißt *Redundanz*! Man hängt an den Teil des Codes, den man zur Identifikation des Produktes braucht, zusätzliche (redundante) Ziffern an, deren einziger Sinn es ist, den Code fehlerresistenter zu machen. Dabei sollten möglichst wenig zusätzliche Ziffern eine möglichst hohe Sicherheit bieten. Weshalb und wie man das mit nur einer Ziffer, der sogenannten *Prüfziffer*, erreicht, hat mit Gruppen zu tun – bei **EAN-13** ganz konkret die Gruppe $\mathbb{Z}_{10}$, die wir im Kapitel 4 kennen lernen.

Ein analoges Verfahren wird bei nahezu allen Ziffern- und Buchstabencodes angewendet, die zur Identifizierung von Produkten und Personen verwendet werden: z.B. Kreditkarten, Personalausweise, **ISBN**-Nummern, Seriennummern von Banknoten, etc.. Aber nicht alle verwenden die gleiche Gruppe, z.B. haben **ISBN**-Nummern bis 2007 die Gruppe $\mathbb{Z}_{11}$ verwendet und die alten DM-Scheine die Diëdergruppe $\mathbb{D}_{10}$. Es gibt gute Gründe, verschiedene Gruppen und Verfahren zu verwenden, denn nicht alle bieten die gleiche Sicherheit!

Zyklische Codes

Die oben angesprochene Prüfzifferkodierung ist ein Spezialfall des allgemeineren Problems, daß man Information über einen störanfälligen Kanal schicken möchte.

$$\boxed{\text{Sender}} \xrightarrow[\boxed{\text{Kanal}}]{\text{Störung}} \boxed{\text{Empfänger}}$$

Bei der Prüfzifferkodierung war der Kanal im wesentlichen die Person, die die Ziffern eingibt bzw. der Scanner. Ziel war es, Fehler zu erkennen.

Ein Beispiel für das allgemeinere Problem ist das Abspielen und Hören von CDs. Man kann die CD als Sender, den Nutzer als Empfänger und den CD-Spieler als Kanal auffassen. Im Gegensatz zur Prüfzifferkodierung wird es uns beim Hören einer CD nicht wirklich reichen, daß ein Fehler erkannt wird. Wir wollen zweifelsohne auch, daß er korrigiert wird. Eine Möglichkeit dazu ist, den Laserstrahl die Stelle, an der ein Fehler aufgetreten ist, noch mal lesen zu lassen. Aber wenn ein Fehler z.B. durch einen Kratzer auf der CD entstanden ist, wird das nicht viel helfen. Besser wäre es, wenn kleinere Fehler nicht nur erkannt, sondern auch korrigiert werden könnten.

---

http://de.wikipedia.org/wiki/European_Article_Number

Dort findet man auch weitere Informationen zur Struktur des EAN-13 Strichcodes.

Wir werden in der Vorlesung die Theorie der fehlerkorrigierenden Codes nicht wirklich behandeln können. Aber die Grundidee läßt sich einfach erläutern. Die Information auf einer CD ist im wesentlichen dadurch gespeichert, daß in einem gewissen Bereich die unteren Schichten des reflektierenden Materials Löcher haben, in anderen nicht – zwei Zustände also, sagen wir 0 und 1. Gehen wir vereinfachend davon aus, daß die Länge eines Bereichs mit Loch bzw. ohne Loch, der Anzahl an Nullen oder Einsen entspricht, so besteht die Information aus einer Ziffernfolge von Nullen und Einsen. Zur sinnvollen Weiterverarbeitung wird die Information in Pakete fester Länge gebündelt, sagen wir etwa Zifferntupel der Länge n. Damit besteht die Information, die über den Kanal geht, also aus Einheiten

$$(c_0, \ldots, c_{n-1}) \in \left(\mathbb{Z}_2\right)^n,$$

d.h. aus Elementen eines Vektorraums über dem Körper $\mathbb{Z}_2$. Was ein Vektorraum ist, wird in den *Grundlagen der Mathematik* erläutert, der *Körper* $\mathbb{Z}_2$ wird in dieser Vorlesung eingeführt.

Wie bei der Prüfzifferkodierung werden nicht alle Ziffern des Tupels für die Kodierung der gesendeten Information benötigt, einige sind nur zur Sicherung der Information da. Anders ausgedrückt, nicht jedes Tupel $(c_0, \ldots, c_{n-1})$ wird eine zulässige Information sein, und es wird darauf ankommen, daß die Menge C der zulässigen Codewörter eine zusätzliche algebraische Struktur aufweist, damit es gute Methoden gibt, Fehler zu erkennen und ggf. zu beheben. Genauer gesagt, C sollte zumindest ein *Untervektorraum* sein, um Methoden der *linearen Algebra* anwenden zu können.

$$\text{Z.B.: } C = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\} \leq \mathbb{Z}_2^3.$$

Aber besser ist es noch, einen Vektor $(c_0, \ldots, c_{n-1})$ mit dem Polynom

$$c_0 + c_1 \cdot t + c_2 \cdot t^2 + \ldots + c_{n-1} \cdot t^{n-1}$$

und den Vektorraum $\mathbb{Z}_2^n$ mit einem Faktorring des Polynomrings $\mathbb{Z}_2[t]$ zu identifizieren, vor allem wenn dann C ein *Ideal* in diesem Faktorring ist. Dann reicht nämlich im wesentlichen 1 Element, um alle Codewörter zu beschreiben, wie wir im Kapitel über den Polynomring sehen werden.

Das RSA-Verfahren und der Chinesische Restsatz

Bei den bisher angesprochenen Kodierungen ging es stets darum, Verfälschungen der Informationen zu erkennen und ggf. zu korrigieren, damit sie korrekt beim Empfänger ankommen. Diesen Zweig der Mathematik nennt man Kodierungstheorie und grenzt ihn von der Kryptographie ab. Auch letztere beschäftigt sich mit dem Schutz von Informationen die ein Sender über einen störanfälligen Kanal zu einem Empfänger schickt. Ziel ist es aber primär zu verhindern, daß ein Störenfried die Informationen mithören und *verstehen* oder *unbemerkt verändern* kann. Da wir den

Kanal als unsicher annehmen, können wir das *Mithören* in aller Regel nicht verhindern. Also muß beim Verstehen und Verändern angesetzt werden. Die Grundidee ist, den Text zu verschlüsseln.

$$\begin{tikzcd}
\underline{\text{Sender}} & & \underline{\text{Empfänger}} \\
\boxed{\text{Klartext}} \arrow[d, "\text{Schlüssel}"'] & & \boxed{\text{Klartext}} \\
\boxed{\text{Geheimtext}} \arrow[rr, "\text{Störenfried}"] & & \boxed{\text{Geheimtext}} \arrow[u, "\text{Schüssel}"']
\end{tikzcd}$$

In der einfachsten Form der aus dem alten Rom überlieferten *Caesar Chiffre* vertauscht man die Buchstaben der Nachricht zyklisch, z.B.

$$\begin{array}{c|c|c|c|c|c|c|c|c}
\mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \dots & \mathtt{x} & \mathtt{y} & \mathtt{z} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow \\
\mathtt{m} & \mathtt{n} & \mathtt{o} & \mathtt{p} & \mathtt{q} & \dots & \mathtt{j} & \mathtt{k} & \mathtt{l}
\end{array}$$

Der Schlüssel besteht hierbei aus einer einzigen Zahl, nämlich um wieviel Buchstaben man das “a” nach rechts geschiftet hat; im obigen Beispiel ist dies 12. Eine solch einfache Verschlüsselung ist natürlich auch sehr einfach von einem Störenfried zu brechen. Aber sie weist ein wichtiges Merkmal auf, das auch allen der nach Caesar entwickelten Verschlüsselungsverfahren bis ins letzte Jahrhundert eigen war: der gleiche Schlüssel dient zum Verschlüsseln und zum Entschlüsseln, muß also *geheim* bleiben! Man nennt solche Verschlüsselungsverfahren deshalb *symmetrisch*, und eines ihrer wesentlichen Sicherheitsrisiken besteht darin, daß Sender und Empfänger zunächst einmal den geheimen Schlüssel austauschen müssen, ohne dabei abgehört werden zu können.

Eine Idee von Whitfield Diffie und Martin Hellman (siehe [DH76]) aus den siebziger Jahren revolutionierte die Kryptographie. Zum Ver- und Entschlüsseln sollten zwei unterschiedliche Schlüssel verwendet werden, und die Kenntnis von einem der beiden und der Nachricht sollte es nicht erlauben, auf den anderen zurückzuschließen. So könnte der Sender einen der beiden Schlüssel *geheim* halten, den anderen aber *öffentlich* bekannt geben. Damit ist es leicht, eine Nachricht so zu verschlüsseln, daß dem Empfänger jede Veränderung auffallen würde. Wir stellen dies in dem folgenden Schema dar, wobei gSS für den *geheimen Schlüssel des Senders* steht und $\mathsf{öSS}$ für den *öffentlichen Schlüssel des Senders*:

$$
\begin{tikzcd}
\underline{\text{Sender}} & & \underline{\text{Empfänger}} \\
\boxed{\text{Klartext}} \arrow[d, "\mathsf{gSS}"'] & & \boxed{\text{Klartext}} \\
\boxed{\text{Geheimtext}} \arrow[rr, "\text{Störenfried}"] & & \boxed{\text{Geheimtext}} \arrow[u, "\mathsf{öSS}"']
\end{tikzcd} \tag{1}
$$

Der Störenfried kann die Nachricht zwar abfangen, mit dem (auch ihm bekannten) öffentlichen Schlüssel entschlüsseln und kennt dann deren Inhalt. Da ihm aber der geheime Schlüssel fehlt, kann er die Nachricht nicht verfälschen, wieder verschlüsseln und gefälscht weiter schicken.

Wenn man die Nachricht geheim halten möchte, sollte der Empfänger je einen geheimen und öffentlichen Schlüssel haben. Wie dann die Verschlüsselung aussehen kann, stellen wir in folgendem Schema dar, wobei wir für den geheimen Schlüssel des Empfängers die Abkürzung *gSE* verwenden und für seinen öffentlichen Schlüssel die Abkürzung *öSE*:

$$
\begin{tikzcd}
\underline{\text{Sender}} & & \underline{\text{Empfänger}} \\
\boxed{\text{Klartext}} \arrow[d, "\mathsf{öSE}"'] & & \boxed{\text{Klartext}} \\
\boxed{\text{Geheimtext}} \arrow[rr, "\text{Störenfried}"] & & \boxed{\text{Geheimtext}} \arrow[u, "\mathsf{gSE}"']
\end{tikzcd} \tag{2}
$$

Da der Störenfried den geheimen Schlüssel des Empfängers nicht kennt, kann er die Nachricht auch nicht entschlüsseln. Verschlüsselungsverfahren dieser Art nennt man *asymmetrisch*, oder spezieller *public key Verfahren*. Aber damit ein solches Verfahren funktionieren kann, muß es einigen wichtigen Anforderungen genügen, und um dies zu beschreiben sollten wir den Begriff der *Verschlüsselung* etwas mathematischer fassen.

Bei der Caesar Chiffre aus obigem Beispiel werden Textblöcke verschlüsselt, die aus einem einzigen Buchstaben bestehen, und man kann die Verschlüsselung als *Abbildung*

$$f_k : \mathcal{N} \longrightarrow \mathcal{N}$$

der Menge

$$\mathcal{N} = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}$$

in sich selbst auffassen, die von dem Schlüssel k abhängt (in obigem Beispiel $k = 12$) und die *Nachricht* um k Stellen verschiebt – wobei wir im Alphabet mit a weiter machen, wenn wir bei z angekommen sind. Wichtig ist dabei, daß die Funktion eine *Umkehrfunktion* besitzt (man nennt die Funktion f_k dann *bijektiv*), die es erlaubt, den Prozess rückgängig zu machen. In unserem Fall ist dies die Funktion f_{-k}, die eine Nachricht um k Stellen nach links verschiebt. Auch sie hängt von einem Schlüssel ab, und es ist im wesentlichen der gleiche Schlüssel – das Verschlüsselungsverfahren ist *symmetrisch*! Da man für jeden zulässigen Schlüssel eine Funktion f_k zum Verschlüsseln benötigt, spricht man auch von einer *Familie* von Funktionen $\{f_k \mid k \in \mathcal{S}\}$, wobei $\mathcal{S}$ die Menge der zulässigen Schlüssel sein soll. Im Fall der Caesar Chiffre könnten wir $\mathcal{S} = \{-25, -24, \ldots, 24, 25\}$ wählen.

Im Allgemeinen wird man Textblöcke größerer Länge verschlüsseln, und man wird sie in aller Regel zunächst durch einen einfachen Übersetzungsmechanismus in Ziffern überführen, um leichter die Methoden der Mathematik anwenden zu können. Bei der Caesar Chiffre könnte man z.B. die Buchstaben durch ihre Position im Alphabet ersetzen, $a = 1$, $b = 2$, etc., und man könnte $\mathcal{N}$ auf dem Weg etwa mit $\{1, 2, \ldots, 26\}$ oder gar mit $\mathbb{Z}_{26}$ gleichsetzen. Jedenfalls schadet es nichts, wenn wir vereinfachend davon ausgehen, daß die Nachricht, die wir verschlüsseln wollen aus einer Zahl besteht! Für das oben beschriebene *public key Verfahren* benötigen wir dann eine Familie von bijektiven Funktionen $\mathcal{F} = \{f_k : \mathcal{N} \to \mathcal{N} \mid k \in \mathcal{S}\}$ auf der Menge $\mathcal{N}$ der Nachrichten, so daß für jeden Schlüssel $gS \in \mathcal{S}$ ein Schlüssel $öS \in \mathcal{S}$ existiert mit

$$f_{gS} \circ f_{öS} = f_{öS} \circ f_{gS} = \mathrm{id}_{\mathcal{N}}\,. \qquad (3)$$

Die Abbildung $f_{öS}$ ist dann die Inverse von f_{gS}, so daß man die Bedingung (3) auch alternativ schreiben könnte als

$$f_k \in \mathcal{S} \quad \Longrightarrow \quad f_k^{-1} \in \mathcal{S}.$$

Die beiden Eigenschaften in (3) bedeuten für die Anwendung, daß es egal ist, ob man den öffentlichen oder den geheimen Schlüssel zum *Verschlüsseln* verwendet, der jeweils andere kann zum *Entschlüsseln* verwendet werden. Das haben wir in den beiden oben beschriebenen Anwendungen (siehe (1) und (2)) bereits ausgenutzt.

Ein ungemein wichtiger Punkt dabei ist natürlich, daß man aus der Kenntnis der Familie $\mathcal{F}$ sowie eines gegebenen öffentlichen Schlüssels $öS$ *keine Chance* hat, den zugehörigen geheimen Schlüssel gS zu bestimmen. Dabei heißt *keine Chance* nicht, daß es prinzipiell unmöglich ist, sondern daß der notwendige Rechenaufwand nicht in sinnvoller Zeit zu bewerkstelligen ist. Zugleich muß der Rechenaufwand zur Bestimmung von $f_k(n)$ bei gegebenem n und k sehr gering sein, damit man das Verfahren auch praktisch anwenden kann!

Eine solche Familie von Funktionen haben Ronald Rivest, Adi Shamir und Leonard Adleman 1977 (siehe [RSA78]) gefunden, und daraus ist das *RSA-Verfahren* entstanden, das aus mathematischer Sicht nicht mehr als die Primfaktorzerlegung der ganzen Zahlen und ein paar einfache Ergebnisse wie den Chinesischen Restsatz oder den Kleinen Satz von Fermat braucht – Ergebnisse, die wir im Rahmen dieser

Vorlesung kennenlernen werden. Entscheidend dabei ist folgende Erkenntnis: so einfach die Zerlegung einer Zahl in Primfaktoren *im Prinzip* auch ist, so schwierig ist sie doch ganz *konkret* durchzuführen (selbst für gute Computer), wenn die Zahlen einmal mehrere hundert Ziffern besitzen!

1 Gruppen und Homomorphismen

In der Einleitung haben wir davon gesprochen, daß es das grundlegende Ziel der Vorlesung sein wird, verschiedene *Strukturen* auf Mengen zu studieren. Was eine *Struktur auf einer Menge* ganz konkret ist, hängt letztlich sehr vom Zweig der Mathematik und der betrachteten Fragestellung ab. In dieser Vorlesung wird die Struktur stets aus einer oder mehreren *zweistelligen Operationen* auf der Menge bestehen, die dann bestimmten *Gesetzmäßigkeiten*, sogenannten *Axiomen*, genügen sollen. Dabei ist eine *zweistellige Operation* auf einer Menge G eine Abbildung, die einem Paar (g, h) von Elementen aus G wieder ein Element in G zuordnet, also eine Abbildung $G \times G \to G$.

A) Gruppen

Die grundlegendste und wichtigste algebraische Struktur auf einer Menge ist die *Gruppenstruktur*.

Definition 1.1

a. Eine *Gruppe* ist ein Paar $(G, \cdot)$ bestehend aus einer *nicht-leeren* Menge G und einer zweistelligen Operation "·", d. h. einer Abbildung

$$\cdot : G \times G \to G : (g, h) \mapsto g \cdot h,$$

so daß die folgenden *Gruppenaxiome* gelten:

G1: $(g \cdot h) \cdot k = g \cdot (h \cdot k) \quad \forall\, g, h, k \in G,$ ("Assoziativgesetz")

G2: $\exists\, e \in G \;:\; \forall\, g \in G \;:\; e \cdot g = g,$ ("Existenz eines Neutralen")

G3: $\forall\, g \in G\; \exists\, g' \in G \;:\; g' \cdot g = e.$ ("Existenz von Inversen")

Ein Element mit der Eigenschaft von e nennt man ein *neutrales Element* der Gruppe G. Ein Element mit der Eigenschaft von g' nennt man ein *Inverses zu* g.

b. Eine Gruppe $(G, \cdot)$ heißt *abelsch* oder *kommutativ*, wenn $(G, \cdot)$ zudem noch dem folgenden Axiom genügt:

G4: $g \cdot h = h \cdot g \quad \forall\, g, h \in G$ ("Kommutativgesetz")

c. Eine Gruppe $(G, \cdot)$ heißt *endlich*, falls $|G| < \infty$, und sonst *unendlich*. $|G|$ heißt die *Ordnung* von G.[3]

Bemerkung 1.2

Für manche Anwendungen ist der Begriff der *Gruppe* stärker als wünschenswert, da mehr Axiome gefordert werden, als die betrachteten Strukturen hergeben. Man kann den Begriff in zweifacher Weise abschwächen. Sei dazu wieder eine Menge G zusammen mit einer zweistelligen Operation "·" auf G gegeben.

a. Erfüllt das Paar $(G, \cdot)$ nur das Axiom G1 so nennt man $(G, \cdot)$ eine *Halbgruppe*.

---

[3] $|G|$ bezeichnet die Anzahl der Elemente in der Menge G, siehe Definition B.17.

b. Wir nennen $(G, \cdot)$ ein *Monoid*, falls nur die Axiome G1 und G2' gelten:

G2': $\exists\, e \in G \,:\, \forall\, g \in G \,:\, e \cdot g = g \cdot e = g$. ("Existenz eines Neutralen")

Man beachte, daß bei Monoiden für die Neutralen eine stärkere Bedingung gefordert wird, als bei Gruppen. Inwieweit sie wirklich stärker ist, werden wir in Lemma 1.4 sehen. Die Begriffe *abelsch*, *endlich*, *unendlich* und *Ordnung* führt man für Halbgruppen und Monoide in der gleichen Weise ein wie für Gruppen. In dieser Vorlesung werden wir uns aber nicht weiter mit speziellen Eigenschaften von Halbgruppen oder Monoiden beschäftigen. Wir erwähnen die Begriffe nur der Vollständigkeit halber. □

Bevor es sinnvoll ist, sich mit Eigenschaften einer neuen Struktur wie den eben eingeführten Gruppen zu beschäftigen, sollte man gute Beispiele kennen. Schließlich möchte man keine Aussagen über die leere Menge oder auch nur eine vollkommen uninteressante Struktur treffen.

Beispiel 1.3

a. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ mit der üblichen Addition als Gruppenoperation sind abelsche Gruppen. Die Zahl Null erfüllt jeweils die Rolle eines neutralen Elements, und zu einer Zahl g existiert mit $-g$ ein inverses Element.

b. $(\mathbb{Q}\setminus\{0\}, \cdot)$ und $(\mathbb{R}\setminus\{0\}, \cdot)$ mit der üblichen Multiplikation als Gruppenoperation sind ebenfalls abelsche Gruppen. Die Zahl 1 ist jeweils ein neutrales Element, und zu einer Zahl g existiert als inverses Element die Zahl $\frac{1}{g}$.

c. $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist hingegen nur ein (abelsches) Monoid mit der Zahl Eins als neutralem Element. Das Axiom G3 ist nicht erfüllt, da nur die Zahlen $g = 1$ und $g = -1$ in $\mathbb{Z} \setminus \{0\}$ ein Inverses $\frac{1}{g}$ besitzen.

d. $(\mathbb{N}, +)$ ist ebenfalls nur ein (abelsches) Monoid mit der Zahl Null als neutralem Element, da zu $g > 0$ kein Inverses $-g$ in $\mathbb{N}$ existiert.

e. Die einfachste Gruppe ist die *einelementige Gruppe* $G = \{e\}$, deren Gruppenoperation durch $e \cdot e = e$ definiert ist.

Man beachte, daß in allen obigen Beispielen ein eindeutig bestimmtes neutrales Element sowie zu jedem g ein eindeutig bestimmtes inverses Element existiert. Dies ist kein Zufall. Die Eindeutigkeit kann aus den Gruppenaxiomen hergeleitet werden.

Lemma 1.4

Es sei $(G, \cdot)$ *eine Gruppe.*

a. *Das neutrale Element* $e \in G$ *ist eindeutig bestimmt und hat zusätzlich die Eigenschaft:*

$$g \cdot e = g \quad \forall\, g \in G.$$

b. *Sei* $g \in G$. *Das inverse Element* g' *zu* g *ist eindeutig bestimmt und hat zusätzlich die Eigenschaft:*

$$g \cdot g' = e.$$

Die in obigem Lemma formulierten Aussagen lassen sich für die bisher betrachteten Beispiele leicht verifizieren, und man könnte dies natürlich für jedes neue Beispiel, das einem einfällt ebenfalls wieder tun. Eine solche Vorgehensweise wäre jedoch wenig befriedigend. Stattdessen wollen wir die Korrektheit der getroffenen Aussagen ganz allgemein aus den Gruppenaxiomen herleiten. Dieses Vorgehen nennen wir einen *Beweis* der Aussagen, und wann immer wir eine Aussage als Lemma, Proposition, Satz oder Korollar formulieren, werden wir sie auch beweisen.[4]

Beweis von Lemma 1.4: Da wir für das Paar $(G, \cdot)$ die Axiome G1-G3 aus Definition 1.1 voraussetzen, gibt es ein neutrales Element $e \in G$, und zu beliebigem, aber fest gegebenem $g \in G$ gibt es ein Inverses $g' \in G$.

Wir wollen zunächst zeigen, daß für dieses e und dieses g' die in a. und b. geforderten zusätzlichen Eigenschaften gelten.

Da $(G, \cdot)$ eine Gruppe ist, gibt es ein $g'' \in G$ mit

$$g'' \cdot g' = e. \tag{4}$$

Also folgt:[5]

$$\begin{aligned} g \cdot g' &\overset{G2}{=} e \cdot \big(g \cdot g'\big) \overset{(4)}{=} \big(g'' \cdot g'\big) \cdot \big(g \cdot g'\big) \overset{G1}{=} g'' \cdot \big(g' \cdot (g \cdot g')\big) \\ &\overset{G1}{=} g'' \cdot \big((g' \cdot g) \cdot g'\big) \overset{G3}{=} g'' \cdot \big(e \cdot g'\big) \overset{G2}{=} g'' \cdot g' \overset{(4)}{=} e. \end{aligned} \tag{5}$$

Damit ist gezeigt, daß g' die zusätzliche Eigenschaft in b. erfüllt, und wir erhalten:

$$g \cdot e \overset{G3}{=} g \cdot \big(g' \cdot g\big) \overset{G1}{=} \big(g \cdot g'\big) \cdot g \overset{(5)}{=} e \cdot g \overset{G2}{=} g. \tag{6}$$

Nun war aber g ein beliebiges Element in G, so daß damit die zusätzliche Eigenschaft von e in a. gezeigt ist.

Sei nun $\tilde{e} \in G$ irgendein Element mit der Eigenschaft des Neutralen, d.h. so daß

$$\tilde{e} \cdot h = h \tag{7}$$

[4] Die Begriffe *Lemma*, *Proposition*, *Satz* und *Korollar* sind in der Mathematik übliche *Ordnungsstrukturen* (vergleichbar etwa einer Karteikarte), in denen bewiesene Aussagen festgehalten werden. Dabei werden die Aussagen, die als Propositionen formuliert werden, meist als wichtiger erachtet, als Aussagen in einem Lemma, und entsprechend sind Aussagen in einem Satz meist wesentlicher als Aussagen in einer Proposition. Das Korollar fällt etwas aus dem Rahmen, da es übersetzt *Folgerung* bedeutet und somit andeutet, daß es aus einer der unmittelbar zuvor getroffenen Aussagen abgeleitet werden kann. – Es kann vorkommen, daß der Beweis einer Aussage den Rahmen dieser Vorlesung sprengen würde oder wir aus anderen Gründen auf den Beweis verzichten wollen oder müssen. In einem solchen Fall werden wir die Aussage nur als *Bemerkung* formulieren und deutlich machen, weshalb wir auf einen Beweis verzichten.

[5] Über den Gleichheitszeichen geben wir als Begründung für die Gleichheit das jeweilige Axiom, das verwendet wird, bzw. die Referenznummer der eingesetzten Gleichung an. Dies ist eine in der Mathematik übliche Notation, die wir auch im Folgenden immer dann anwenden werden, wenn wir sehr genau argumentieren wollen.

für alle $h \in G$. Wir müssen zeigen, daß $e = \tilde{e}$ gilt. Da wir bereits wissen, daß e die zusätzliche Eigenschaft in a. erfüllt, können wir diese, d.h. (6), mit $\tilde{e}$ in der Rolle von g anwenden, und anschließend (7) mit e in der Rolle von h:

$$\tilde{e} \stackrel{(6)}{=} \tilde{e} \cdot e \stackrel{(7)}{=} e.$$

Schließlich müssen wir noch zeigen, wenn $\tilde{g}' \in G$ ein weiteres inverses Element zu g ist, d.h. wenn

$$\tilde{g}' \cdot g = e \tag{8}$$

gilt, dann ist schon $g' = \tilde{g}'$. Wenden wir das bislang gezeigte an, so gilt:

$$\tilde{g}' \stackrel{(6)}{=} \tilde{g}' \cdot e \stackrel{(5)}{=} \tilde{g}' \cdot \left(g \cdot g'\right) \stackrel{\text{G1}}{=} \left(\tilde{g}' \cdot g\right) \cdot g' \stackrel{(8)}{=} e \cdot g' \stackrel{\text{G2}}{=} g'.$$

Damit sind alle Aussagen des Lemmas bewiesen.[6] □

Notation 1.5

Statt $(G, \cdot)$ schreiben wir häufig nur G, sofern keine Unklarheiten über die Operation bestehen. Außerdem schreiben wir, für $g, h \in G$, statt $g \cdot h$ oft verkürzt gh. Das neutrale Element bezeichnen wir auch mit 1 statt mit e, oder mit 1_G bzw. e_G, wenn wir hervorheben wollen, in welcher Gruppe es das Neutrale ist. Und das zu $g \in G$ existierende, eindeutig bestimmte inverse Element wird mit g^{-1} bezeichnet, oder mit g_G^{-1}, wenn wir wieder hervorheben wollen, in welcher Gruppe es das Inverse zu g ist.

Ist die Gruppe abelsch, so bezeichnet man die Operation oft mit $+$ anstatt mit $\cdot$. In diesem Fall verwenden wir die Bezeichnung 0 (bzw. 0_G) für das neutrale Element und $-g$ (bzw. $-g_G$) für das zu $g \in G$ eindeutig bestimmte Inverse. □.

Lemma 1.6

Sei $(G, \cdot)$ *eine Gruppe,* $g, h, a, b \in G$. *Dann gelten:*

a. $\left(g^{-1}\right)^{-1} = g$ *und* $(gh)^{-1} = h^{-1}g^{-1}$.

b. *In* G *gelten die* Kürzungsregeln*:*
   (i) $ga = gb \;\Rightarrow\; a = b$, *und*
   (ii) $ag = bg \;\Rightarrow\; a = b$.

Beweis: a. Um die erste Gleichheit zu zeigen, reicht es wegen der Eindeutigkeit des Inversen zu g^{-1} zu zeigen, daß g die Eigenschaft *des* Inversen zu g^{-1} besitzt. Beim Beweis können wir die Gruppenaxiome sowie die in Lemma 1.4 bewiesenen zusätzlichen Eigenschaften des Inversen anwenden:

$$g \cdot g^{-1} \stackrel{\text{Lem. 1.4b.}}{=} e.$$

[6] Das Zeichen □ am *Ende* eines Beweises zeigt stets an, daß der Beweis fertig ist. Manchmal verwenden wir das Zeichen auch bei einer Bemerkung oder Notation an, um deren Ende anzuzeigen.

Also ist g ein Inverses zu g^{-1}, und damit gilt wie angedeutet wegen der Eindeutigkeit des Inversen zu g^{-1}:

$$\left(g^{-1}\right)^{-1} = g.$$

Analog ist nach Voraussetzung $(gh)^{-1}$ ein Inverses zu gh, und es reicht wegen der Eindeutigkeit des Inversen zu gh zu zeigen, daß $h^{-1}g^{-1}$ ebenfalls die Eigenschaft eines Inversen zu gh hat:

$$\begin{aligned}\left(h^{-1}g^{-1}\right)\cdot(gh) &\stackrel{G1}{=} h^{-1}\cdot\left(g^{-1}\cdot(gh)\right) \stackrel{G1}{=} h^{-1}\cdot\left((g^{-1}\cdot g)\cdot h\right)\\ &\stackrel{G3}{=} h^{-1}\cdot(e\cdot h) \stackrel{G2}{=} h^{-1}\cdot h \stackrel{G3}{=} e.\end{aligned}$$

Mithin ist $h^{-1}g^{-1}$ ein Inverses zu gh, und somit

$$(gh)^{-1} = h^{-1}g^{-1}.$$

b. Die erste Kürzungsregel folgt durch Multiplikation mit dem Inversen zu g von links:[7]

$$\begin{aligned} a &\stackrel{G2}{=} e\cdot a \stackrel{G3}{=} \left(g^{-1}\cdot g\right)\cdot a \stackrel{G1}{=} g^{-1}\cdot(g\cdot a)\\ &\stackrel{\text{Vor.}}{=} g^{-1}\cdot(g\cdot b) \stackrel{G1}{=} \left(g^{-1}\cdot g\right)\cdot b \stackrel{G3}{=} e\cdot b \stackrel{G2}{=} b.\end{aligned}$$

Entsprechend folgt die zweite Kürzungsregel durch Multiplikation mit g^{-1} von rechts und unter Berücksichtigung der zusätzlichen Eigenschaft des Inversen aus Lemma 1.4. Die Details überlassen wir dem Leser.

□

Bemerkung 1.7

In den Beweisen der obigen beiden Lemmata haben wir wiederholt das Assoziativgesetz auf Terme mit verschachtelter Klammersetzung angewandt. Wir haben dies in sehr kleinen Schritten getan, werden aber in Zukunft beim Umsetzen von Klammern meist mehrere Schritte zusammenfassen. Daraus sollten keine Unklarheiten entstehen. □

Wiederholtes Multiplizieren einer Zahl mit sich selbst sind wir gewohnt als Potenzieren zu schreiben. Diese Schreibweise übernehmen wir auch bei Gruppen.

Definition 1.8

Sei $(G,\cdot)$ eine Gruppe, $g\in G$. Wir setzen $g^0 := e$, und für $n\in\mathbb{Z}$, $n>0$, definieren wir rekursiv $g^n := g\cdot g^{n-1}$, und schließlich $g^{-n} := (g^{-1})^n$.

Bei dieser Definition haben wir eine Eigenschaft der natürlichen Zahlen verwendet, die jedem wohlbekannt ist, und auch als *Prinzip der vollständigen Induktion* bezeichnet wird:

> *Ausgehend von einer natürlichen Zahl n_0 kann man durch wiederholtes Addieren der Zahl 1 jede andere natürliche Zahl erreichen, die größer als n_0 ist.*

[7] Das Kürzel *Vor.* über einem Gleichheitszeichen in einer Gleichung deutet an, daß die Gleichung *nach Voraussetzung* gilt. In diesem Falle war $ga = gb$ vorausgesetzt.

Wollte man die natürlichen Zahlen *axiomatisch* einführen, so wäre dieses eines der Axiome. Für uns ist es einfach eine der bekannten Eigenschaften der natürlichen Zahlen. Wir haben diese Eigenschaft bereits verwendet, als wir die n-te Potenz g^n von g *rekursiv* definiert haben. Dazu haben wir nämlich zunächst einmal g^n für $n = 0$ definiert und dann die Definition von g^n für $n > 0$ auf die Definition von g^{n-1} zurück geführt.

Man kann diese Eigenschaft der natürlichen Zahlen oft dann als Beweistechnik einsetzen,

- wenn man eine Aussage $\mathcal{A}$ beweisen will, die von einer natürlichen Zahl n abhängt, und
- wenn man zudem diese Aussage für eine beliebige Wahl von $n \geq n_0$ zeigen will.

Die Abhängigkeit der Aussage $\mathcal{A}$ von der natürlichen Zahl n drückt man dann dadurch aus, daß man sie als Index anhängt, sprich $\mathcal{A}_n$ statt nur $\mathcal{A}$ schreibt. Ein typisches Beispiel für eine solche Aussage wäre

$$\mathcal{A}_n : \textit{eine Zahl der Form } n^3 - n \textit{ ist durch } 6 \textit{ teilbar}$$

wobei hier $n \in \mathbb{N}$ irgend eine natürliche Zahl größer oder gleich Null sein darf, d.h. $n_0 = 0$ in diesem Beispiel. Will man diese Aussage $\mathcal{A}_n$ nun für jedes $n \geq n_0$ zeigen, so zeigt man sie zunächst für die Zahl n_0 selbst (dies nennt man den *Induktionsanfang*) und zeigt dann, wenn sie für eine feste Zahl n bereits gilt (anzunehmen, daß sie für n gilt, nennt man die *Induktionsvoraussetzung*), gilt sie auch für die nachfolgende Zahl $n + 1$ (dies nennt man den *Induktionsschritt*). Die oben beschriebene Eigenschaft der natürlichen Zahlen erlaubt es uns dann, ausgehend von der Korrektheit von $\mathcal{A}_{n_0}$ auf die von $\mathcal{A}_{n_0+1}$ zu schließen, dann auf die von $\mathcal{A}_{n_0+2}$ und so fortfahrend auf die Korrektheit der Aussage $\mathcal{A}_n$ für jede natürliche Zahl $n \geq n_0$. Wir überlassen es dem Leser, die Aussage aus unserem Beispiel zu beweisen, und formulieren das Prinzip der vollständigen Induktion als Beweisprinzip noch einmal etwas kompakter.

Bemerkung 1.9 (Prinzip der vollständigen Induktion)
Es gelte eine Aussage $\mathcal{A}_n$ für die natürliche Zahl $n = n_0$ (*Induktionsanfang*), außerdem sei folgendes richtig: gilt die Aussage für ein $n \geq n_0$ (*Induktionsvoraussetzung*), so gilt sie auch für $n + 1$ (*Induktionsschluß*). Dann gilt die Aussage für alle natürlichen Zahlen $n \geq n_0$. □

Wendet man diese Beweistechnik an und sind die Aussagen mit n induziert, so sagt man auch, man führe den Beweis durch *Induktion nach* n. Sofern es nicht bereits aus der Vorlesung *Grundlagen der Mathematik* bekannt ist, wird der Beweis der Potenzgesetze zeigen, wie man das Prinzip der vollständigen Induktion als Beweistechnik einsetzen kann.

Lemma 1.10 (Potenzgesetze)
Sei $(G, \cdot)$ *eine Gruppe,* $g \in G$*,* $n, m \in \mathbb{Z}$*, so gelten die Potenzgesetze:*

$$g^n \cdot g^m = g^{n+m} \qquad \textit{und} \qquad (g^m)^n = g^{m \cdot n}.$$

Beweis: Wir wollen zunächst zeigen, daß

$$g^n = (g^{-1})^{-n}. \tag{9}$$

Ist $n < 0$, so gilt dies nach Definition. Ist $n > 0$, so ist $-n < 0$ und nach Definition und Lemma 1.6 gilt wieder:[8]

$$(g^{-1})^{-n} \stackrel{\text{Def.}}{=} \left((g^{-1})^{-1}\right)^{-(-n)} \stackrel{\text{Lem. 1.6}}{=} g^n.$$

Und wenn schließlich $n = 0$, dann ist $g^n = e = (g^{-1})^{-n}$ nach Definition. Damit ist (9) gezeigt.

Als nächstes zeigen wir einen Spezialfall des ersten Potenzgesetzes, nämlich, daß

$$g \cdot g^n = g^{n+1}. \tag{10}$$

für alle ganzen Zahlen $n \in \mathbb{N}$ gilt. Ist $n \geq 0$, so folgt dies aus der Definition. Ist $n < 0$, so ist $-n - 1 \geq 0$ und nach Definition gilt

$$\left(g^{-1}\right) \cdot g^{n+1} \stackrel{(9)}{=} \left(g^{-1}\right) \cdot \left(g^{-1}\right)^{-n-1} \stackrel{\text{Def}}{=} \left(g^{-1}\right)^{-n-1+1} = \left(g^{-1}\right)^{-n} \stackrel{(9)}{=} g^n. \tag{11}$$

Multipliziert man nun beide Seiten der Gleichung mit g, so erhalten wir

$$g \cdot g^n \stackrel{(11)}{=} g \cdot \left(g^{-1} \cdot g^{n+1}\right) \stackrel{\text{G1}}{=} \left(g \cdot g^{-1}\right) \cdot g^{n+1} \stackrel{\text{G3}}{=} e_G \cdot g^{n+1} \stackrel{\text{G2}}{=} g^{n+1}.$$

Damit ist auch (10) gezeigt.

Wenden wir uns nun der allgemeinen Regel

$$g^n \cdot g^m = g^{n+m} \tag{12}$$

für $n, m \in \mathbb{Z}$ zu, und führen den Beweis durch Fallunterscheidung.

<u>1. Fall: $n \geq 0$.</u> Wir wollen diesen Fall durch *Induktion nach* n *beweisen.* Sauberer formuliert wollen wir für beliebige, aber fest gegebene $g \in G$ und $m \in \mathbb{Z}$ zeigen, daß die Aussage

$$\mathcal{A}_n : \qquad g^n \cdot g^m = g^{n+m}$$

für alle $n \in \mathbb{N}$ korrekt ist. Dazu müssen wir zunächst den sogenannten *Induktionsanfang* zeigen, d.h. daß die Aussage für einen Startwert gilt – in Bemerkung 1.9 war das das n_0, hier ist die Zahl 0.

Ist $n = 0$, dann gilt

$$g^n \cdot g^m \stackrel{n=0}{=} g^0 \cdot g^m \stackrel{\text{Def.}}{=} e \cdot g^m \stackrel{\text{G2}}{=} g^m \stackrel{n=0}{=} g^{n+m}.$$

Damit ist der Induktionsanfang $\mathcal{A}_0$ gezeigt. Nun müssen wir den *Induktionsschritt* zeigen, d.h. wann immer die Aussage für eine Zahl n gilt dann gilt sie auch für

[8] Das Kürzel *Def.* über einem Gleichheitszeichen deutet an, daß die Gleichheit *nach Definition* gilt.

den folgenden Wert $n+1$. Dazu dürfen wir die *Induktionsvoraussetzung*, daß $\mathcal{A}_n$ für ein gegebenes $n \geq 0$ richtig ist, als korrekt annehmen, und müssen daraus die Korrektheit von $\mathcal{A}_{n+1}$ folgern: Nach Definition und Induktionsvoraussetzung gilt[9]

$$g^{n+1} \cdot g^m \overset{\text{Def.}}{=} (g \cdot g^n) \cdot g^m \overset{\text{G1}}{=} g \cdot (g^n \cdot g^m) \overset{\text{Ind.}}{=} g \cdot g^{n+m} \overset{(10)}{=} g^{n+1+m}.$$

Damit haben wir gezeigt, daß sich aus der Annahme der Korrektheit von $\mathcal{A}_n$ die Korrektheit von $\mathcal{A}_{n+1}$ ableiten läßt. Das Prinzip der vollständigen Induktion erlaubt uns nun hieraus und aus dem Umstand, daß die Aussage für $n = 0$ richtig ist, abzuleiten, daß die Aussage $\mathcal{A}_n$ für alle $n \geq 0$ korrekt ist. Es bleibt, den Fall $n < 0$ zu betrachten.

$\underline{\text{2. Fall: } n < 0.}$ Aus dem 1. Fall (angewendet auf g^{-1} und $-m$) folgt (da $-n > 0$):

$$g^n \cdot g^m \overset{(9)}{=} (g^{-1})^{-n} \cdot (g^{-1})^{-m} \overset{\text{1. Fall}}{=} (g^{-1})^{-n-m} \overset{(9)}{=} g^{n+m}.$$

Damit ist das erste der Potzenzgesetze (12) gezeigt, und wir wollen daraus zunächst

$$(g^n)^{-1} = g^{-n}. \tag{13}$$

als Spezialfall des zweiten Potenzgesetzes ableiten. Aus $g^{-n} \cdot g^n = g^{-n+n} = g^0 = e$ folgt, daß g^{-n} ein Inverses zu g^n ist, und somit gilt (13) wegen der Eindeutigkeit des Inversen.

Damit können wir nun das zweite Potenzgesetz, d.h.

$$(g^m)^n = g^{m \cdot n}$$

für $m, n \in \mathbb{Z}$, zeigen, was wir wieder durch die Betrachtung verschiedener Fälle tun wollen.[10]

$\underline{\text{1. Fall: } n \geq 0.}$ Wir wollen für beliebige, aber feste $g \in G$ und $m \in \mathbb{Z}$ durch Induktion nach n die Aussage

$$\mathcal{A}_n : \qquad (g^m)^n = g^{m \cdot n}$$

zeigen.

$\underline{n = 0:}$ Dann gilt

$$(g^m)^n \overset{n=0}{=} (g^m)^0 \overset{\text{Def.}}{=} e \overset{\text{Def.}}{=} g^0 \overset{n=0}{=} g^{m \cdot n}.$$

[9] Das Kürzel *Ind.* bedeutet, daß wir an der Stelle die *Induktionsvoraussetzung* einsetzen, nach der die Aussage $\mathcal{A}_n$ korrekt ist. In unserer Situation bedeutet das, daß für die festen Werte m und n und für das feste $g \in G$ gilt, daß $g^n \cdot g^m = g^{n+m}$.

[10] Den ersten Fall $n \geq 0$ werden wir wieder mit Hilfe von Induktion nach n beweisen. Allerdings werden wir unsere Schreibweise eines Induktionsbeweises stark verkürzen. Wir wissen nun, daß wir die Aussage, die zu beweisen gilt, stets für den ersten Wert, für den sie gelten soll, zeigen müssen (*Induktionsanfang*) und daß wir stets unter der Annahme, daß die Aussage für ein festes n gilt (*Induktionsvoraussetzung*), herleiten müssen, daß sie auch für $n+1$ gilt (*Induktionsschritt*). Wir werden dies verkürzt schreiben als $\underline{n = 0}$ für den *Induktionsanfang* und als $\underline{n \mapsto n+1}$ für den *Induktionsschritt*. Diese kürzere Schreibweise ist zwar gewöhnungsbedürftig, hat aber den Vorteil, daß sie nicht durch allzuviel Text den Blick auf das Wesentliche versperrt.

$\underline{n \mapsto n+1:}$ Nach Definition, Induktionsvoraussetzung und dem 2. Potenzgesetz gilt:

$$(g^m)^{n+1} \overset{\text{Def.}}{=} (g^m) \cdot (g^m)^n \overset{\text{Ind.}}{=} g^m \cdot g^{m \cdot n} \overset{(12)}{=} g^{m+m \cdot n} \overset{\text{Def.}}{=} g^{m \cdot (n+1)}.$$

<u>2. Fall: $n < 0$.</u> Aus dem 1. Fall folgt dann (da $-n > 0$):

$$(g^m)^n \overset{(9)}{=} \left((g^m)^{-1}\right)^{-n} \overset{(13)}{=} (g^{-m})^{-n} \overset{\text{1. Fall}}{=} g^{(-m)\cdot(-n)} \overset{\text{Def.}}{=} g^{m \cdot n}.$$

□

Bemerkung 1.11
Ist $(H, \cdot)$ eine Halbgruppe (bzw. ein Monoid) und $g \in H$, so definiert man für $0 \neq n \in \mathbb{N}$ (bzw. $n \in \mathbb{N}$) das Element g^n analog und zeigt für $0 \neq n, m \in \mathbb{N}$ (bzw. $n, m \in \mathbb{N}$) die obigen Potenzgesetze mit den gleichen Beweisen. □

Bemerkung 1.12
Bisher haben wir die Beweise in sehr kleinen Schritten geführt und nach Möglichkeit jede Umformung einer Gleichung durch Angabe einer Begründung über dem Gleichheitszeichen gerechtfertigt. Das Grundprinzip sollte mittlerweile verstanden sein, und wir werden deshalb von jetzt an sparsamer mit Umformungsschritten und Begründungen sein. □

Alle in Beispiel 1.3 betrachteten Beispiele von Gruppen waren abelsch. In einer abelschen Gruppe gilt das Kommutativgesetz und die Rechenregel "$(gh)^{-1} = h^{-1}g^{-1}$" nimmt die vielleicht eher erwartete Form "$(gh)^{-1} = g^{-1}h^{-1}$" an. Um zu sehen, daß dies im Allgemeinen falsch ist, braucht man notwendig ein Beispiel für eine Gruppe, in der das Kommutativgesetz G4 nicht gilt. Dazu erinnern wir uns an *bijektive Abbildungen* (siehe Definition B.8) sowie deren *Komposition* (siehe Definition B.14).

Definition 1.13
Für eine nicht-leere Menge M definieren wir

$$\text{Sym}(M) := \{f : M \to M \mid f \text{ ist bijektiv}\}.$$

Die Komposition $\circ$ definiert eine zweistellige Operation auf $\text{Sym}(M)$, und wir nennen das Paar $(\text{Sym}(M), \circ)$ die *symmetrische Gruppe auf der Menge* M. Die Elemente von $\text{Sym}(M)$ werden auch *Permutationen* von M genannt.

Ist $M = \{1, \ldots, n\}$, so schreiben wir $\mathbb{S}_n$ statt $\text{Sym}(M)$ und wir nennen $\mathbb{S}_n$ die *symmetrische Gruppe auf* n *Ziffern* oder die *Permutationsgruppe vom Grad* n.

Damit der Begriff symmetrische *Gruppe* gerechtfertigt ist, müssen wir zeigen, daß $(\text{Sym}(M), \circ)$ in der Tat eine Gruppe ist.

Proposition 1.14
$(\text{Sym}(M), \circ)$ *ist eine Gruppe, die genau dann abelsch ist, wenn* $|M| \leq 2$. *Das neutrale Element ist* id_M, *und das Inverse zu einer Abbildung* $f \in \text{Sym}(M)$ *ist ihre Umkehrabbildung.*

Beweis: Zunächst wollen wir uns davon überzeugen, daß die Komposition zweier bijektiver Abbildung wieder bijektiv ist, sprich, daß das Bild der Abbildung "$\circ$" auch wirklich wieder in $\mathrm{Sym}(M)$ liegt.

Sind $f, g : M \to M$ bijektiv, so existieren Abbildungen $f^{-1} : M \to M$ und $g^{-1} : M \to M$ nach Lemma B.20, und für diese gilt (unter Verwendung der Assoziativität der Komposition, Lemma B.15):

$$(f \circ g) \circ \left(g^{-1} \circ f^{-1}\right) = f \circ \left(g \circ g^{-1}\right) \circ f^{-1} = f \circ \mathrm{id}_M \circ f^{-1} = f \circ f^{-1} = \mathrm{id}_M,$$

und analog $\left(g^{-1} \circ f^{-1}\right) \circ (f \circ g) = \mathrm{id}_M$. Folglich gilt wieder mit Lemma B.20, daß $f \circ g$ bijektiv ist.

Die Assoziativität von "$\circ$", sprich Axiom G1, ist bereits in Lemma B.15 gezeigt. Die Identität id_M auf M ist bijektiv (siehe Beispiel B.22) und hat die Eigenschaft, daß $\mathrm{id}_M \circ f = f$ für alle $f \in \mathrm{Sym}(M)$. Sie ist mithin das neutrale Element von $(\mathrm{Sym}(M), \circ)$. Die zu $f \in \mathrm{Sym}(M)$ nach Lemma B.20 existierende Umkehrabbildung ist, wie dort gezeigt, die Inverse im Sinne von Axiom G3. Also ist $(\mathrm{Sym}(M), \circ)$ eine Gruppe.

Es bleibt zu zeigen:

$$(\mathrm{Sym}(M), \circ) \text{ ist abelsch} \quad \Longleftrightarrow \quad |M| \leq 2.$$

Falls $|M| \geq 3$, so können wir drei paarweise verschiedene Elemente[11] $m, m', m'' \in M$ wählen und die Abbildungen

$$f : M \longrightarrow M : n \mapsto \begin{cases} m', & \text{falls } n = m, \\ m, & \text{falls } n = m', \\ n, & \text{sonst,} \end{cases}$$

und

$$g : M \longrightarrow M : n \mapsto \begin{cases} m'', & \text{falls } n = m, \\ m, & \text{falls } n = m'', \\ n, & \text{sonst} \end{cases}$$

betrachten. Man sieht sofort, daß $f \circ f = \mathrm{id}_M$ und $g \circ g = \mathrm{id}_M$, also sind f und g bijektive mit Umkehrabbildung $f^{-1} = f$ und $g^{-1} = g$. Zudem gilt nach Definition

$$(f \circ g)(m) = f\big(g(m)\big) = f(m'') = m'',$$

aber

$$(g \circ f)(m) = g\big(f(m)\big) = g(m') = m' \neq m''.$$

[11]Die drei Elemente heißen *paarweise verschieden* wenn $m \neq m'$, $m' \neq m''$ und $m'' \neq m$, wenn also je zwei der drei Element ungleich sind. Für Mengen mit beliebig vielen Elementen ist der Begriff analog zu verstehen.

Mithin ist $g \circ f \neq f \circ g$, und $(\mathrm{Sym}(M), \circ)$ ist nicht abelsch. Damit haben wir die Richtung "$\Longrightarrow$" der Aussage mittels *Kontraposition* bewiesen.[12] Die Richtung "$\Longleftarrow$" überlassen wir dem Leser als Aufgabe. □

Aufgabe 1.15
Untersuche, ob die folgende zweistellige Operation die Menge $G := \mathbb{Q} \times \mathbb{Q}$ zu einer Gruppe macht:

$$G \times G \longrightarrow G : \big((a, b), (a', b')\big) \mapsto (a, b) \cdot (a', b') := (aa', bb').$$

Aufgabe 1.16
Untersuche, ob die folgende zweistellige Operation die Menge $G := \mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$ zu einer Gruppe macht:

$$G \times G \longrightarrow G : \big((a, b), (a', b')\big) \mapsto (a, b) \cdot (a', b') := (aa', bb').$$

Aufgabe 1.17
Es seien $(G, \cdot)$ und $(H, *)$ zwei Gruppen. Wir definieren auf der Menge $G \times H = \{(x, y) \mid x \in G, y \in H\}$ eine zweistellige Operation durch

$$(x, y) \circ (x', y') := (x \cdot x', y * y')$$

für $(x, y), (x', y') \in G \times H$. Zeige, daß dann $(G \times H, \circ)$ eine Gruppe ist.

Aufgabe 1.18
Untersuche, welche der folgenden zweistelligen Operationen Gruppen definieren:

a. $G = \big(\mathbb{Q}\backslash\{0\}\big) \times \big(\mathbb{Q}\backslash\{0\}\big)$ mit $(a, b) \cdot (a', b') = (ab', ba')$ für $a, a', b, b' \in \mathbb{Q}\backslash\{0\}$,

b. $G = \mathbb{R} \times \mathbb{R} \backslash \big\{(0, 0)\big\}$ mit $(a, b) \cdot (a', b') = (aa' - bb', ab' + ba')$ für $a, a', b, b' \in \mathbb{R}$.

Aufgabe 1.19
Finde alle möglichen zweistelligen Operationen auf der Menge $G = \{e, a, b\}$, bezüglich derer G eine Gruppe mit neutralem Element e wird.

Aufgabe 1.20
Finde alle möglichen zweistelligen Operationen auf der Menge $G = \{e, a, b, c\}$, bezüglich derer G eine Gruppe mit neutralem Element e wird. Dabei sollten nur Möglichkeiten aufgelistet werden, die nicht durch Vertauschung der Buchstaben a, b und c ineinander überführt werden können.

Aufgabe 1.21
Ein Schema der Form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

[12] Eine Folgerung "$A \Longrightarrow B$" durch *Kontraposition* zu zeigen bedeutet, stattdessen die Folgerung "$\neg B \Longrightarrow \neg A$" zu zeigen. Die beiden Folgerungen sind gleichwertig, besitzen also den gleichen Wahrheitswert, d.h. ist die eine wahr so ist es die andere und umgekehrt.

mit $a, b, c, d \in \mathbb{R}$ wollen wir eine *relle 2x2-Matrix* nennen, und $\mathrm{Mat}_2(\mathbb{R})$ soll die Menge solcher Matrizen sein. Für zwei relle 2x2-Matrizen definieren wir ihr Produkt als

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Ferner bezeichnen wir

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in \mathbb{R}$$

als *Determinante* der Matrix, und definieren

$$\mathrm{Gl}_2(\mathbb{R}) = \{A \in \mathrm{Mat}_2(\mathbb{R}) \mid \det(A) \neq 0\}.$$

Zeige:

a. Für $A, B \in \mathrm{Mat}_2(\mathbb{R})$ gilt $\det(A \cdot B) = \det(A) \cdot \det(B)$.

b. $\big(\mathrm{Gl}_2(\mathbb{R}), \cdot\big)$ ist eine nicht-abelsche Gruppe.

Aufgabe 1.22
Es sei $(G, \cdot)$ eine Gruppe und $a \in G$ sei fest gegeben. Wir definieren eine zweistellige Operation auf G durch

$$* : G \times G \longrightarrow G : (g, h) \mapsto g * h = g \cdot \big(a^{-1} \cdot h\big).$$

Überprüfe, ob $(G, *)$ eine Gruppe ist?

Aufgabe 1.23 (Boolsche Gruppe)
Es sei M eine Menge.

a. Sind $X, Y, Z \subseteq M$, dann gelten

$$X \setminus \big((Y \setminus Z) \cup (Z \setminus Y)\big) = \big(X \setminus (Y \cup Z)\big) \cup (X \cap Y \cap Z)$$

und

$$\big((X \setminus Y) \cup (Y \setminus X)\big) \setminus Z = \big(X \setminus (Y \cup Z)\big) \cup \big(Y \setminus (X \cup Z)\big).$$

b. Wir definieren auf der Potenzmenge $G = \mathcal{P}(M) = \{A \mid A \subseteq M\}$ von M eine zweistellige Operation durch

$$A + B := (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

für $A, B \in G$. Zeige, $(G, +)$ ist eine abelsche Gruppe.

Aufgabe 1.24
Es sei $(G, \cdot)$ ein Gruppe mit neutralem Element e. Zeige, falls $g^2 = e$ für alle $g \in G$, so ist G abelsch.

Aufgabe 1.25
Sei M eine Menge, $m \in M$, $k \in \mathbb{N}$ und $\sigma \in \mathrm{Sym}(M)$ mit $\sigma^k(m) = m$. Zeige, dann ist auch $\sigma^{q \cdot k}(m) = m$ für alle $q \in \mathbb{Z}$.

B) **Untergruppen**

Ein wichtiges Prinzip in der Mathematik ist es, zu jeder betrachteten Struktur auch ihre *Unter-* oder *Teilstrukturen* zu betrachten. Für eine Menge sind das einfach ihre Teilmengen, für eine Gruppe werden es ihre *Untergruppen* sein – das sind Teilmengen, die die zusätzliche Struktur *respektieren*. Eine *Gruppe* besteht aus einer Menge G und zusätzlich einer zweistelligen Operation $\cdot : G \times G \to G$, die gewissen Axiomen genügt. Ist $U \subseteq G$ eine Teilmenge von G, so kann man die Abbildung "$\cdot$" auf $U \times U$ einschränken und erhält eine Abbildung

$$U \times U \longrightarrow G : (u, v) \mapsto u \cdot v,$$

wobei der Ausdruck $u \cdot v$ ein Element aus G ist, in aller Regel aber nicht in U liegt. Letzteres bedeutet, daß die Einschränkung von "$\cdot$" auf $U \times U$ in aller Regel keine zweistellige Operation auf U definiert! Das ist aber sicher eine Minimalforderung an U um zu sagen, daß U die Gruppenoperation "$\cdot$" respektiert. Nehmen wir nun an, daß wider Erwarten die Einschränkung von "$\cdot$" tatsächlich eine zweistellige Operation auf U definiert, dann stellt sich die Frage, ob das Paar bestehend aus U und der Einschränkung von "$\cdot$" den Gruppenaxiomen G1-G3 genügt, sprich selbst eine Gruppe ist – und erst in letzterem Fall kann man wirklich guten Gewissens sagen, die Teilmenge U respektiere die zusätzliche Struktur. Diese Überlegungen führen zur Definition des Begriffs der *Untergruppe*, und lassen sich im Übrigen auf alle weiteren von uns betrachteten algebraischen Strukturen übertragen.

Definition 1.26
Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ heißt *Untergruppe* von G, wenn

$$u \cdot v \in U \quad \text{für alle } u, v \in U$$

und zudem $(U, \cdot)$ eine Gruppe ist, d. h. die Einschränkung der Operation "$\cdot$" auf $U \times U$ macht U zu einer Gruppe.

Notation 1.27
Ist $(G, \cdot)$ eine Gruppe und $U \subseteq G$, so wollen wir durch die Schreibweise $U \leq G$ ausdrücken, daß U eine Untergruppe von $(G, \cdot)$ ist.

Bevor wir uns Beispiele von Untergruppen anschauen, wollen wir ein Kriterium formulieren, das die Überprüfung, ob eine Teilmenge einer Gruppe eine Untergruppe ist, deutlich vereinfacht.

Proposition 1.28 (Untergruppenkriterium)
Sei $(G, \cdot)$ eine Gruppe und $\emptyset \neq U \subseteq G$ eine nicht-leere Teilmenge. Dann sind gleichwertig:

a. U *ist eine Untergruppe von* G,

b. $\forall\, u, v \in U$ *gilt:* $uv \in U$ *und* $u_G^{-1} \in U$.

Man bezeichnet die Eigenschaften in b. als die Abgeschlossenheit *von* U *bezüglich der Gruppenoperation und der Inversenbildung.*

Beweis: "a. $\Rightarrow$ b.": Sei zunächst U eine Untergruppe von G. Nach Definition bedeutet dies, daß das Bild von $U \times U$ unter der Abbildung "$\cdot$" in U liegt, d. h. für $u, v \in U$ gilt $uv \in U$. Außerdem gelten in U die Gruppenaxiome. Sei also $e_U \in U$ das Neutrale in U und $e_G \in G$ das Neutrale in G. Ferner bezeichne zu $u \in U \subseteq G$ u_G^{-1} das Inverse zu u in G und u_U^{-1} das Inverse zu u in U, d. h. $u_G^{-1}u = uu_G^{-1} = e_G$ und $u_U^{-1}u = uu_U^{-1} = e_U$. In der folgenden Gleichung benötigen wir das Inverse von e_U in der Gruppe G, was in unserer Notation zu dem etwas unübersichtlichen $(e_U)_G^{-1}$ wird. Mit dieser Schreibweise gilt nun:

$$e_U \overset{\text{G2 in G}}{=} e_G e_U \overset{\text{G3 in G}}{=} \big((e_U)_G^{-1} e_U\big) e_U \overset{\text{G1 in G}}{=} (e_U)_G^{-1}(e_U e_U) \overset{\text{G2 in U}}{=} (e_U)_G^{-1} e_U \overset{\text{G3 in G}}{=} e_G. \tag{14}$$

Zudem gilt aber

$$u_U^{-1}u \overset{\text{G3 in U}}{=} e_U \overset{(14)}{=} e_G,$$

also ist $u_U^{-1} = u_G^{-1}$ wegen der Eindeutigkeit des Inversen in G, und damit $u_G^{-1} \in U$.
"a. $\Leftarrow$ b.": Da $uv \in U$ für alle $u, v \in U$, ist das Bild von $U \times U$ unter der Abbildung "$\cdot$" in der Tat in U enthalten. Es bleibt also, die Axiome G1-G3 nachzuprüfen. Dabei überträgt sich G1 von der größeren Menge G auf die Teilmenge U. Da $U \neq \emptyset$, existiert ein $u \in U$. Nach Voraussetzung gilt dann aber $u_G^{-1} \in U$ und damit $e_G = u_G^{-1}u \in U$. Da aber $e_G u = u$ für alle $u \in U$, ist auch G2 erfüllt und es gilt $e_U = e_G$. Ferner haben wir bereits bemerkt, daß für $u \in U$ auch $u_G^{-1} \in U$, und es gilt

$$u_G^{-1} \cdot u = e_G = e_U.$$

Somit ist auch G3 erfüllt und die Inversen von u in U bzw. in G stimmen überein. □

Ein Teil des Beweises des Untergruppenkriteriums ist die Aussage des folgenden Korollars.

Korollar 1.29
Ist $(G, \cdot)$ *eine Gruppe und* $U \leq G$*, so stimmen das neutrale Element* e_U *der Gruppe* $(U, \cdot)$ *und das neutrale Element* e_G *der Gruppe* $(G, \cdot)$ *überein. Außerdem gilt für jedes Element* $u \in U$*, daß das Inverse* u_U^{-1} *von* u *in* $(U, \cdot)$ *mit dem Inversen* u_G^{-1} *von* u *in* $(G, \cdot)$ *übereinstimmt.*

Wir wollen das Untergruppenkriterium nun anwenden um Untergruppen der zuvor betrachteten Gruppen zu finden. Man interessiert sich im Übrigen auch deshalb für die Untergruppen einer Gruppe, weil die Kenntnis dieser wichtige Informationen über die Struktur der Gruppe selbst liefert.

Beispiel 1.30

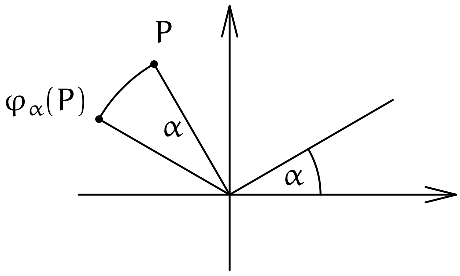
a. Ist $(G, \cdot)$ eine Gruppe mit neutralem Element e_G, so sind die beiden Teilmengen $\{e_G\}$ und G von G stets Untergruppen. Man nennt sie deshalb auch die *trivialen Untergruppen.* Sie geben keine zusätzliche Information über die Struktur der Gruppe selbst.

b. $(\{-1,1\},\cdot)$ ist eine Untergruppe von $(\mathbb{Q}\setminus\{0\},\cdot)$, wie unmittelbar aus Proposition 1.28 folgt.

c. Für $\alpha \in \mathbb{R}$ bezeichnet

$$\varphi_\alpha : \mathbb{R}^2 \to \mathbb{R}^2 : (x,y) \to \big(\cos(\alpha)\cdot x - \sin(\alpha)\cdot y, \sin(\alpha)\cdot x + \cos(\alpha)\cdot y\big)$$

die Drehung der Ebene $\mathbb{R}^2$ um den Nullpunkt um den Winkel α im Bogenmaß.

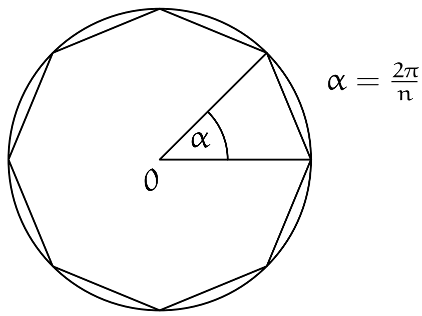


Offensichtlich gilt $\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha+\beta}$ für $\alpha, \beta \in \mathbb{R}$, und für $\alpha \in \mathbb{R}$ ist somit $\varphi_{-\alpha} = (\varphi_\alpha)^{-1}$, da $\varphi_0 = \mathrm{id}_{\mathbb{R}^2}$. Insbesondere ist φ_α also bijektiv für jedes $\alpha \in \mathbb{R}$. Damit folgt aus Proposition 1.28, daß

$$\mathrm{SO}(2) := \{\varphi_\alpha : \mathbb{R}^2 \to \mathbb{R}^2 \mid \alpha \in \mathbb{R}\}$$

eine Untergruppe von $\mathrm{Sym}\left(\mathbb{R}^2\right)$ ist.

d. Sei $E_n \subset \mathbb{R}^2$ das *reguläre* n-*Eck.*



Wir setzen

$$U := \big\{\varphi_\alpha \in \mathrm{SO}(2) \;\big|\; \varphi_\alpha(E_n) = E_n\big\}.$$

Behauptung: $(U,\circ)$ ist eine Untergruppe von $\big(\mathrm{SO}(2),\circ\big)$.

Für $\varphi_\alpha, \varphi_\beta \in U$ gilt

$$(\varphi_\alpha \circ \varphi_\beta)(E_n) = \varphi_\alpha\big(\varphi_\beta(E_n)\big) = \varphi_\alpha(E_n) = E_n$$

und

$$\varphi_\alpha^{-1}(E_n) = \varphi_\alpha^{-1}\big(\varphi_\alpha(E_n)\big) = \big(\varphi_\alpha^{-1} \circ \varphi_\alpha\big)(E_n) = \mathrm{id}_{\mathbb{R}^2}(E_n) = E_n.$$

Also gilt $\varphi_\alpha \circ \varphi_\beta \in U$ und $\varphi_\alpha^{-1} \in U$, und da $\mathrm{id}_{\mathbb{R}^2} = \varphi_0 \in U$, ist $U \neq \emptyset$ und folglich ist U nach Proposition 1.28 eine Untergruppe von $\mathrm{SO}(2)$.

Man überzeugt sich leicht, daß U aus allen Drehungen φ_α mit $\alpha = k \cdot \frac{2\pi}{n}$, $k = 0, \ldots, n-1$, besteht. Insbesondere gilt also, $|U| = n$.

e. Sei $n \in \mathbb{Z}$ und $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ die Menge aller Vielfachen von n.

   Behauptung: $(n\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$.

   Seien $nz, nz' \in n\mathbb{Z}$, dann gilt $nz + nz' = n(z + z') \in n\mathbb{Z}$ und $-(nz) = n \cdot (-z) \in n\mathbb{Z}$. Da ferner $\emptyset \neq n\mathbb{Z} \subset \mathbb{Z}$, folgt wieder mit Proposition 1.28 die Behauptung.

f. Für zwei ganze Zahlen $m, n \in \mathbb{Z}$ gilt $m\mathbb{Z} \subseteq n\mathbb{Z}$ genau dann, wenn m ein Vielfaches von n ist.

g. Die Inklusionen $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Z} \subset \mathbb{R}$ und $\mathbb{Q} \subset \mathbb{R}$ machen die Teilmenge bezüglich der Addition als Gruppenstruktur jeweils zu Untergruppen.

Bemerkung 1.31
Wie verhalten sich Untergruppen gegenüber Mengenoperationen wie z.B. der Vereinigung?

Betrachten wir die Gruppe $(\mathbb{Z}, +)$ und ihre Untergruppen $2\mathbb{Z} \leq \mathbb{Z}$ sowie $3\mathbb{Z} \leq \mathbb{Z}$. Die Menge $U = 2\mathbb{Z} \cup 3\mathbb{Z}$ ist nicht abgeschlossen bezüglich der Gruppenoperation, denn

$$2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z},$$

da 5 weder durch 2 noch durch 3 teilbar ist. Mithin ist die Vereinigung von Untergruppen im allgemeinen keine Untergruppe mehr.

Im Gegensatz zur Vereinigung verhalten sich Gruppen bei der Bildung von Schnittmengen gut.

Lemma 1.32
Es sei $(G, \cdot)$ eine Gruppe, I eine beliebige Indexmenge und $U_i \leq G$ für $i \in I$. Dann gilt

$$\bigcap_{i \in I} U_i \leq G.$$

Beweis: Wir überlassen den Beweis dem Leser als leichte Anwendung des Untergruppenkriteriums. □

Wir verwenden die gute Schnitteigenschaft der Untergruppen um den Makel der schlechten Vereinigung auszutilgen, und betrachten bei Gruppen statt der Vereinigung von Untergruppen stets das *Erzeugnis* der Vereinigung als kleinste Untergruppe, die die Vereinigung enthält, oder allgemeiner:

Definition 1.33
Es sei $(G, \cdot)$ eine Gruppe und $M \subseteq G$ eine Teilmenge. Das *Erzeugnis* von M ist die Untergruppe

$$\langle M \rangle = \bigcap_{M \subseteq U \leq G} U,$$

d.h. der Schnitt über alle Untergruppen von G, die M enthalten. Ist $M = \{g_1, \ldots, g_n\}$, so schreiben wir wir statt $\langle \{g_1, \ldots, g_n\} \rangle$ in aller Regel nur $\langle g_1, \ldots, g_n \rangle$.

Eine solche Definition ist nützlich, da sie frei Haus liefert, daß das Erzeugnis eine Untergruppe ist und daß es die *kleinste* Untergruppe ist, die M enthält. Sie ist aber wenig hilfreich, wenn man bei gegebenem M entscheiden soll, welche Elemente letztlich im Erzeugnis liegen. Dies wird durch die folgende Proposition beschrieben, die auch den Begriff *Erzeugnis* rechtfertigt, da die Elemente von $\langle M\rangle$ in der Tat durch die Elemente von M *erzeugt* werden.

Proposition 1.34
Es sei $(G,\cdot)$ *eine Gruppe und* $M \subseteq G$ *eine Teilmenge. Dann gilt*[13]

$$\langle M\rangle = \big\{g_1^{\alpha_1}\cdots g_n^{\alpha_n} \mid n \geq 0, g_1,\ldots,g_n \in M, \alpha_1,\ldots,\alpha_n \in \mathbb{Z}\big\}.$$

Beweis: Wir geben zunächst der rechten Seite der Gleichung einen Namen,

$$N = \{g_1^{\alpha_1}\cdots g_n^{\alpha_n} \mid n \geq 0, g_1,\ldots,g_n \in M, \alpha_1,\ldots,\alpha_n \in \mathbb{Z}\big\},$$

und zeigen, daß $N \subseteq \langle M\rangle$. Falls $U \leq G$, so daß $M \subseteq U$, dann ist $g_1^{\alpha_1}\cdots g_n^{\alpha_n} \in U$ für alle $g_i \in M$ und $\alpha_1,\ldots,\alpha_n \in \mathbb{Z}$. Also ist $N \subseteq U$, und damit $N \subseteq \langle M\rangle$.

Es bleibt zu zeigen, daß $\langle M\rangle \subseteq N$. Dafür reicht es aber zu zeigen, daß $N \leq G$ mit $M \subseteq N$. Da das leere Produkt nach Konvention das neutrale Element e_G ist, ist N nicht leer. Seien nun also $h = g_1^{\alpha_1}\cdots g_n^{\alpha_n}, h' = g_{n+1}^{\alpha_{n+1}}\cdots g_m^{\alpha_m} \in N$ zwei beliebige Elemente in N, dann gilt

$$h\cdot h' = g_1^{\alpha_1}\cdots g_m^{\alpha_m} \in N$$

und

$$h^{-1} = g_n^{-\alpha_n}\cdots g_1^{-\alpha_1} \in N.$$

Also ist $N \leq G$. Da aber $M \subseteq N$ ohnehin gilt, folgt die Behauptung. □

Beispiel 1.35
Ist $(G,\cdot)$ eine Gruppe und $g \in G$, so folgt aus Proposition 1.34

$$\langle g\rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

Wenden wir dies auf die Gruppe $(\mathbb{Z},+)$ und eine Zahl $n \in \mathbb{Z}$ an, so ist das Erzeugnis der Menge $M = \{n\}$ die Untergruppe

$$n\mathbb{Z} = \{n\cdot z \mid z \in \mathbb{Z}\} = \langle n\rangle = \langle M\rangle.$$

Definition 1.36
Eine Gruppe $(G,\cdot)$ heißt *zyklisch*, wenn sie von einem Element erzeugt wird, d.h. wenn es ein $g \in G$ gibt, so daß $G = \langle g\rangle$.

Für den Beweis der nächsten Proposition benötigt man das Prinzip der *Division mit Rest* in den ganzen Zahlen, eine Eigenschaft der ganzen Zahlen, die wir als bekannt voraussetzen, die sich aber auch leicht durch Induktion herleiten läßt, wie wir der Vollständigkeit halber weiter unten in Bemerkung 1.39 zeigen. Zudem werden wir das

[13]Man beachte, daß wir für $n = 0$ das leere Produkt erhalten, das wir als das Neutrale Element e_G definieren.

Archimedische Prinzip der natürlichen Zahlen verwenden, dessen Aussage ebenfalls wohlbekannt sein dürfte.

Bemerkung 1.37 (Archimedisches Prinzip)
Jede nicht-leere Teilmenge der natürlichen Zahlen $\mathbb{N}$ besitzt ein kleinstes Element.

Proposition 1.38
$U \subseteq \mathbb{Z}$ ist genau dann eine Untergruppe von $(\mathbb{Z}, +)$, wenn es eine ganze Zahl $n \geq 0$ gibt mit $U = n\mathbb{Z} = \langle n \rangle$. Insbesondere ist jede Untergruppe von $(\mathbb{Z}, +)$ zyklisch.

Beweis: Aus Beispiel 1.30 und Beispiel 1.35 wissen wir, daß die Mengen der Form $n\mathbb{Z} = \langle n \rangle$ Untergruppen von $(\mathbb{Z}, +)$ sind.

Sei nun $U \leq \mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$ so bleibt zu zeigen, daß es ein $n \geq 0$ gibt mit $U = n\mathbb{Z}$. Ist $U = \{0\}$, so können wir $n = 0$ wählen. Ist $U \neq \{0\}$, so gibt es eine Zahl $0 \neq z \in U$ und eine der Zahlen $z \in U$ oder $-z \in U$ ist positiv. Also ist die Teilmenge

$$\{m \in \mathbb{N} \mid 0 \neq m \in U\}$$

der natürlichen Zahlen nicht leer und besitzt wegen des Archimedischen Prinzips somit ein kleinstes Element, d.h. die Zahl

$$n := \min\{z \in U \mid z > 0\} \in U$$

existiert.

Wir wollen zeigen, daß $U = \langle n \rangle$ gilt. Wegen $n \in U$ folgt $\langle n \rangle \subseteq U$ unmittelbar aus der Definition des Erzeugnisses. Sei nun umgekehrt $u \in U$ gegeben. Division von u durch n mit Rest liefert ganze Zahlen $q, r \in \mathbb{Z}$ mit

$$u = q \cdot n + r$$

und

$$0 \leq r < n. \tag{15}$$

Da sowohl u als auch n Elemente von U sind, folgt

$$r = u - q \cdot n \in U,$$

und da n die kleinste *echt positive* Zahl in U ist, bedingt (15), daß $r = 0$ gilt. Mithin ist $u = q \cdot n \in \langle n \rangle$. Damit haben wir $U = \langle n \rangle$ gezeigt. □

Bemerkung 1.39 (Division mit Rest)
Zu $m, n \in \mathbb{Z}$ mit $n \neq 0$ existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

$$m = qn + r \quad \text{und} \quad 0 \leq r < |n|. \tag{16}$$

Man bezeichnet dabei r auch als den *Rest von m modulo n*.

Beweis: Seien $m, n \in \mathbb{Z}$ gegeben mit $n \neq 0$. Wir wollen zunächst die Existenz von q und r zeigen und betrachten dazu verschiedene Fälle.

1. Fall: $n > 0$ und $m \geq 0$. Wir führen den Beweis mittels Induktion nach m und betrachten als Induktionsanfang alle m mit $0 \leq m < n$. In diesem Fall können wir $q = 0$ und $r = m$ wählen und sind fertig. Für den Induktionsschluß nehmen wir nun an, daß $m \geq n$ gilt und daß für alle echt kleineren nicht-negativen Zahlen entsprechende q's und r's existieren. Da $m \geq n$ ist $0 \leq m - n < m$, und nach Induktionsvoraussetzung existieren q', r' so daß

$$m - n = q' \cdot n + r' \quad \text{und} \quad 0 \leq r' < |n| = n.$$

Dann gilt (16) mit $q = q' + 1$ und $r = r'$.

2. Fall: $n \geq 1$ und $m < 0$. Wir setzen $m' = -m > 0$ und müssen zeigen, daß es $q, r \in \mathbb{Z}$ gibt mit

$$-m' = q \cdot n + r \quad \text{und} \quad 0 \leq r < n. \tag{17}$$

Wir führen den Beweis mittels Induktion nach m', wobei wir als Induktionsanfang diesmal alle $0 < m' \leq n$ betrachten. In letzterem Fall sind wir fertig mit $q = -1$ und $r = n - m' = n + m$. Für den Induktionsschluß können wir also annehmen, daß $m' > n$ und daß für alle kleineren positiven Zahlen m' entsprechende q's und r's existieren. Nach Voraussetzung ist also wieder $0 < m' - n < m'$, so daß wir aus der Induktionsvoraussetzung die Existenz von $q', r' \in \mathbb{Z}$ erhalten, für die gilt:

$$-(m' - n) = q' \cdot n + r' \quad \text{und} \quad 0 \leq r' < n.$$

Dann erfüllen aber $q = q' - 1$ und $r = r'$ die Gleichung (17).

3. Fall: $n < 0$. Wegen der bereits betrachteten Fälle und weil $-n > 0$ gibt es $q', r' \in \mathbb{Z}$, so daß

$$m = q' \cdot (-n) + r' \quad \text{und} \quad 0 \leq r' < |-n| = |n|.$$

Dann erfüllen aber $q = -q'$ und $r = r'$ die Gleichung (16).

Damit ist die Existenz von q und r gezeigt, und es bleibt, die Eindeutigkeit zu zeigen. Sei dazu $\big(q', r'\big)$ ein weiteres Zahlenpaar, für das (16) gilt, so folgt:

$$x = qy + r = q'y + r'. \tag{18}$$

O. E.[14] gilt $r' \geq r$, also $0 \leq r \leq r' < |y|$. Dann folgt aber aus (18)

$$0 \leq (q - q')y = r' - r < |y|.$$

Da $q - q' \in \mathbb{Z}$, muß folglich $q - q' = 0$ gelten, also $q = q'$ und dann auch $r = r'$. $\square$

Aufgabe 1.40
Beweise Lemma 1.32.

[14] O.E. ist die Abkürzung von *ohne Einschränkung* und bedeutet, daß man eigentlich zwei oder mehr Fälle betrachten müßte, daß aber alle Fälle das gleiche Lösungsmuster aufweisen. Deshalb beschränkt man sich darauf, einen der Fälle ausführlich zu zeigen, und überläßt es dem Leser, die übrigen Fälle selbst auszuführen. Hier wäre der 2. Fall $r' < r$, und der Beweis geht exakt gleich, wenn man in den Formeln r und r' sowie q und q' austauscht.

Aufgabe 1.41
Zeige, die Menge

$$U = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R}, (a,b) \neq (0,0) \right\}$$

ist eine Untergruppe von $\big(\mathrm{Gl}_2(\mathbb{R}), \cdot\big)$.

Aufgabe 1.42
Es sei $(G, \cdot)$ eine Gruppe, $g \in G$ und $\emptyset \neq U \subseteq G$ eine endliche Teilmenge von G.

a. Ist $\{g^n \mid n > 0\}$ endlich, so gibt es ein $n > 0$ mit $g^n = e_G$.

b. Genau dann ist U eine Untergruppe von G, wenn für alle $u, v \in U$ auch $u \cdot v \in U$.

Aufgabe 1.43
Welche der folgenden Mengen sind Untergruppen von $\big(\mathrm{Sym}(\mathbb{R}), \circ\big)$?

a. $U = \{f \in \mathrm{Sym}(\mathbb{R}) \mid f(x) < f(y) \text{ falls } x > y\}$,

b. $V = \{f \in \mathrm{Sym}(\mathbb{R}) \mid |f(x)| = |x| \text{ für alle } x \in \mathbb{R}\}$.

Aufgabe 1.44
Für zwei reelle Zahlen $a, b \in \mathbb{R}$ definieren wir die Abbildung

$$f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto a \cdot x + b.$$

Welche der folgenden Mengen sind Untergruppen von $\big(\mathrm{Sym}(\mathbb{R}), \circ\big)$?

a. $U = \{f_{a,b} \mid a, b \in \mathbb{R}, a \neq 0\}$,

b. $V = \{f_{a,1} \mid a \in \mathbb{R}, a \neq 0\}$.

Aufgabe 1.45
Sei $(G, \cdot)$ eine Gruppe. Zeige, daß die Menge

$$Z(G) := \{g \in G \mid g \cdot h = h \cdot g \ \ \forall\, h \in H\}$$

eine Untergruppe von G ist. Sie wird das Zentrum von G genannt.

C) Gruppenhomomorphismen

Immer wenn man eine Struktur auf einer Menge definiert hat, spielen die *strukturerhaltenden Abbildungen* eine besondere Rolle. Diese werden (Struktur-)*Morphismen* oder (Struktur-)*Homomorphismen* genannt.

Definition 1.46
Es seien $(G, \cdot)$ und $(H, *)$ zwei Gruppen. Eine Abbildung $\alpha : G \to H$ heißt *Gruppenhomomorphismus* (oder kürzer *Homomorphismus* oder nur *Morphismus*), falls für alle $g, h \in G$ gilt:

$$\alpha(g \cdot h) = \alpha(g) * \alpha(h).$$

Wieder wollen wir uns zunächst Beispiele anschauen.

Beispiel 1.47

a. Ist $(G, \cdot)$ eine Gruppe und $U \leq G$ eine Untergruppe, dann ist die kanonische Inklusion $i_U : U \to G$ ein Gruppenhomomorphismus, da für $g, h \in U$ gilt $i_U(g \cdot h) = g \cdot h = i_U(g) \cdot i_U(h)$.

b. Sei $a \in \mathbb{R}$ und $m_a : (\mathbb{R}, +) \to (\mathbb{R}, +) : g \mapsto ag$ die Multiplikation mit a, dann ist m_a ein Gruppenhomomorphismus, da für $g, h \in \mathbb{R}$ gilt

$$m_a(g + h) = a(g + h) = ag + ah = m_a(g) + m_a(h).$$

c. Ist $(G, \cdot)$ eine Gruppe und $g \in G$, so hat man Abbildungen

$$R_g : G \to G : h \mapsto hg \qquad \text{(die “\textit{Rechtstranslation}”)}$$

und

$$L_g : G \to G : h \mapsto gh \qquad \text{(die “\textit{Linkstranslation}”)}$$

Für $g \neq e$ gilt jedoch wegen der Kürzungsregel

$$L_g(g \cdot g) = g^3 \neq g^4 = L_g(g) \cdot L_g(g)$$

und entsprechend für R_g. Also sind L_g und R_g für $g \neq e$ *keine* Gruppenhomomorphismen. Man sieht leicht, daß L_g und R_g bijektive Abbildungen sind, mit Inverser $L_{g^{-1}}$ bzw. $R_{g^{-1}}$.

d. Ist $(G, \cdot)$ eine Gruppe und $g \in G$, so definiert man

$$i_g : G \to G : h \mapsto ghg^{-1} =: h^g.$$

i_g heißt *innerer Automorphismus* oder *Konjugation* mit g.

Behauptung: Die Konjugation ist ein bijektiver Gruppenhomomorphismus.

Für $h, k \in G$ gilt:

$$\begin{aligned} i_g(hk) =& g(hk)g^{-1} = g\big(hek\big)g^{-1} = g\big(h\big(g^{-1}g\big)k\big)g^{-1} \\ =& \big(ghg^{-1}\big)\big(gkg^{-1}\big) = i_g(h) \cdot i_g(k), \end{aligned}$$

also ist i_g ein Gruppenhomomorphismus. Außerdem gilt für ein beliebiges $h \in G$:

$$(i_g \circ i_{g^{-1}})(h) = g\Big(g^{-1}h\big(g^{-1}\big)^{-1}\Big)g^{-1} = \big(gg^{-1}\big)h\big(gg^{-1}\big) = ehe = h = \mathrm{id}_G(h),$$

also ist $i_g \circ i_{g^{-1}} = \mathrm{id}_G$. Analog sieht man $i_{g^{-1}} \circ i_g = \mathrm{id}_G$, und folglich ist i_g bijektiv mit Inverser $i_{g^{-1}}$ nach Lemma B.20.

Mit der Notation aus obigem Beispiel ist offenbar $i_g = R_g \circ L_{g^{-1}}$. Die Komposition zweier Nicht-Homomorphismen kann also durchaus ein Homomorphismus sein. Das folgende Lemma sagt, daß umgekehrt die Komposition zweier Homomorphismen stets wieder ein Homomorphismus ist.

Lemma 1.48

Sind $\alpha_1 : (G_1, \cdot) \to (G_2, *)$ und $\alpha_2 : (G_2, *) \to (G_3, \times)$ Gruppenhomomorphismen, so ist auch $\alpha_2 \circ \alpha_1 : (G_1, \cdot) \to (G_3, \times)$ ein Gruppenhomomorphismus.

Beweis: Seien $g, h \in G_1$, dann gilt:

$$
\begin{aligned}
(\alpha_2 \circ \alpha_1)(g \cdot h) = \alpha_2\big(\alpha_1(g \cdot h)\big) &= \alpha_2\big(\alpha_1(g) * \alpha_1(h)\big) = \alpha_2\big(\alpha_1(g)\big) \times \alpha_2\big(\alpha_1(h)\big) \\
&= (\alpha_2 \circ \alpha_1)(g) \times (\alpha_2 \circ \alpha_1)(h).
\end{aligned}
$$

□

Definition 1.49
Sei $\alpha : (G, \cdot) \to (H, *)$ ein Gruppenhomomorphismus.

a. Wir nennen α einen *Monomorphismus*, falls α injektiv ist.

b. Wir nennen α einen *Epimorphismus*, falls α surjektiv ist.

c. Wir nennen α einen *Isomorphismus*, falls α bijektiv ist.

d. Wir nennen α einen *Endomorphismus*, falls $(G, \cdot) = (H, *)$.

e. Wir nennen α einen *Automorphismus*, falls α ein bijektiver Endomorphismus ist.

f. Wir nennen die Gruppen $(G, \cdot)$ und $(H, *)$ *isomorph*, wenn es einen Isomorphismus $\alpha : G \to H$ gibt. Wir schreiben dann kurz $G \cong H$.

Beispiel 1.50

a. In Beispiel 1.47 ist m_a ein Endomorphismus. Zudem ist m_a ein Automorphismus mit Inverser $m_{\frac{1}{a}}$ genau dann wenn $a \neq 0$.

b. Ist $(G, \cdot)$ eine Gruppe und $g \in G$, dann ist die Konjugation i_g mit g nach Beispiel 1.47 ein Automorphismus mit Inverser $i_{g^{-1}}$.

c. Die Abbildung $\det : \big(\mathrm{Gl}_2(\mathbb{R}), \cdot\big) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$ aus Aufgabe 1.21 ist ein Epimorphismus.

Der Umstand, daß die Gruppenhomomorphismen die Gruppenstruktur *erhalten*, hat einige einfache, aber ungemein wichtige Auswirkungen.

Proposition 1.51
Es sei $\alpha : (G, \cdot) \to (H, *)$ ein Gruppenhomomorphismus. Dann gelten:

a. $\alpha(e_G) = e_H$.

b. $\alpha\big(g^{-1}\big) = \big(\alpha(g)\big)^{-1}$ *für* $g \in G$.

c. $\alpha\big(g^n\big) = \big(\alpha(g)\big)^n$ *für* $g \in G$ *und* $n \in \mathbb{Z}$.

d. *Ist α bijektiv, so ist $\alpha^{-1} : H \to G$ ein Gruppenhomomorphismus.*

e. *Ist* $U \leq G$*, dann ist* $\alpha(U) \leq H$. $\alpha(U)$ *heißt das* Bild *von* U *unter* α.

f. *Ist* $V \leq H$*, dann ist* $\alpha^{-1}(V) \leq G$. $\alpha^{-1}(V)$ *heißt das* Urbild *von* V *unter* α.

g. $\mathrm{Im}(\alpha) := \alpha(G)$*, das* Bild *von* α*, ist eine Untergruppe von* H.

h. $\mathrm{Ker}(\alpha) := \alpha^{-1}(e_H)$*, der* Kern *von* α*, ist eine Untergruppe von* G.

Beweis: a. Es gilt

$$e_H * \alpha(e_G) = \alpha(e_G) = \alpha(e_G \cdot e_G) = \alpha(e_G) * \alpha(e_G).$$

Mit Hilfe der Kürzungsregel 1.6 folgt dann $e_H = \alpha(e_G)$.

b. Für $g \in G$ gilt:

$$\alpha\big(g^{-1}\big) * \alpha(g) = \alpha\big(g^{-1} \cdot g\big) = \alpha(e_G) = e_H.$$

Wegen der Eindeutigkeit der Inversen in H folgt die Behauptung.

c. Es sei $g \in G$ und $n \in \mathbb{Z}$. Den Fall $n \geq 0$ beweisen wir mit Hilfe von Induktion nach n. Ist $n = 0$, so folgt die Behauptung aus a., und ist $n > 0$, so gilt nach Definition und mittels Induktion nach n

$$\alpha(g^n) = \alpha(g^{n-1} \cdot g) = \alpha(g^{n-1}) \cdot \alpha(g) \overset{\text{Ind.}}{=} \alpha(g)^{n-1} \cdot \alpha(g) = \alpha(g)^n. \tag{19}$$

Ist nun $n < 0$, so ist $-n > 0$ und es gilt wegen der Potzenzgesetze

$$\alpha(g^n) = \alpha\big((g^{-1})^{-n}\big) \overset{(19)}{=} \alpha\big(g^{-1}\big)^{-n} \overset{\text{b.}}{=} \big(\alpha(g)^{-1}\big)^{-n} = \alpha(g)^n.$$

d. Ist $\alpha : G \to H$ bijektiv, so existiert die Umkehrabbildung $\alpha^{-1} : H \to G$. Seien $u, v \in H$. Setze $g := \alpha^{-1}(u)$ und $h := \alpha^{-1}(v)$, also $u = \alpha(g)$ und $v = \alpha(h)$. Dann gilt:

$$\alpha^{-1}(u * v) = \alpha^{-1}\big(\alpha(g) * \alpha(h)\big) = \alpha^{-1}\big(\alpha(g \cdot h)\big) = g \cdot h = \alpha^{-1}(u) \cdot \alpha^{-1}(v).$$

Also ist α^{-1} ein Gruppenhomomorphismus.

e. Sind $u, v \in \alpha(U)$, dann existieren $g, h \in U$ mit $\alpha(g) = u$ und $\alpha(h) = v$. Da $g \cdot h \in U$, gilt:

$$u * v = \alpha(g) * \alpha(h) = \alpha(g \cdot h) \in \alpha(U).$$

Außerdem gilt $g^{-1} \in U$ und somit:

$$u^{-1} = \big(\alpha(g)\big)^{-1} = \alpha\big(g^{-1}\big) \in \alpha(U).$$

Da zudem $\alpha(e_G) \in \alpha(U)$, also $\alpha(U) \neq \emptyset$, folgt mit Proposition 1.28, daß $\alpha(U)$ eine Untergruppe von H ist.

f. Seien $g, h \in \alpha^{-1}(V)$, so gilt $\alpha(g \cdot h) = \alpha(g) * \alpha(h) \in V$, da V eine Untergruppe ist. Also gilt $g \cdot h \in \alpha^{-1}(V)$. Außerdem gilt $\alpha\big(g^{-1}\big) = \big(\alpha(g)\big)^{-1} \in V$, wieder da V eine Untergruppe ist. Somit liegt auch g^{-1} in $\alpha^{-1}(V)$. Da das Urbild von V unter α ferner nicht leer ist, weil wegen $\alpha(e_G) = e_H \in V$ gilt, daß $e_G \in \alpha^{-1}(V)$, folgt wieder mit Proposition 1.28, daß $\alpha^{-1}(V)$ eine Untergruppe von G ist.

g. Dies folgt aus e., da G eine Untergruppe von G ist.

h. Dies folgt aus f., da $\{e_H\}$ eine Untergruppe von H ist.

$\square$

Nach Definition muß man für die Injektivität einer Abbildung nachprüfen das jedes Element im Bild nur ein Urbild hat. Bei Gruppenhomomorphismen gibt es ein einfacheres Kriterium.

Lemma 1.52
Ein Gruppenhomomorphismus $\alpha : (G, \cdot) \to (H, *)$ *ist genau dann injektiv, wenn* $\mathrm{Ker}(\alpha) = \{e_G\}$.

Beweis: Ist α injektiv, so ist $\alpha^{-1}(e_H)$ höchstens einelementig, und wegen $\alpha(e_G) = e_H$ gilt dann $\mathrm{Ker}(\alpha) = \alpha^{-1}(e_H) = \{e_G\}$.

Gilt umgekehrt $\mathrm{Ker}(\alpha) = \{e_G\}$, und sind $g, h \in G$ mit $\alpha(g) = \alpha(h)$, so folgt wegen:

$$e_H = \alpha(g) * \big(\alpha(h)\big)^{-1} = \alpha(g) * \alpha\big(h^{-1}\big) = \alpha\big(g \cdot h^{-1}\big),$$

daß $g \cdot h^{-1} = e_G$, also $g = h$. Somit ist α injektiv. □

Aufgabe 1.53
Betrachte die Gruppe $(G, \cdot)$ aus Aufgabe 1.18 b. und die Gruppe $(U, \cdot)$ aus Aufgabe 1.41. Zeige, die Abbildung

$$\alpha : G \longrightarrow U : (a, b) \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

ist ein Gruppenisomorphismus.

Aufgabe 1.54
Wir betrachten die Gruppe $U = \{f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto ax + b \mid a, b \in \mathbb{R}, a \neq 0\}$ aus Aufgabe 1.44, wobei die Gruppenoperation die Verknüpfung von Abbildungen ist, sowie die Gruppe $(\mathbb{R} \setminus \{0\}, \cdot)$. Zeige, daß die Abbildung

$$\alpha : U \longrightarrow \mathbb{R} \setminus \{0\} : f_{a,b} \mapsto a$$

ein Gruppenhomomorphismus ist.

Aufgabe 1.55
Es sei $(G, \cdot)$ eine Gruppe und $g \in G$. Zeige:

a. Die Abbildung
$$\alpha : \mathbb{Z} \longrightarrow G : n \mapsto g^n$$
ist ein Gruppenhomomorphismus mit Bild $\mathrm{Im}(\alpha) = \langle g \rangle$.

b. α ist genau dann injektiv, wenn $g^k \neq g^l$ für alle $k, l \in \mathbb{Z}$ mit $k \neq l$.

c. Gibt es ganze Zahlen $k \neq l$ mit $g^k = g^l$, so existiert die Zahl
$$n = \min\{m \in \mathbb{N} \mid m > 0, g^m = e_G\}$$
und es gelten:
   (i) $\mathrm{Ker}(\alpha) = \{m \in \mathbb{Z} \mid g^m = e\} = n\mathbb{Z}$,
   (ii) $\langle g \rangle = \{e_G, g, g^2, \ldots, g^{n-1}\}$, und
   (iii) $|\langle g \rangle| = n$.

Aufgabe 1.56
Es sei $(G, \cdot)$ eine Gruppe und $h, k \in G$ fest gegeben. Prüfe, welche Bedingungen für h und k gelten müssen, damit die folgenden Abbildungen Gruppenhomomorphismen sind:

a. $\alpha : G \to G : g \mapsto h \cdot g$,

b. $\alpha : G \to G : g \mapsto h \cdot g \cdot h$,

c. $\beta : G \to G : g \mapsto h^{-1} \cdot g \cdot k$,

Aufgabe 1.57
Es sei $(G, \cdot)$ eine Gruppe. Zeige, $\alpha : G \longrightarrow G : g \mapsto g^2$ ist genau dann ein Gruppenhomomorphismus, wenn G abelsch ist.

Aufgabe 1.58
Es sei $(G, \cdot)$ eine Gruppe. Zeige, $\mathrm{inv} : G \longrightarrow G : g \mapsto g^{-1}$ ist genau dann ein Gruppenhomomorphismus, wenn G abelsch ist.

Aufgabe 1.59
Es sei $\alpha : (G, \cdot) \longrightarrow (H, *)$ ein Gruppenhomomorphismus, $g \in G$ und $g' \in \mathrm{Ker}(\alpha)$. Zeige, dann gilt $g^{-1} \cdot g' \cdot g \in \mathrm{Ker}(\alpha)$.

Aufgabe 1.60
Es sei $(G, \cdot)$ eine Gruppe und $g \in G$.

a. Die Abbildung $L_g : G \longrightarrow G : h \mapsto g \cdot h$ ist bijektiv.

b. Die Abbildung $\alpha : G \longrightarrow \mathrm{Sym}(G) : g \mapsto L_g$ ist ein Monomorphismus.

Anmerkung: Man nennt die Aussage in Teil b. auch den *Satz von Cayley*. Er besagt letztlich, daß jede Gruppe isomorph zu einer Untergruppe einer symmetrischen Gruppe ist.

Es ist ein wichtiges Prinzip, daß ein Monomorphismus alle guten Eigenschaften einer Gruppe bzw. ihrer Elemente erhält. Die Ordnung eines Elementes ist ein Beispiel für dieses Prinzip.

Aufgabe 1.61
Es sei $\alpha : (G, \cdot) \longrightarrow (H, *)$ ein Gruppenhomomorphismus und $g \in G$. Wir nennen die Mächtigkeit des Erzeugnisses von g die *Ordnung* von g und bezeichnen sie mit $o(g) := |\langle g \rangle|$. Zeige:

a. Ist $o(g) < \infty$, so ist $o(g)$ ein Vielfaches von $o\big(\alpha(g)\big)$.

b. Ist α injektiv, so gilt $o(g) = o\big(\alpha(g)\big)$.

Aufgabe 1.62
Da $(\mathbb{R}, +)$ eine Gruppe ist, ist nach Aufgabe 1.17 auch $(\mathbb{R}^2, +)$ mit der komponentenweisen Addition eine Gruppe. Zeige, daß folgende Abbildung

$$\alpha : \mathbb{R}^2 \longrightarrow \mathbb{R} : (x, y) \mapsto 2x + 3y$$

ein Gruppenhomomorphismus ist. Bestimme das Bild und den Kern von α. Ist α injektiv / surjektiv?

Aufgabe 1.63
Da $(\mathbb{R}\setminus\{0\},\cdot)$ und $(\mathbb{R},+)$ Gruppen sind, ist nach Aufgabe 1.17 auch die Menge $G=(\mathbb{R}\setminus\{0\})\times\mathbb{R}$ mit der Operation

$$(r,s)*(r',s'):=(r\cdot s',r+s')$$

eine Gruppe. Zudem wissen wir, daß die komplexen Zahlen $(\mathbb{C}\setminus\{0\},\cdot)$ ohne die Null bezüglich der Multiplikation eine Gruppe sind. Zeige, daß die Abbildung

$$\alpha:G\longrightarrow\mathbb{C}\setminus\{0\}:(r,s)\mapsto r\cdot\exp(s\cdot\pi\cdot i)$$

ein Gruppenhomomorphismus ist. Bestimme das Bild und den Kern von α. Ist α injektiv / surjektiv? Dabei ist π die Kreiszahl und i die imaginäre Einheit.

Aufgabe 1.64
Bestimme alle Gruppenhomomorphismen von $(\mathbb{Z},+)$ nach $(\mathbb{R},+)$.

2 Äquivalenzrelationen

Äquivalenzrelationen stellen ein sehr wichtiges *Ordnungs-* und *Konstruktionsprinzip* innerhalb der Mathematik dar, das wir im Verlauf der Vorlesung an einigen zentralen Stellen benötigen. Wir wollen deshalb die Betrachtung von Gruppen für einen Augenblick zurückstellen und uns diesem zentralen Begriff widmen.

Unter einer *Relation* auf einer Menge M versteht man in der Mathematik einfach eine Teilmenge R des kartesischen Produktes $M \times M$, und die Grundidee dabei ist, daß $(x, y) \in R$ bedeutet, daß x in irgendeiner Weise, die noch mit Leben zu füllen wäre, mit y in Relation steht. Bei geeigneter Betrachtung sind Abbildungen nur Spezialfälle von Relationen (siehe Definition B.5). Ein typischeres Beispiel sind aber sicher die *Ordnungsrelationen*, bei denen x in Relation zu y steht, wenn x kleiner oder gleich y ist (siehe Definition B.23). Ordnungsrelationen bereiten in der Regel keine großen begrifflichen Schwierigkeiten. Wohl auch deshalb, da im täglichen Leben alles mögliche verglichen wird - seien es Größen, Entfernungen oder Geschwindigkeiten.

Bei dem folgenden Begriff der *Äquivalenzrelation* ist das ganz anders. Er bereitet den Studenten oft extreme Schwierigkeiten. Dabei liegt auch ihm ein ganz einfaches Prinzip zugrunde, das wir zunächst an einem Beispiel erläutern wollen.

Die Gesamtheit aller Schüler einer Schule werden von der Schulleitung zwecks sinnvoller Organisation des Unterrichts in Schulklassen eingeteilt. Dabei achtet die Schulleitung darauf, daß jeder Schüler zu einer Schulklasse gehört und auch nur zu dieser einen. Etwas mathematischer ausgedrückt, die Schulleitung teilt die *Menge* S der Schüler in *paarweise disjunkte Teilmengen* K_i, $i = 1, \ldots, k$, ein, so daß wir anschließend eine *disjunkte Zerlegung* (siehe Definition 2.6)

$$S = \dot{\bigcup_{i=1}^{k}} K_i$$

der Menge S in die Schulklassen $K_1, \ldots, K_k$ haben. Dabei kann man für die Zugehörigkeit der Schüler Alfred, Ben und Christoph zu einer Schulklasse folgendes feststellen:

1) Alfred gehört zu einer Schulklasse.
2) Wenn Alfred in der gleichen Schulklasse ist wie Ben, dann ist Ben auch in der gleichen Schulklasse wie Alfred.
3) Wenn Alfred in der gleichen Schulklasse ist wie Ben und wenn zugleich Ben in der gleichen Schulklasse ist wie Christoph, dann ist auch Alfred in der gleichen Schulklasse wie Christoph.

Diese Aussagen sind so offensichtlich, daß man kaum glauben mag, daß es einen tieferen Sinn hat, sie zu erwähnen. Aber nehmen wir für einen Augenblick an, die Schulleitung hat ihre Einteilung der Schüler vorgenommen und für jede Schulklasse eine Liste mit den Namen der Schüler erstellt, die zu dieser Schulklasse gehören sollen. Nehmen wir ferner an, die Schulleitung hat noch nicht überprüft, ob jeder Schüler in genau einer Schulklasse eingeteilt ist. Dann behaupte ich, wenn man in den drei Aussagen 1)-3) die Schüler Alfred, Ben und Christoph durch beliebige Schüler ersetzt und die Aussagen richtig sind für jede Kombination der Schülernamen, dann ist sichergestellt, daß auch jeder Schüler in genau einer Schulklasse eingeteilt ist.

Als Mathematiker suchen wir nach möglichst einfachen Regeln, denen die Einteilung der Schulklassen genügen muß, um sicherzustellen, daß sie wirklich eine disjunkte Zerlegung von S ist, d.h. daß wirklich jeder Schüler in genau einer Schulklasse ist, und die Regeln 1)-3) sind genau die Regeln, die wir dazu brauchen. Wenn wir nun die Zugehörigkeit zweier Schüler x und y zur gleichen Klasse verstehen als "x *steht in Relation zu* y", dann definieren uns die drei Regeln 1)-3) zudem eine Teilmenge von $S \times S$, nämlich die Teilmenge

$$R = \{(x, y) \in S \times S \mid x \text{ ist in der gleichen Schulklasse wie } y\}.$$

Die Regeln 1)-3) lassen sich für Schüler $x, y, z \in S$ dann wie folgt formulieren:

- $(x, x) \in R$.
- Wenn $(x, y) \in R$, dann ist auch $(y, x) \in R$.
- Wenn $(x, y) \in R$ und $(y, z) \in R$, dann ist auch $(x, z) \in R$.

Eine solche Relation nennt man eine *Äquivalenzrelation*, man nennt Schüler der gleichen Schulklasse *äquivalent* und die Schulklassen nennt man dann auch *Äquivalenzklassen*.

Natürlich führen wir den Begriff der *Äquivalenzrelation* nun für beliebige Mengen ein, und wir werden ihn im Folgenden immer wieder verwenden, um eine gegebene Menge in paarweise disjunkte Äquivalenzklassen zu zerlegen. Unser Ziel wird es dann sein, mit diesen neuen Einheiten weiterzuarbeiten, anstatt mit deren einzelnen Elementen.

Definition 2.1
Es sei M eine Menge. Eine *Äquivalenzrelation* auf M ist eine Teilmenge $R \subseteq M \times M$, so daß für alle $x, y, z \in M$ gilt:

R1: $(x, x) \in R$, ("Reflexivität")
R2: $(x, y) \in R \Rightarrow (y, x) \in R$, ("Symmetrie")
R3: $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$. ("Transitivität")

Bei Äquivalenzrelationen hat sich (ähnlich wie bei Ordnungsrelationen und Abbildungen) eine alternative Schreibweise zu $(x, y) \in R$ durchgesetzt, die auch wir im folgenden verwenden wollen.

Notation 2.2
Sei M eine Menge und R eine Äquivalenzrelation auf M. Wir definieren für $x, y \in M$

$$x \sim y \quad :\Longleftrightarrow \quad (x, y) \in R,$$

und wir sprechen dann meist von der Äquivalenzrelation "$\sim$" statt R, sofern keine Mißverständnisse zu befürchten sind.

Mit dieser Schreibweise lassen sich die drei Axiome in Definition 2.1 wie folgt formulieren. Für $x, y, z \in M$ soll gelten:

R1: $x \sim x$, ("Reflexivität")
R2: $x \sim y \;\Rightarrow\; y \sim x$, ("Symmetrie")
R3: $x \sim y, y \sim z \;\Rightarrow\; x \sim z$. ("Transitivität")

Definition 2.3
Es sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Für $x \in M$ heißt die Menge

$$\overline{x} := \{y \in M \mid y \sim x\}$$

die *Äquivalenzklasse* von x. Jedes $y \in \overline{x}$ heißt ein *Repräsentant* der Klasse $\overline{x}$. Mit

$$M/\sim := \left\{\overline{x} \mid x \in M\right\}$$

bezeichnen wir die Menge der *Äquivalenzklassen modulo der Äquivalenzrelation* $\sim$.

Beispiel 2.4
Wir betrachten die Menge $M = \mathbb{R}^2$ der Punkte in der reellen Zahlenebene und wir bezeichnen mit $|P|$ den Abstand von P zum Ursprung $(0,0)$. Für zwei Punkte $P, Q \in M$ definieren wir

$$P \sim Q \quad \Longleftrightarrow \quad |P| = |Q|,$$

d.h. wir nennen die Punkte *äquivalent*, falls ihr Abstand zum Ursprung gleich ist. Dann ist $\sim$ eine Äquivalenzrelation.

R1: Sei $P \in M$, dann ist $|P| = |P|$, also $P \sim P$.
R2: Falls $P, Q \in M$ mit $P \sim Q$, dann ist $|P| = |Q|$ und somit auch $|Q| = |P|$. Damit gilt aber $Q \sim P$.
R3: Falls $P, Q, R \in M$ mit $P \sim Q$ und $Q \sim R$, dann gilt $|P| = |Q|$ und $|Q| = |R|$. Aber damit gilt auch $|P| = |R|$ und somit $P \sim R$.

Die Äquivalenzklasse

$$\overline{P} = \{Q \in M \mid |Q| = |P|\}$$

von $P \in M$ ist der Kreis um den Ursprung vom Radius $|P|$.

Ein Beispiel aus dem Alltag für eine Äquivalenzrelation haben wir oben bereits gesehen. Ein weiteres wichtiges und wohlbekanntes Beispiel sind die rationalen Zahlen! Ein Bruch ist nichts weiter als die Äquivalenzklasse eines Tupels von ganzen Zahlen, und das Kürzen des Bruches, z.B. $\frac{1}{2} = \frac{2}{4}$, ist nur die Wahl eines möglichst einfachen Repräsentanten.

Beispiel 2.5
Man kann die rationalen Zahlen wie folgt als Äquivalenzklassen von Paaren ganzer Zahlen definieren. Für $(p, q), (p', q') \in M := \mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$ definiere

$$(p, q) \sim (p', q') \quad :\Longleftrightarrow \quad pq' = p'q.$$

Wir wollen nun zeigen, daß hierdurch wirklich eine Äquivalenzrelation auf M definiert wird. Seien dazu $x = (p, q), x' = (p', q'), x'' = (p'', q'') \in M$ gegeben:[15]

R1: Für die Reflexivität müssen wir $x \sim x$ zeigen. Nun gilt aber $pq = pq$, woraus $x = (p, q) \sim (p, q) = x$ folgt.

R2: Für die Symmetrie nehmen wir an, daß $x \sim x'$ gilt und müssen $x' \sim x$ folgern. Wegen $x \sim x'$ gilt aber nach Definition $pq' = p'q$, und folglich auch $p'q = pq'$. Letzteres bedeutet aber, daß $x' = (p', q') \sim (p, q) = x$.

R3: Für die Transitivität nehmen wir schließlich an, daß $x \sim x'$ und $x' \sim x''$ gilt, und müssen daraus schließen, daß $x \sim x''$. Wegen $x \sim x'$ gilt nun aber $pq' = p'q$, und wegen $x' \sim x''$ gilt $p'q'' = p''q'$. Multiplizieren wir die erste der Gleichungen mit q'' und die zweite mit q, so erhalten wir

$$pq'q'' = p'qq'' = p'q''q = p''q'q.$$

Da nach Voraussetzung $q' \neq 0$, können wir beide Seiten der Gleichung durch q' teilen und erhalten:

$$pq'' = p''q.$$

Das wiederum bedeutet, daß $x = (p, q) \sim (p'', q'') = x''$ gilt.

Die drei Axiome einer Äquivalenzrelation sind also erfüllt.

Wir setzen nun $\mathbb{Q} := M/\sim$ und für $(p, q) \in M$ setzen wir $\frac{p}{q} := \overline{(p, q)}$, d. h. die rationale Zahl $\frac{p}{q}$ ist die Äquivalenzklasse des Paares (p, q) unter der obigen Äquivalenzrelation. Dann bedeutet die Definition von $\sim$ soviel wie, daß $\frac{p}{q}$ und $\frac{p'}{q'}$ gleich sind, wenn die kreuzweisen Produkte von Zähler und Nenner, pq' und $p'q$, übereinstimmen, oder in der vielleicht etwas bekannteren Formulierung, wenn die Brüche nach *Erweitern* mit q' bzw. mit q übereinstimmen: $\frac{p}{q} = \frac{pq'}{qq'} \overset{!}{=} \frac{p'q}{q'q} = \frac{p'}{q'}$.

Auch die Rechenregeln für rationale Zahlen lassen sich mit Hilfe der Äquivalenzklassen definieren. Für $(p, q), (r, s) \in M$ definiere:

$$\overline{(p, q)} + \overline{(r, s)} := \overline{(ps + qr, qs)},$$
$$\overline{(p, q)} \cdot \overline{(r, s)} := \overline{(pr, qs)}.$$

In Anlehnung an unser erstes Beispiel, der Einteilung der Schüler in Schulklassen, kann man das obige Rechenprinzip als “Rechnen mit Klassen” bezeichnen. Will man

[15] Man sollte sich nicht dadurch verwirren lassen, daß die Elemente von M nun selbst schon Zahlenpaare sind! Wollte man die Relation als Teilmenge von $M \times M$ schreiben, so müßte man

$$R = \big\{\big((p, q), (p', q')\big) \in M \times M \,\big|\, pq' = p'q\big\}$$

betrachten. Das erläutert vielleicht auch, weshalb wir die *alternative* Schreibeweise bevorzugen – solche Paare von Paaren werden doch leicht unübersichtlich.

zwei Klassen addieren (bzw. multiplizieren), so nimmt man aus jeder der Klasse ein Element, addiert (bzw. multipliziert) diese Elemente und schaut, in welche Klasse das Resultat gehört. Diese Klasse ist dann die Summe (bzw. das Produkt) der beiden Klassen.

Was man sich bei diesem Vorgehen allerdings klar machen muß, ist, daß das Ergebnis nicht von der Wahl der Repräsentanten (d.h. der Elemente aus den Klassen) abhängt. Man spricht davon, daß die Operation *wohldefiniert* ist (vgl. Fußnote 26 auf Seite 70). Wir führen das für die Addition der rationalen Zahlen vor.

Sind $(p', q') \in \overline{(p, q)}$ und $(r', s') \in \overline{(r, s)}$ andere Repräsentanten, dann gilt $p'q = q'p$ und $r's = s'r$. Es ist zu zeigen, daß $(p's' + q'r', q's') \in \overline{(ps + qr, qs)}$ gilt. Ausmultiplizieren liefert

$$(p's' + q'r')(qs) = p'qs's + q'qr's = q'ps's + q'qs'r = (ps + qr)(q's'),$$

was zu zeigen war. $\square$

Wir haben anfangs behauptet, daß die drei Axiome einer Äquivalenzrelation sicherstellen, daß die zugehörigen Äquivalenzklassen eine disjunkte Zerlegung von M induzieren, und umgekehrt, daß jede disjunkte Zerlegung eine Äquivalenzrelation mit sich bringt. Dies wollen wir im Folgenden beweisen. Dazu sollten wir zunächst den Begriff disjunkt klären.

Definition 2.6

a. Zwei Mengen M und N heißen *disjunkt*, falls $M \cap N = \emptyset$.

b. Eine Familie $(M_i)_{i \in I}$ von Mengen heißt *paarweise disjunkt*, wenn M_i und M_j für alle $i, j \in I$ mit $i \neq j$ disjunkt sind.

c. Es sei M eine Menge. Eine paarweise disjunkte Familie $(M_i)_{i \in I}$ von Teilmengen von M heißt eine *disjunkte Zerlegung* von M, falls $M = \bigcup_{i \in I} M_i$. Wir schreiben in diesem Fall:

$$M = \dot{\bigcup_{i \in I}} M_i.$$

Proposition 2.7

Ist $(M_i)_{i \in I}$ *eine disjunkte Zerlegeung von* M *und definieren wir eine Relation auf* M *durch*

$$x \sim y \iff \exists\, i \in I\, :\, x, y \in M_i,$$

dann ist $\sim$ *eine Äquivalenzrelation auf* M.

Beweis: Ist $x \in M = \dot{\bigcup}_{i \in I} M_i$, so gibt es ein $i \in I$ mit $x \in M_i$ und somit gilt $x \sim x$. $\sim$ ist also reflexiv.

Sind $x, y \in M$ mit $x \sim y$, so gibt es ein $i \in I$ mit $x, y \in M_i$. Dann gilt aber auch $y \sim x$. Die Relation ist also symmetrisch.

Sind $x, y, z \in M$ mit $x \sim y$ und $y \sim z$, so gibt es $i, j \in I$ mit $x, y \in M_i$ und $y, z \in M_j$. Da die Zerlegung disjunkt ist und $y \in M_i \cap M_j$, folgt $M_i = M_j$. Also gilt $x, z \in M_i$ und somit $x \sim z$. $\sim$ ist also auch transitiv. $\square$

Proposition 2.8
Es sei M eine Menge. Ist $\sim$ eine Äquivalenzrelation auf M, dann bilden die Äquivalenzklassen eine disjunkte Zerlegung von M, d. h. jedes $x \in M$ liegt in genau einer Äquivalenzklasse.

Insbesondere gilt für je zwei Äquivalenzklassen $\overline{x}$ und $\overline{y}$ entweder $\overline{x} = \overline{y}$ oder $\overline{x} \cap \overline{y} = \emptyset$.

Beweis: Sei $x \in M$ beliebig. Aus $x \sim x$ folgt $x \in \overline{x} \subseteq \bigcup_{\overline{y} \in M/\sim} \overline{y}$. Mithin gilt

$$M = \bigcup_{\overline{y} \in M/\sim} \overline{y}.$$

Es bleibt also zu zeigen, daß die Äquivalenzklassen paarweise disjunkt sind.

Seien $\overline{x}, \overline{y} \in M/\sim$ mit $\overline{x} \cap \overline{y} \neq \emptyset$. Dann gibt es ein $z \in \overline{x} \cap \overline{y}$, und es gilt $z \sim x$ und $z \sim y$. Wegen der Symmetrie gilt aber auch $x \sim z$ und mittels der Transitivität dann $x \sim y$. Sei nun $u \in \overline{x}$ beliebig, dann gilt $u \sim x$ und wieder wegen der Transitivität $u \sim y$. Also $u \in \overline{y}$ und damit $\overline{x} \subseteq \overline{y}$. Vertauschung der Rollen von x und y in der Argumentation liefert schließlich $\overline{x} = \overline{y}$. $\square$

Korollar 2.9
Sei M eine endliche Menge, $\sim$ eine Äquivalenzrelation auf M und $M_1, \ldots, M_s$ seien die paarweise verschiedenen Äquivalenzklassen von $\sim$. Dann gilt:

$$|M| = \sum_{i=1}^{s} |M_i|.$$

Beweis: Mit M sind auch alle M_i endlich und die Behauptung folgt aus Proposition 2.8. $\square$

Aufgabe 2.10
Es sei $M = \{(a_n)_{n \in \mathbb{N}} \mid a_n \in \mathbb{Q}\}$ die Menge aller Folgen rationaler Zahlen. Zeige, daß durch

$$(a_n)_{n \in \mathbb{N}} \sim (b_n)_{n \in \mathbb{N}} \quad :\Longleftrightarrow \quad \lim_{n \to \infty} (a_n - b_n) = 0$$

eine Äquivalenzrelation auf M definiert wird.

Aufgabe 2.11
Wir definieren für zwei Punkte $(x, y), (x', y') \in \mathbb{R}^2$

$$(x, y) \sim (x', y') \quad :\Longleftrightarrow \quad |x| + |y| = |x'| + |y'|.$$

Zeige, $\sim$ ist eine Äquivalenzrelation auf $\mathbb{R}^2$. Zeichne die Äquivalenzklassen zu $(1, 1)$ und zu $(-2, 3)$ in die Zahlenebene $\mathbb{R}^2$ ein.

Aufgabe 2.12 (Die projektive Gerade)
Wir definieren für $v = (v_1, v_2), w = (w_1, w_2) \in \mathbb{R}^2 \setminus \{(0,0)\}$

$$v \sim w \quad \Longleftrightarrow \quad \exists\, \lambda \in \mathbb{R} \setminus \{0\} \, : \, v = \lambda \cdot w$$

wobei $\lambda \cdot w := (\lambda \cdot w_1, \lambda \cdot w_2)$.

a. Zeige, daß $\sim$ eine Äquivalenzrelation auf $M = \mathbb{R}^2 \setminus \{(0,0)\}$ ist. Es ist üblich die Äquivalenzklasse $\overline{(v_1, v_2)}$ von (v_1, v_2) mit $(v_1 : v_2)$ zu bezeichnen, und man nennt die Menge $M/\sim$ der Äquivalenzklassen die *projektive Gerade* über $\mathbb{R}$ und bezeichnet sie mit $\mathbb{P}^1_{\mathbb{R}}$.

b. Wir definieren auf $\mathbb{P}^1_{\mathbb{R}}$ eine zweistellige Operation durch

$$(v_1 : v_2) \cdot (w_1 : w_2) := (v_1 \cdot w_1 - v_2 \cdot w_2 : v_1 \cdot w_2 + v_2 \cdot w_2).$$

Zeige, daß diese Operation wohldefiniert ist, d.h. nicht von der Wahl der Repräsentanten für die Äquivalenzklasse abhängt, und daß $\mathbb{P}^1_{\mathbb{R}}$ mit dieser Operation eine Gruppe ist. (Man darf hierbei die Ergebnisse, die im Beweis von Aufgabe 1.18 b. erzielt wurden verwenden.)

c. Ist $(G, \cdot)$ die Gruppe aus Aufgabe 1.18 b., so zeige man, daß die Abbildung

$$\alpha : G \longrightarrow \mathbb{P}^1_{\mathbb{R}} : (a, b) \mapsto (a : b)$$

ein Gruppenepimorphismus mit Kern $\mathrm{Ker}(\alpha) = (\mathbb{R} \setminus \{0\}) \times \{0\}$ ist.

d. Die Menge $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ ist Kreis vom Radius Eins um den Mittelpunkt $(0, 0)$. Zeige, daß die Abbilung

$$\Phi : S^1 \longrightarrow \mathbb{P}^1_{\mathbb{R}} : (x, y) \mapsto \overline{(x, y)}$$

surjektiv ist.

e. Wenn wir in der Definition von $\sim$ alle Elemente $v, w \in \mathbb{R}^2$ zulassen, definiert $\sim$ dann eine Äquivalenzrelation auf $\mathbb{R}^2$? Falls ja, was ist die Äquivalenzklasse von $(0, 0)$?

Aufgabe 2.13 (Die ganzen Zahlen)
Es sei $M = \mathbb{N} \times \mathbb{N}$ und $m = (a, b) \in M$ und $m' = (a', b') \in M$ seien zwei Elemente in M. Wir definieren

$$m \sim m' \quad \longleftrightarrow \quad a + b' = a' + b.$$

Zeige, daß $\sim$ eine Äquivalenzrelation definiert und daß die Abbildung

$$\Phi : \mathbb{Z} \longrightarrow M/\sim : z \mapsto \begin{cases} \overline{(z, 0)}, & \text{falls } z \geq 0, \\ \overline{(0, -z)}, & \text{falls } z < 0 \end{cases}$$

bijektiv ist.

Aufgabe 2.14
Es sei M eine Menge und $\sigma \in \mathrm{Sym}(M)$ eine bijektive Selbstabbildung.

a. Durch
$$a \sim b \quad \Longleftrightarrow \quad \exists\, m \in \mathbb{Z} \,:\, b = \sigma^m(a)$$
für $a, b \in M$ wird eine Äquivalenzrelation auf der Menge M definiert.

b. Es sei $\overline{a}$ für $a \in M$ eine *endliche* Äquivalenzklasse bezüglich $\sim$ der Mächtigkeit $|\overline{a}| = n < \infty$. Dann gelten die folgenden Aussagen:
   (i) Das Minimum $k = \min\{l > 0 \mid \sigma^l(a) = a\}$ existiert.
   (ii) Für $q \in \mathbb{Z}$ ist $\sigma^{q \cdot k}(a) = a$.
   (iii) $\overline{a} = \left\{a, \sigma(a), \ldots, \sigma^{k-1}(a)\right\}$.
   (iv) $\overline{a}$ enthält genau k Elemente.

c. Es sei $M = \{1, \ldots, 7\}$ und $\sigma \in \mathrm{Sym}(M) = \mathbb{S}_7$ sei durch folgende Wertetabelle gegeben:

a	1	2	3	4	5	6	7
$\sigma(a)$	3	4	1	7	2	6	5

Was sind die Äquivalenzklassen bezüglich obiger Äquivalenzrelation?

3 Die symmetrische Gruppe

Die symmetrische Gruppe $\mathrm{Sym}(M)$ der bijektiven Selbstabbildungen einer Menge M ist in gewissem Sinn die *Urmutter* aller Gruppen, da jede Gruppe isomorph zu einer Untergruppe von $\mathrm{Sym}(M)$ für ein geeignetes M ist.[16] Für eine beliebige Menge M ist $\mathrm{Sym}(M)$ allerdings wenig nützlich, da man außer der Definition kaum etwas über sie aussagen kann.

Für eine endliche Menge M ist das ganz anders. Zunächst einmal ist es egal, ob wir $\mathrm{Sym}\left(\{m_1, \ldots, m_n\}\right)$, für eine beliebige n-elementige Menge $M = \{m_1, \ldots, m_n\}$, betrachten oder $\mathbb{S}_n = \mathrm{Sym}\left(\{1, \ldots, n\}\right)$. Die beiden Gruppen sind isomorph, und zwar so offensichtlich, daß wir keinen Unterschied machen - wir identifizieren sie. $\mathbb{S}_n$ ist für praktische Anwendungen sehr wichtig. In den Grundlagen der Mathematik wird die Gruppe $\mathbb{S}_n$ vor allem im Zusammenhang mit Determinanten benötigen.

Da die Menge $\{1, \ldots, n\}$ endlich ist, können wir die Abbildungsvorschrift einer Permutation $\sigma \in \mathbb{S}_n$ leicht durch eine Art *Wertetabelle* angeben. Als solche sollte man das zweizeilige Schema in der folgenden Definition auffassen. Aus dem Schema ist unmittelbar der Definitionsbereich und der Wertebereich der Permutation ablesbar, so daß wir darauf verzichten können, diesen gesondert anzugeben. D.h. σ ist als Abbildung eindeutig durch dieses Schema bestimmt.

Definition 3.1
Ist $\sigma \in \mathbb{S}_n$ eine *Permutation* der Menge $\{1, \ldots, n\}$, so können wir σ durch das folgende zweizeilige Schema beschreiben:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

bzw.

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ \sigma(a_1) & \sigma(a_2) & \ldots & \sigma(a_n) \end{pmatrix},$$

falls $a_1, \ldots, a_n$ irgendeine Anordnung der Zahlen $1, \ldots, n$ ist.

Beispiel 3.2
Die Gruppe $\mathbb{S}_n$ ist für $n \geq 3$ nicht abelsch, denn für die Permutationen

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in \mathbb{S}_3$$

gilt

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

[16] Dies ist die Aussage des Satzes von Cayley. Vergleiche dazu Aufgabe 1.60.

Beachte, daß es bei dem Schema nicht darauf ankommt, in welcher Reihenfolge die Zahlen von 1 bis n in der ersten Zeile stehen. Es gilt etwa:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Es empfiehlt sich aber der Übersichtlichkeit halber für gewöhnlich, die Ziffern in aufsteigender Reihenfolge anzuordnen.

Bemerkung 3.3

Die oben eingeführte Darstellung einer Permutation hat den angenehmen Nebeneffekt, daß man das Inverse der Permutation leicht angeben kann, indem man einfach die beiden Zeilen vertauscht. Sprich, für eine Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} \in \mathbb{S}_n$$

ist das Inverse σ^{-1} gegeben ist durch

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \ldots & \sigma(n) \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Nun sind Mathematiker von Haus aus *faule* oder vielleicht richtiger *effiziente* Menschen, und so haben sie sich eine Schreibweise ersonnen, wie man eine Permutation darstellen kann und dabei jede der Zahlen $1, \ldots, n$ höchstens *einmal* statt zweimal schreiben muß. Um dies zu bewerkstelligen, benötigen wir einen speziellen Typ von Permutation – eine, die k der Zahlen $1, \ldots, n$ *zyklisch vertauscht.*

Definition 3.4

a. Sei $\{1, \ldots, n\} = \{a_1, \ldots, a_k\} \cup \{b_1, \ldots, b_{n-k}\}$, $k \geq 2$, und

$$\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k & b_1 & \ldots & b_{n-k} \\ a_2 & a_3 & \ldots & a_k & a_1 & b_1 & \ldots & b_{n-k} \end{pmatrix} \in \mathbb{S}_n,$$

so heißt σ ein **k-Zyklus**, und wir sagen, daß sie die Zahlen $a_1, \ldots, a_k$ *zyklisch vertauscht.* Die Abbildungsvorschrift eines solchen k-Zyklus läßt sich deutlich kompakter durch das folgende einzeilige Schema repräsentieren:

$$\sigma = (a_1 \ldots a_k). \tag{20}$$

b. Ein $2-\mathrm{Zyklus}$ wird auch eine **Transposition** genannt. Eine Transposition $\tau = (i\ j)$ ist mithin eine Permutation, die nur die zwei Zahlen i und j miteinander vertauscht, alle anderen aber fest läßt.

c. Das neutrale Element von $\mathbb{S}_n$, per definitionem $\mathrm{id}_{\{1,\ldots,n\}}$, wollen wir der Einfachheit halber mit id bezeichnen.

Bemerkung 3.5

Die Interpretation der Schreibweise in Gleichung (20) ist offensichtlich, das erste Element a_1 wird auf das zweite a_2 abgebildet, das zweite auf das dritte, und so weiter, bis schließlich das letzte, nämlich a_k, auf das erste, das heißt auf a_1, abgebildet wird – der *Kreis* schließt sich. Beachte hierbei, daß die Zyklen $(a_1 \ldots a_k)$,

$(a_k a_1 \ldots a_{k-1})$, etc. stimmen überein! Um diese Mehrdeutigkeit zu vermeiden, empfiehlt es sich, einen Zyklus stets mit der kleinsten der Zahlen $a_1, \ldots, a_k$ zu beginnen.

Bisher haben wir k-Zyklen nur für $k \geq 2$ definiert. Wir nun auch 1-Zyklen, etwa (1) oder (3), zulassen und definieren diese in natürlicher Weise als die Identität. $\square$

Beispiel 3.6
Die Permutationen

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \in \mathbb{S}_4 \quad \text{und} \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} \in \mathbb{S}_5$$

sind jeweils 3-Zyklen, die die Zahlen $1, 4, 2$ zyklisch vertauschen. In der oben eingeführten Zyklenschreibweise gilt

$$\sigma = (1\ 4\ 2) \quad \text{und} \quad \pi = (1\ 4\ 2).$$

Damit wird der Nachteil dieser Schreibweise gegenüber dem zweizeiligen Schema deutlich – weder der Definitionsbereich noch der Wertebereich lassen sich aus der Zyklenschreibweise eindeutig ablesen. Aber diesen Preis sind wir für die gewonnene *Übersichtlichkeit* gerne bereit zu zahlen. Denn einerseits ist in Anwendungen meist zweifelsfrei bekannt, was n ist, und andererseits ist die wesentliche Information für uns letztlich, welche Zahlen durch die Permutation vertauscht werden, und nicht, welche unbewegt bleiben. $\square$

Nun wäre die Zyklenschreibweise aber nicht sehr hilfreich, wenn wir sie nur für k-Zyklen anwenden könnten, alle anderen Permutationen aber weiterhin in dem zweireihigen Schema angegeben werden müßten. Da kommt uns die Feststellung zu Hilfe, daß jede Permutation sich als Komposition von paarweise *disjunkten* Zyklen schreiben läßt.

Satz 3.7
Ist $\sigma \in \mathbb{S}_n$ eine Permutation, so gibt es eine disjunkte Zerlegung

$$\{1, \ldots, n\} = \dot{\bigcup_{i=1}^{t}} \{a_{i1}, \ldots, a_{ik_i}\},$$

so daß

$$\sigma = (a_{11} \cdots a_{1k_1}) \circ \ldots \circ (a_{t1} \cdots a_{tk_t}).$$

Wir nennen diese Darstellung die Zyklenzerlegung *von σ, und wir nennen die Zyklen* paarweise disjunkt. *Beachte auch, daß $k_1 + \ldots + k_t = n$ und daß $0 \leq k_i \leq n$ für $i = 1, \ldots, t$.*

Beweis: Um die Zyklen der Zyklenzerlegung zu finden, betrachten wir die Äquivalenzrelation aus Aufgabe 2.14 auf $\{1, \ldots, n\}$, die durch

$$a \sim b \quad \Longleftrightarrow \quad \exists\, m \in \mathbb{Z} \,:\, b = \sigma^m(a)$$

für $a, b \in \{1, \ldots, n\}$ gegeben ist. Für $a \in \{1, \ldots, n\}$ hat die Äquivalenzklasse von a die Form

$$\overline{a} = \big\{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{k-1}(a)\big\}, \tag{21}$$

wobei

$$k = \min\{l > 0 \mid \sigma^l(a) = a\} = |\overline{a}|.$$

Gemäß Proposition 2.8 bilden die Äquivalenzklassen von $\sim$ eine disjunkte Zerlegung von $\{1, \ldots, n\}$. Wir können also Zahlen $a_{11}, \ldots, a_{t1} \in \{1, \ldots, n\}$ so wählen, daß

$$\{1, \ldots, n\} = \dot{\bigcup_{i=1}^{t}} \overline{a_{i1}}.$$

Setzen wir nun $k_i = |\overline{a_{i1}}|$ und $a_{ij} = \sigma^{j-1}(a_{i1})$, dann gilt wegen (21)

$$\{1, \ldots, n\} = \dot{\bigcup_{i=1}^{t}} \{a_{i1}, a_{i2}, \ldots, a_{ik_i}\}. \tag{22}$$

Es bleibt also noch

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_t$$

zu zeigen, wobei $\sigma_i = (a_{i1} \cdots a_{ik_i})$ ein k_i-Zyklus ist. Sei dazu $b \in \{1, \ldots, n\}$, so ist $b = a_{ij} = \sigma^{j-1}(a_{i1})$ für ein $1 \leq i \leq t$ und ein $1 \leq j \leq k_i$. Wenden wir nun σ auf b an, so erhalten wir

$$\sigma(b) = \sigma(a_{ij}) = \sigma^j(a_{i1}) = \left\{ \begin{array}{ll} a_{ij+1}, & \text{falls } j < k_i, \\ a_{i1}, & \text{falls } j = k_i \end{array} \right\} = \sigma_i(b).$$

Da die Zerlegung in (22) disjunkt ist und sowohl b, als auch $\sigma_i(b)$ in $\{a_{i1}, \ldots, a_{ik_i}\}$ liegen, werden b und $\sigma_i(b)$ von allen σ_l mit $l \neq i$ fest gelassen, d.h.

$$\big(\sigma_1 \circ \cdots \circ \sigma_t\big)(b) = \sigma_i(b) = \sigma(b).$$

Damit ist die Aussage des Satzes gezeigt. □

Bemerkung 3.8

Beachte, daß für zwei disjunkte Zyklen $\sigma = (a_1 \ \ldots \ a_k), \pi = (b_1 \ \ldots \ b_l) \in \mathbb{S}_n$ offenbar

$$\sigma \circ \pi = \pi \circ \sigma$$

gilt. Denn für $c \in \{a_1, \ldots, a_k\}$ gilt $\sigma(c) \in \{a_1, \ldots, a_k\}$ und deshalb notwendig $c, \sigma(c) \notin \{b_1, \ldots, b_l\}$, so daß

$$(\sigma \circ \pi)(c) = \sigma\big(\pi(c)\big) = \sigma(c) = \pi\big(\sigma(c)\big) = (\pi \circ \sigma)(c). \tag{23}$$

In den Fällen $c \in \{b_1, \ldots, b_l\}$ und $c \notin \{a_1, \ldots, a_k\} \cup \{b_1, \ldots, b_l\}$ zeigt man (23) analog, so daß die obige Behauptung folgt.

Zudem ist offensichtlich, daß die Zyklenzerlegung von σ bis auf die Reihenfolge der Zyklen *eindeutig* ist, da die Elemente der Zyklen von σ zyklisch vertauscht werden.

Und schließlich ist eine Permutation auch in Zyklenschreibweise leicht zu invertieren, indem man sie einfach von hinten nach vorne liest. Denn für einen k-Zyklus $\sigma = (a_1 \ \ldots \ a_k)$ ist offenbar das Inverse

$$\sigma^{-1} = (a_k \, a_{k-1} \ \ldots \ a_2 \, a_1)$$

wieder ein k-Zyklus, und somit ist für

$$\pi = (a_{11} \cdots a_{1k_1}) \circ \ldots \circ (a_{t1} \cdots a_{tk_t})$$

das Inverse gegeben durch

$$\pi^{-1} = (a_{tk_t} \cdots a_{t1}) \circ \ldots \circ (a_{1k_1} \cdots a_{11}).$$

□

Beispiel 3.9
Die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \in \mathbb{S}_5$$

hat die Zyklenzerlegung

$$\sigma = (1\,2\,5) \circ (3\,4) = (3\,4) \circ (1\,2\,5). \tag{24}$$

Ferner ist das Inverse zu σ gegeben durch

$$\sigma^{-1} = (4\,3) \circ (5\,2\,1) = (1\,5\,2) \circ (3\,4).$$

Eine berechtigte Frage ist, wie wir die Zyklenzerlegung in (24) gefunden haben. Wir wollen versuchen, dies so in Worte zu fassen, daß dem Leser daraus die allgemeine Vorgehensweise ersichtlich wird. Man starte mit der kleinsten Zahl, 1, und suche ihr Bild unter σ, also $\sigma(1) = 2$. Das liefert den Startteil des ersten Zyklus:

$$(1\,2$$

Sodann betrache man das Bild von 2 unter σ, also $\sigma(2) = 5$, und erhält:

$$(1\,2\,5$$

Man fährt mit dem Bild von 5 unter σ, also $\sigma(5) = 1$, fort. Da dieses das erste Element des ersten Zyklus war, schließen wir den Zyklus,

$$(1\,2\,5),$$

und beginnen den zweiten Zyklus mit der kleinsten Zahl in $\{1, \ldots, 5\}$, die noch nicht in dem ersten Zyklus vorkommt, also mit 3:

$$(1\,2\,5) \circ (3$$

Dann betrachten wir deren Bild unter σ, also $\sigma(3) = 4$, und setzen so unseren zweiten Zyklus fort:

$$(1\,2\,5) \circ (3\,4$$

Da bereits alle fünf Elemente von $\{1, \ldots, 5\}$ aufgebraucht sind, muß notwendig $\sigma(4) = 3$ gelten, was es auch tut, und wir können damit auch den zweiten Zyklus schließen:

$$\sigma = (1\ 2\ 5) \circ (3\ 4).$$

Wie gesagt, da in $\{1, \ldots, 5\}$ keine Zahl mehr übrig ist, sind wir fertig und haben die Zyklenzerlegung von σ gefunden.

Das hier beschriebene Verfahren ist die praktische Umsetzung des Beweises von Satz 3.7, denn wir können die Zyklenzerlegung nun auch in folgender Form schreiben

$$\sigma = \Big(1\ \ \sigma(1)\ \ \sigma^2(1)\Big) \circ \big(3\ \ \sigma(3)\big),$$

wobei $\sigma^3(1) = 1$ und $\sigma^2(3) = 3$ gilt. $\square$

Von jetzt an werden wir zwischen den beiden Darstellungsarten für Permutationen hin und her wechseln und stets die verwenden, die für unsere Zwecke am besten geeignet ist.

Bemerkung 3.10
Für kleine Werte n ist $\mathbb{S}_n$ sehr übersichtlich, für große Werte n wird $\mathbb{S}_n$ jedoch riesig. $\mathbb{S}_1 = \{\mathrm{id}\}$ und $\mathbb{S}_2 = \{\mathrm{id}, (1\ 2)\}$. $\mathbb{S}_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ hat schon sechs Elemente, $\mathbb{S}_4$ gar 24 und $\mathbb{S}_{60}$ ungefähr 10^{82}. Letztere Zahl entspricht in etwa der angenommenen Anzahl der Nukleone des Universums.

Proposition 3.11
$|\mathbb{S}_n| = n! = 1 \cdot 2 \cdot 3 \cdots n.$

Bevor wir einen formalen Beweis dieser Aussage mittels Induktion geben, wollen wir ein Argument dafür geben, weshalb die Aussage richtig sein sollte. Im Prinzip handelt es sich dabei um die Idee des anschließenden formalen Beweises.

Beweisidee für Proposition 3.11: Eine Permutation $\sigma \in \mathbb{S}_n$ ist durch die Bilder $\sigma(1), \ldots, \sigma(n)$ der Zahlen $1, \ldots, n$ festgelegt, wobei jede der Zahlen $1, \ldots, n$ unter den Zahlen $\sigma(1), \ldots, \sigma(n)$ genau einmal vorkommt. Wir wollen nun zählen, wieviele Möglichkeiten es für die Definition einer solchen Permutation gibt. Zunächst müssen wir $\sigma(1)$, d.h. das Bild von 1, festlegen. Dazu haben wir noch volle n Zahlen zur Auswahl. Ist dieses festgelegt, so bleiben für das Bild $\sigma(2)$ der 2 nur noch $n-1$ Zahlen übrig. Für $\sigma(3)$ sind es schon nur noch $n-2$. Wenn man so fortfährt, hat man allgemein für $\sigma(i)$ noch $n-i+1$ Möglichkeiten, also schließlich für $\sigma(n-1)$ noch $n-(n-1)+1 = 2$ und für $\sigma(n)$ noch genau eine. Insgesamt gibt es deshalb

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$$

Möglichkeiten eine Permutation zu definieren, und mithin gibt es $n!$ verschiedene Permutationen. $\square$

Unsauber an dieser Beweisidee ist der Teil “*und wenn man so fortfährt*”. Ihn mathematisch sauber und korrekt zu fassen, heißt, eine Induktion zu führen.

Beweis von Proposition 3.11: Wir zeigen durch Induktion über n etwas allgemeiner:

Behauptung: Sind $M = \{m_1, \ldots, m_n\}$ und $N = \{n_1, \ldots, n_n\}$ zwei n-elementige Mengen, so hat die Menge

$$\mathrm{Iso}(M,N) := \{f : M \to N \mid f \text{ ist bijektiv}\}$$

genau $n!$ Elemente.

Induktionsanfang: Sei $n = 1$, dann gilt offensichtlich $|\mathrm{Iso}(M,N)| = 1 = 1!$.

Induktionsvoraussetzung: Es sei $n > 1$ beliebig, aber fest, und es gelte $|\mathrm{Iso}(M', N')| = (n-1)!$ für alle $n-1$-elementigen Mengen M' und N'.

Induktionsschluß: Seien nun M und N zwei n-elementige Mengen. Für $i \in \{1, \ldots, n\}$ definieren wir:

$$\mathrm{Iso}_i := \{f \in \mathrm{Iso}(M,N) \mid f(m_1) = n_i\}.$$

Offensichtlich ist die Einschränkung[17]

$$\mathrm{Iso}_i \to \mathrm{Iso}\left(M \setminus \{m_1\}, N \setminus \{n_i\}\right) : f \mapsto f_{|M\setminus\{m_1\}}$$

bijektiv, und daher gilt nach Induktionsvoraussetzung $|\mathrm{Iso}_i| = (n-1)!$. Da nun außerdem

$$\mathrm{Iso}(M,N) = \dot{\bigcup_{i=1}^{n}} \mathrm{Iso}_i,$$

d. h. $(\mathrm{Iso}_1, \ldots, \mathrm{Iso}_n)$ ist eine disjunkte Zerlegung von $\mathrm{Iso}(M,N)$, folgt:

$$|\mathrm{Iso}(M,N)| = \sum_{i=1}^{n} |\mathrm{Iso}_i| = n \cdot (n-1)! = n!.$$

□

Bemerkung 3.12
Wir wollen uns jetzt mit den Transpositionen näher beschäftigen. Zunächst ist klar, daß für eine Transposition $\tau \in \mathbb{S}_n$ gilt $\tau^{-1} = \tau$, also $\tau^2 = \mathrm{id}$.

Proposition 3.13
Jede Permutation in $\mathbb{S}_n$, $n \geq 2$, läßt sich als Komposition von höchstens n Transpositionen darstellen.

Beweis: Ist $\sigma = (a_1 \ \ldots \ a_k)$ ein k-Zyklus mit $k \geq 2$, so gilt offenbar, daß

$$\sigma = (a_1 \ a_2) \circ (a_2 \ a_3) \circ \ldots \circ (a_{k-2} \ a_{k-1}) \circ (a_{k-1} \ a_k) \tag{25}$$

ein Produkt von $k-1$ Transpositionen ist. Ist nun $\mathrm{id} \neq \sigma \in \mathbb{S}_n$ beliebig, so hat σ nach Satz 3.7 eine Zyklenzerlegung der Form

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_t$$

[17]Siehe Bemerkung B.9.

wobei $\sigma_i = (a_{i1} \cdots a_{ik_i})$ ein k_i-Zyklus ist. Da disjunkte Zyklen miteinander kommutieren, können wir ohne Einschränkung[18] annehmen, daß $k_1 \geq k_2 \geq \ldots \geq k_t$. Zudem ist σ nicht das neutrale Element id, so daß notwendig $k_1 \geq 2$ gilt und die Zahl $s = \max\{r \mid 1 \leq r \leq t, k_r \geq 2\}$ definiert ist. Damit ist aber $\sigma_i = \mathrm{id}$ für $i = s+1, \ldots, t$ und somit ist

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_s$$

das Produkt von s Zyklen. Da sich σ_i als Produkt von $k_i - 1$ Transpositionen schreiben läßt, läßt sich σ als Produkt von

$$(k_1 - 1) + \ldots + (k_s - 1) = (k_1 + \ldots + k_s) - s \leq n - 1$$

Transpositionen schreiben. Die Behauptung ist also für $\sigma \neq \mathrm{id}$ gezeigt. Da aber $n \geq 2$ und zudem $\mathrm{id} = (1\ 2) \circ (1\ 2)$ das Produkt von zwei Transpositionen ist, ist die Proposition bewiesen. □

Der Beweis ist *konstruktiv*, da die Gleichung (25) angibt, wie man einen Zyklus in Transpositionen zerlegt und somit die Aufgabe, eine Permutation als Produkt von Transpositionen zu schreiben, auf die Berechnung einer Zyklenzerlegung reduziert. Allerdings haben wir zur Zerlegung (25) lediglich gesagt, daß diese *offensichtlich* gilt. Man sieht dies, indem man die beiden Abbildungen, die links und rechts des Gleichheitszeichens in (25) vorkommen auf die Zahlen $\{1, \ldots, n\}$ anwendet – das haben wir durch *Hinschauen* getan, aber man könnte es natürlich auch formal mit allen zu betrachtenden Fällen hinschreiben. Der Beweis würde dadurch nicht verständlicher.

Der Beweis von Satz 3.7 war ziemlich technisch, und so mag es dem einen oder anderen Leser Unbehagen bereiten, daß wir diese Aussage im Beweis von Proposition 3.13 verwendet haben. Deshalb geben wir noch einen alternativen Beweis der Aussage von Proposition 3.13, der ohne Satz 3.7 auskommt, für das Finden der Zerlegung in Transpositionen aber weniger hilfreich ist.

Alternativer Beweis von Proposition 3.13: Wir führen den Beweis durch Induktion über n.

Induktionsanfang: Sei $n = 2$. Es ist $\mathbb{S}_2 = \{\mathrm{id}, (1\ 2)\}$, und $\mathrm{id} = (1\ 2) \circ (1\ 2)$, also folgt die Behauptung.

Induktionsschluß: Sei nun $n \geq 2$ gegeben, und die Behauptung gelte für n bereits. Ferner sei $\sigma \in \mathbb{S}_{n+1}$ beliebig, aber fest. Es gibt ein $i \in \{1, \ldots, n+1\}$ mit $\sigma(n+1) = i$.

[18] Die Aussage "*wir können ohne Einschränkung annehmen*" bedeutet, daß wir nur einen *speziellen* Fall betrachten, daß aber offensichtlich ist, wie man aus diesem Spezialfall den allgemeinen Fall herleiten würde. Letzteres tut man dann nicht explizit, da es meist mit einem hohen Notationsaufwand und vielen Indizes verbunden wäre, ohne eine tiefere Einsicht zu bringen. Man sollte allerdings nur dann etwas ohne Einschränkung annehmen, wenn man sich sicher ist, daß die übrigen Fälle in der Tat leicht aus dem Spezialfall folgen!

Dann gilt mit $\tau = (n+1\ \ i)$

$$(\tau \circ \sigma)(n+1) = n+1,$$

also können wir die Einschränkung[19] $\sigma' = (\tau\circ\sigma)_{|\{1,\ldots,n\}}$ als Element von $\mathbb{S}_n$ auffassen. Mithin gilt nach Induktionsvoraussetzung, es gibt Transpositionen $\tau'_1, \ldots, \tau'_k \in \mathbb{S}_n$, $k \leq n$, mit

$$\sigma' = \tau'_1 \circ \cdots \circ \tau'_k.$$

Bezeichnen wir mit τ_j die Fortsetzung von τ'_j, die definiert wird durch

$$\tau_j : \{1, \ldots, n+1\} \to \{1, \ldots, n+1\} : l \mapsto \begin{cases} \tau'_j(l), & \text{falls } l \leq n \\ n+1, & \text{falls } l = n+1, \end{cases}$$

so folgt unmittelbar

$$\tau \circ \sigma = \tau_1 \circ \cdots \circ \tau_k,$$

und mithin

$$\sigma = (\tau \circ \tau) \circ \sigma = \tau \circ (\tau \circ \sigma) = \tau \circ \tau_1 \circ \cdots \circ \tau_k.$$

D. h. σ ist Komposition von $k+1 \leq n+1$ Transpositionen. □

Korollar 3.14

Jede Permutation in $\mathbb{S}_n$, $n \geq 2$, läßt sich als Produkt von Transpositionen zweier aufeinanderfolgender Zahlen schreiben.

Beweis: Wegen Proposition 3.13 reicht es, dies für eine Transposition $(i\ j)$ mit $i < j$ zu zeigen. Es gilt aber offenbar

$$\begin{aligned}(i\ j) \quad = \quad & (i\ i+1) \circ (i+1\ \ i+2) \circ \cdots \circ (j-2\ \ j-1) \circ (j-1\ \ j) \circ \\ & \circ (j-2\ \ j-1) \circ \cdots \circ (i+1\ \ i+2) \circ (i\ i+1).\end{aligned}$$

□

Die Darstellung einer Permutation als Komposition von Transpositionen ist also keineswegs eindeutig. Was jedoch unabhängig ist, ist, daß eine Permutation entweder immer durch eine gerade oder immer durch eine ungerade Anzahl von Transpositionen darstellbar ist. Das wollen wir nun beweisen und definieren dazu das Vorzeichen einer Permutation.

Definition 3.15

Es sei $\sigma \in \mathbb{S}_n$ gegeben.

a. Ein Zahlenpaar (i, j) mit $1 \leq i, j \leq n$ heißt ein *Fehlstand* von σ, falls $i < j$, aber $\sigma(i) > \sigma(j)$.

b. Wir definieren das *Signum* oder *Vorzeichen* von σ durch

$$\operatorname{sgn}(\sigma) = \begin{cases} +1, & \text{falls } \sigma \text{ eine gerade Anzahl von Fehlständen besitzt,} \\ -1, & \text{falls } \sigma \text{ eine ungerade Anzahl von Fehlständen besitzt.} \end{cases}$$

---

[19] Siehe Bemerkung B.9.

Beispiel 3.16
Eine Transposition $\tau = (i\ j) \in \mathbb{S}_n$, mit $i < j$, hat die $2 \cdot (j - i - 1) + 1$ Fehlstände

$$(i, i+1), (i, i+2), \ldots, (i, j), (i+1, j), (i+2, j), \ldots, (j-1, j),$$

und mithin gilt $\text{sgn}(\tau) = -1$.

Die Permutation
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$
hat die Fehlstände $(1, 2)$ und $(3, 4)$. Also gilt $\text{sgn}(\sigma) = 1$. □

Manchmal ist die folgende geschlossene Formel nützlich, deren Beweis als Übungsaufgabe dem Leser überlassen sei, da wir sie im folgenden nicht verwenden werden.

Bemerkung 3.17
Für $\sigma \in \mathbb{S}_n$ gilt:
$$\text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \frac{\sigma(2) - \sigma(1)}{2 - 1} \cdot \frac{\sigma(3) - \sigma(1)}{3 - 1} \cdots \frac{\sigma(n) - \sigma(n-1)}{n - (n-1)}.$$
□

Weit wichtiger ist für uns die folgende Eigenschaft des Signums.

Satz 3.18

a. *Die Abbildung*
$$\text{sgn} : (\mathbb{S}_n, \circ) \longrightarrow \big(\{1, -1\}, \cdot\big)$$
ist ein Gruppenhomomorphismus, d.h. für $\sigma_1, \sigma_2 \in \mathbb{S}_n$ *gilt*
$$\text{sgn}(\sigma_1 \circ \sigma_2) = \text{sgn}(\sigma_1) \cdot \text{sgn}(\sigma_2).$$

b. *Ist* $\sigma = \tau_1 \circ \cdots \circ \tau_k \in \mathbb{S}_n$ *eine Komposition von* k *Transpositionen, dann gilt:*
$$\text{sgn}(\sigma) = (-1)^k.$$

c. *Ist* $\sigma \in \mathbb{S}_n$*, so kann* σ *entweder nur als Produkt einer geraden Anzahl von Transpositionen geschrieben werden oder nur als Produkt einer ungeraden Anzahl von Transpositionen.*

Beweis: Es sei $\sigma = \sigma' \circ \tau \in \mathbb{S}_n$ mit $\sigma' \in \mathbb{S}_n$ und $\tau = (i\ \ i+1)$ für ein $i \in \{1, \ldots, n-1\}$. Ist $(i, i+1)$ ein Fehlstand von σ', so hebt τ diesen auf und σ hat einen Fehlstand weniger als σ'. Ist hingegen $(i, i+1)$ kein Fehlstand von σ', so erzeugt die Komposition mit τ diesen Fehlstand neu und σ hat einen Fehlstand mehr als σ'. Damit gilt dann aber

$$\text{sgn}(\sigma) = -\,\text{sgn}(\sigma') = \text{sgn}(\sigma') \cdot \text{sgn}(\tau).$$

Nach Korollar 3.14 läßt sich jede Permutation als Produkt von Transpositionen aufeinanderfolgender Zahlen schreiben.

Seien nun $\sigma_1 = \tilde{\tau}_1 \circ \cdots \circ \tilde{\tau}_r$ und $\sigma_2 = \tilde{\tau}_{r+1} \circ \cdots \circ \tilde{\tau}_{r+s}$ als Produkte solcher Transpositionen aufeinanderfolgender Zahlen gegeben. Dann folgt mit Induktion über $r+s$, daß

$$\operatorname{sgn}(\sigma_1 \circ \sigma_2) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \operatorname{sgn}(\sigma_1) \cdot \operatorname{sgn}(\sigma_2).$$

Damit ist a. gezeigt und b. folgt mittels Induktion nach k.

Für c. sei schließlich $\sigma = \tau_1 \circ \cdots \circ \tau_k = \tau_1' \circ \cdots \circ \tau_l'$ mit Transpositionen $\tau_i, \tau_j' \in \mathbb{S}_n$. Dann folgt aus b.

$$(-1)^k = \operatorname{sgn}(\sigma) = (-1)^l,$$

und deshalb sind entweder k und l beide gerade oder beide ungerade. □

Definition 3.19
$\mathbb{A}_n := \operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in \mathbb{S}_n \mid \operatorname{sgn}(\sigma) = 1\}$ heißt *alternierende Gruppe* vom Grad n.

Bemerkung 3.20
Der Kern des Signums besteht aus allen Permutationen mit positivem Vorzeichen, man nennt diese auch *gerade* Permutationen, und ist nach Proposition 1.51 eine Untergruppe der $\mathbb{S}_n$.

Die Menge $\{\sigma \in \mathbb{S}_n \mid \operatorname{sgn}(\sigma) = -1\}$ ist keine Untergruppe der $\mathbb{S}_n$, da sie etwa das neutrale Element id nicht enthält.

Aufgabe 3.21
Betrachte die Permutationen

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 7 & 5 & 1 & 4 \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 1 & 4 & 5 & 6 \end{pmatrix} \in \mathbb{S}_7.$$

a. Berechne $\sigma \circ \pi$, $\pi \circ \sigma$, σ^{-1}, π^{-1}.

b. Bestimme für jede der Permutationen in a. die Zyklenzerlegung.

c. Schreibe $\sigma \circ \pi$ als ein Produkt von Transpositionen.

d. Schreibe π^{-1} als ein Produkt von Transpositionen aufeinander folgender Zahlen.

e. Berechne für jede der Permutationen in a. das Signum.

Aufgabe 3.22
Finde zwei Untergruppen von $\mathbb{S}_4$, die beide die Mächtigkeit 4 besitzen, aber nicht isomorph zueinander sind. Begründe, weshalb es Untergruppen sind und weshalb sie nicht isomorph zueinander sind.

Aufgabe 3.23
Bestimme die Elemente der Untergruppe $\mathbb{D}_8 = \langle (1\ 2\ 3\ 4), (2\ 4) \rangle \leq \mathbb{S}_4$ von $\mathbb{S}_4$.

Aufgabe 3.24
Bestimme die Elemente der Untergruppe $\mathbb{D}_{10} = \langle (1\ 2\ 3\ 4\ 5), (1\ 5) \circ (2\ 4) \rangle \leq \mathbb{S}_5$ von $\mathbb{S}_5$.

Aufgabe 3.25
Zeige, daß ein k-Zyklus σ die Ordnung[20] k und das Signum $(-1)^{k-1}$ hat.

Bemerkung 3.26
Für $n \in \mathbb{Z}$ mit $n \geq 3$ können wir zwei Permutationen

$$\pi_n = (1\ 2\ \ldots\ n-1\ n)$$

und

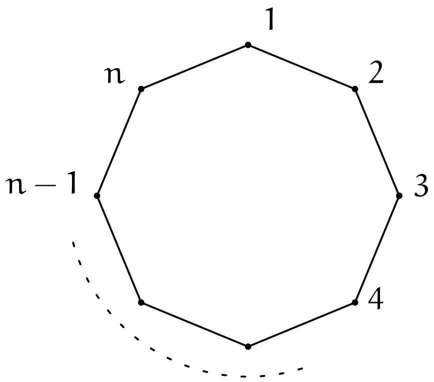
$$\sigma_n = \begin{cases} (1\ n) \circ (2\ n-1) \circ \ldots \circ \left(\frac{n}{2}\ \frac{n}{2}+1\right), & \text{falls } n \text{ gerade,} \\ (1\ n) \circ (2\ n-1) \circ \ldots \circ \left(\frac{n-1}{2}\ \frac{n+3}{2}\right), & \text{falls } n \text{ ungerade} \end{cases}$$

in $\mathbb{S}_n$ betrachten. Sie erzeugen die sogenannte *Diëdergruppe*

$$\mathbb{D}_{2n} = \langle \pi_n, \sigma_n \rangle \leq \mathbb{S}_n$$

der Ordnung $2n$.

Numeriert man die Ecken eines regulären n-Ecks im Uhrzeigersinn von 1 bis n,



so kann man π_n als Drehung des n-Ecks im Uhrzeigersinn um den Winkel $\frac{2\pi}{n}$ im Bogenmaß auffassen, die die Ecke mit Nummer 1 auf die Ecke mit Nummer 2 abbildet, die Ecke mit Nummer 2 auf die Ecke mit Nummer 3 und so weiter. Ensprechend kann man σ_n als Achsenspiegelung interpretieren. Die Diëdergruppe $\mathbb{D}_{2n}$ ist dann die volle Symmetriegruppe des regulären n-Ecks. Jedes Element entspricht entweder einer Drehung oder einer Spiegelung. (Siehe auch Beispiel 1.30.)

Die Gruppen $\mathbb{D}_8$ und $\mathbb{D}_{10}$ in den Aufgaben 3.23–4.18 sind Spezialfälle von solchen Diëdergruppen. Sie sind die Symmetriegruppen des Quadrates bzw. des regulären Fünfecks.

[20] Für den Begriff der Ordnung eines Elementes siehe Aufgabe 1.61

4 Normalteiler und Faktorgruppen

Der Begriff der *Faktorgruppe* zählt ganz ohne Frage zu den Begriffen, die Studienanfängern in Mathematik die größten Probleme bereiten. Die ersten Gruppen, die wir kennen gelernt haben, sind $(\mathbb{Z},+)$ und $(\mathbb{Q},+)$ – die Elemente sind schlicht Zahlen, etwas sehr vertrautes. Dann haben wir die symmetrische Gruppe betrachtet, deren Elemente Abbildungen sind. Für eine beliebige Menge M ist $\mathrm{Sym}(M)$ sicher schon nicht so ganz einfach gewesen, mußte doch z.B. die Gleichheit im Assoziativgesetz durch Einsetzen der Elemente von M in die Funktionen getestet werden. Der Übergang zur $\mathbb{S}_n$ sollte das Leben dann wieder einfacher gemacht haben, da die Elemente zu matrixähnlichen Schemata mit festen Rechenregeln wurden. Der Schritt zur Faktorgruppe scheint noch einmal höhere Anforderungen an das Abstraktionsvermögen der Studenten zu stellen, sind doch die Elemente jetzt plötzlich selbst eigentlich Mengen. Wie gesagt, damit tun sich die meisten Studienanfänger recht schwer, dabei ist es eigentlich sehr einfach. Man muß nur bereit sein, zu vergessen, was die Elemente eigentlich sind und sich (wie bei den Permutationen in der $\mathbb{S}_n$) nur die Rechenregeln für Faktorgruppen merken – und die sind so einfach wie sie nur sein können.

Wie alle Gruppen bestehen auch Faktorgruppen aus einer Menge zusammen mit einer Gruppenoperation. Die ersten beiden Abschnitte dieses Kapitels beschäftigen sich mehr oder weniger mit den Voraussetzungen für die einer Faktorgruppe zugrundeliegenden Menge.

A) **Der Satz von Lagrange**

In diesem Abschnitt betrachten wir einen bestimmten Typ von Äquivalenzrelation. Allerdings wollen wir jetzt voraussetzen, daß die zugrundeliegende Menge eine Gruppe ist. Zur Beschreibung der Äquivalenzklassen benötigen wir die folgende Notation, die auch im weiteren Verlauf der Vorlesung noch öfter von Nutzen sein wird.

Notation 4.1
Es sei $(G,\cdot)$ ein Gruppe und $A, B \subseteq G$ seien zwei Teilmengen. Wir definieren

$$A \cdot B = \{a \cdot b \mid a \in A, b \in B\}.$$

Manchmal schreiben wir abküzend AB für $A \cdot B$, und wenn $A = \{g\}$ einelementig ist, dann schreiben wir gB statt $\{g\}B$ und Bg statt $B\{g\}$.

Man beachte, daß sich die Assoziativität der Gruppenoperation auf das Produkt von Teilmengen überträgt, das heißt, für $A, B, C \subseteq G$ gilt

$$\begin{aligned}(A \cdot B) \cdot C &= \{(a \cdot b) \cdot c \mid a \in A, b \in B, c \in C\} \\ &= \{a \cdot (b \cdot c) \mid a \in A, b \in B, c \in C\} = A \cdot (B \cdot C).\end{aligned}$$

Proposition 4.2
Es sei G *eine Gruppe und* $U \leq G$*. Für zwei Elemente* $g, h \in G$ *definieren wir*

$$g \sim h \quad :\Longleftrightarrow \quad g^{-1}h \in U.$$

Dann ist $\sim$ *eine Äquivalenzrelation auf der Menge* G *und die zu* g *gehörende Äquivalenzklasse ist*

$$\overline{g} = gU = \{gu \mid u \in U\}.$$

Wir nennen gU *die zu* g *gehörende* Linksnebenklasse *von* U *in* G *und* g *einen* Repräsentanten *der Linksnebenklasse. Außerdem bezeichnen wir mit*

$$G/U = \{gU \mid g \in G\}$$

die Menge aller Linksnebenklassen von U *in* G *und nennen die Mächtigkeit von* G/U

$$|G : U| := |G/U|$$

den Index *von* U *in* G*.*

Beweis: Wir müssen zeigen, daß die durch $\sim$ definierte Relation auf G reflexiv, symmetrisch und transitiv ist. Seien dazu $g, h, k \in G$.

R1: Da $g^{-1}g = e \in U$, gilt $g \sim g$ und $\sim$ reflexiv.
R2: Es gelte $g \sim h$ und damit $g^{-1}h \in U$. Aus der Abgeschlossenheit von U bezüglich der Inversenbildung folgt dann aber $h^{-1}g = \left(g^{-1}h\right)^{-1} \in U$. Es ist also $h \sim g$, und $\sim$ ist symmetrisch.
R3: Es gelte $g \sim h$ und $h \sim k$ und damit $g^{-1}h \in U$ und $h^{-1}k \in U$. Wegen der Abgeschlossenheit von U bezüglich der Gruppenoperation folgt daraus $g^{-1}k = \left(g^{-1}h\right)\left(h^{-1}k\right) \in U$ und somit $g \sim k$. $\sim$ ist also auch transitiv.

Mithin ist $\sim$ eine Äquivalenzrelation.

Es bleibt zu zeigen, daß die Menge der zu g äquivalenten Elemente gU ist. Ist $h \in G$ mit $g \sim h$, so gilt nach Definition $g^{-1}h \in U$ und damit $h = g \cdot (g^{-1}h) \in gU$. Ist umgekehrt $h = gu \in gU$ mit $u \in U$, so gilt $g^{-1}h = g^{-1}gu = u \in U$ und somit $g \sim h$. □

Da eine Äquivalenzrelation auf der Menge, auf der sie definiert ist, eine disjunkte Zerlegung in Äquivalenzklassen induziert (siehe Proposition 2.8), erhalten wir das folgende Korollar geschenkt.

Korollar 4.3
Es sei G *eine Gruppe und* $U \leq G$*. Für* $g, h \in G$ *gilt entweder* $gU = hU$ *oder* $gU \cap hU = \emptyset$*, und* G *ist die disjunkte Vereinigung der Linksnebenklassen von* U *in*

G.[21]

$$G = \dot{\bigcup_{\lambda \in G/U}} g_\lambda U,$$

wobei $g_\lambda \in G$ *irgendein Repräsentant der Linksnebenklasse* λ *ist, d.h.* $\lambda = g_\lambda U$.

Beispiel 4.4
Betrachten wir die Gruppe $G = \mathbb{S}_3$ und die Untergruppe $U = \mathbb{A}_3$. Dann gibt es zwei Nebenklassen:

$$\mathbb{A}_3 = \mathrm{id}\,\mathbb{A}_3 = (1\ 2\ 3)\mathbb{A}_3 = (1\ 3\ 2)\mathbb{A}_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

und

$$(1\ 2)\mathbb{A}_3 = (1\ 3)\mathbb{A}_3 = (2\ 3)\mathbb{A}_3 = \{(1\ 2), (1\ 3), (2\ 3)\}.$$

Mithin ist der Index $|\mathbb{S}_3 : \mathbb{A}_3|$ von $\mathbb{A}_3$ in $\mathbb{S}_3$ zwei.

Bemerkung 4.5
Eine Linksnebenklasse von U in G kennt man, ganz unabhängig davon, was U und G konkret sind, nämlich die Linksnebenklasse des neutralen Elementes:

$$eU = U$$

D.h. die Untergruppe selbst ist immer eine Linksnebenklasse.

Zudem sollte man beachten, daß die möglichen Repräsentanten einer Linksnebenklasse genau die Elemente in der Nebenklasse sind. Insbesondere gilt $uU = U$ für jedes $u \in U$. □

Das vielleicht wichtigste Beispiel für unsere Vorlesung ist die Menge $\mathbb{Z}/n\mathbb{Z}$ der Linksnebenklassen der Untergruppe $n\mathbb{Z}$ in der Gruppe $(\mathbb{Z}, +)$. Um in diesem Beispiel alle Linksnebenklassen beschreiben zu können und für jede einen möglichst *einfachen* Repräsentanten angeben zu können, benötigen wir das Prinzip der *Division mit Rest* auf den ganzen Zahlen.

Proposition 4.6
Ist $(G, \cdot) = (\mathbb{Z}, +)$ *und* $U = n\mathbb{Z}$ *für eine natürliche Zahl* $n \geq 1$, *dann hat* U *genau*

[21] Man beachte, daß bei der Vereinigung $\dot{\bigcup}_{\lambda \in G/U} g_\lambda U$ jede Nebenklasse von U in G nur *genau einmal* in der Vereinigung aufgeführt wird, da für jede Nebenklasse nur ein Vertreter gewählt wurde.

n *Linksnebenklassen in* G*, nämlich:*[22]

$$\begin{array}{rcccc} \overline{0} & = & 0+n\mathbb{Z} & = & n\mathbb{Z}, \\ \overline{1} & = & 1+n\mathbb{Z} & = & \{1+nz \mid z \in \mathbb{Z}\}, \\ \overline{2} & = & 2+n\mathbb{Z} & = & \{2+nz \mid z \in \mathbb{Z}\}, \\ \vdots & & & & \\ \overline{n-1} & = & (n-1)+n\mathbb{Z} & = & \{n-1+nz \mid z \in \mathbb{Z}\}. \end{array}$$

Der Index $|\mathbb{Z} : n\mathbb{Z}|$ *von* $n\mathbb{Z}$ *in* $\mathbb{Z}$ *ist mithin* n*.*

Beweis: Wir müssen zeigen, daß jede ganze Zahl $m \in \mathbb{Z}$ in einer der oben angeführten n Äquivalenzklassen liegt, und daß diese paarweise verschieden sind.

Sei also $m \in \mathbb{Z}$ eine beliebige ganze Zahl, dann existieren aufgrund der Division mit Rest ganze Zahlen $q, r \in \mathbb{Z}$, so daß

$$m = qn + r \quad \text{mit} \quad 0 \leq r \leq n-1.$$

Aber damit folgt[23]

$$m - r = qn = nq \in n\mathbb{Z} = U.$$

Damit ist m äquivalent zu r, und deshalb $m \in \overline{r}$, wobei $\overline{r}$ eine der oben aufgeführten n Äquivalenzklassen ist.

Es bleibt für $0 \leq i < j \leq n-1$ zu zeigen, daß $\overline{i} \neq \overline{j}$. Würde $\overline{i} = \overline{j}$ gelten, dann wäre j äquivalent zu i und somit $j - i \in n\mathbb{Z}$ ein Vielfaches von n. Nach Voraussetzung wissen wir aber, daß $0 < j - i < n$ kein Vielfaches von n sein kann. Also sind $\overline{i}$ und $\overline{j}$ nicht gleich. □

Notation 4.7
Im folgenden werden wir meist $\mathbb{Z}_n$ statt $\mathbb{Z}/n\mathbb{Z}$ schreiben. Außerdem schreiben wir für eine Restklasse $\overline{a}$ aus $\mathbb{Z}_n$ manchmal $\overline{a}_n$, wenn wir verdeutlichen wollen, modulo welcher Zahl wir rechnen. Dies ist immer dann wichtig, wenn wir parallel modulo verschiedener Zahlen rechnen wollen.

Die Menge $\mathbb{Z}_n$ ist uns bereits in der Einleitung in den Fällen $n = 10$ und $n = 26$ begegnet und wird für den Rest der Vorlesung von großer Bedeutung sein. Wir führen deshalb hier noch einige übliche Sprechweisen im Zusammenhang mit diesem Beispiel ein.

[22] Man beachte, daß dadurch, daß die Gruppenoperation die Addition ist, eine Linksnebenklasse nicht "$g \cdot U$" ist, sondern "$g + U$". Das wäre an sich vielleicht noch nicht so verwirrend, wenn in diesem konkreten Beispiel nicht auch noch die Untergruppe $U = n\mathbb{Z}$ selbst einer multiplikativ geschriebenen Nebenklasse zum Verwechseln ähnlich sähe! Das ist einer der wesentlichen Gründe, weshalb wir im Folgenden für dieses konkrete Beispiel meist die Notation $\overline{k}$ der Notation $k + n\mathbb{Z}$ vorziehen.

[23] Man beachte wieder, daß die Gruppenoperation in $(\mathbb{Z}, +)$ die Addition ist. Die Bedingung "$g^{-1}h \in U$" übersetzt sich hier deshalb zu "$-g + h \in U$". Und da die Addition zudem kommutativ ist, schreiben wir meist lieber "$h - g \in U$".

Bemerkung 4.8
Sei $n \in \mathbb{Z}$ fest gewählt. $x, y \in \mathbb{Z}$ heißen *kongruent modulo* n, falls

$$x - y \in n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}.$$

Die Kongurenz ist genau die in Proposition 4.6 betrachtete Äquivalenzrelation, aber statt des Zeichens "∼" hat sich in dieser Situation folgende Notation dafür eingebürgert, daß x kongruent zu y modulo n ist:

$$x \equiv y \ (n) \quad \text{oder} \quad x \equiv y \ (\mathrm{mod}\ n).$$

□

Wir wollen diesen Abschnitt mit einem wichtigen Satz, dem Satz von Lagrange abschließen. Seine wichtigste Aussage ist, daß bei einer endlichen Gruppe die Mächtigkeit einer Untergruppe stets die Mächtigkeit der Gruppe teilen muß! Das folgende Lemma ist ein zentraler Baustein im Beweis des Satzes.

Lemma 4.9
Es sei G *eine Gruppe,* $U \leq G$ *und* $g \in G$. *Dann ist die Abbildung*

$$l_g : U \longrightarrow gU : u \mapsto gu$$

eine Bijektion. Insbesondere haben also alle Linksnebenklassen von U *in* G *die Mächtigkeit* $|U|$.

Beweis: Wegen der Kürzungsregel folgt aus $l_g(u) = gu = gu' = l_g(u')$ für $u, u' \in U$ unmittelbar, daß $u = u'$. Also ist l_g injektiv. Ist nun $h \in gU$ ein beliebiges Element, so gibt es nach Definition von gU ein $u \in U$, so daß $h = gu$. Aber damit ist $h = gu = l_g(u)$, und mithin ist l_g surjektiv. Die Aussage zur Mächtigkeit von Linksnebenklassen folgt, da zwei Mengen nach Definition genau dann gleichmächtig sind, wenn es eine Bijektion zwischen ihnen gibt. □

Satz 4.10 (Satz von Lagrange)
Es sei G *eine endliche Gruppe und* $U \leq G$ *eine Untergruppe von* G. *Dann gilt*

$$|G| = |U| \cdot |G : U|.$$

Insbesondere gilt, $|U|$ *und* $|G/U| = |G : U|$ *sind Teiler von* $|G|$.

Beweis: Da G endlich ist notwendig auch G/U endlich. Sei also $G/U = \{\lambda_1, \ldots, \lambda_k\}$ und die λ_i seien paarweise verschieden, insbesondere also $|G : U| = |G/U| = k$. Da die Elemente von G/U Linksnebenklassen von U in G sind, können wir für jedes λ_i einen Repräsentanten $g_i \in G$ wählen, so daß $\lambda_i = g_iU$ gilt. Aus Korollar 2.9 und Lemma 4.9 folgt dann:

$$|G| \stackrel{2.9}{=} \sum_{i=1}^{k} |\lambda_i| = \sum_{i=1}^{k} |g_iU| \stackrel{4.9}{=} \sum_{i=1}^{k} |U| = |U| \cdot k = |U| \cdot |G : U|.$$

□

Aus dem Satz von Lagrange erhalten wir unmittelbar folgendes Korollar.

Korollar 4.11
Ist G *eine Gruppe und* $g \in G$*, so definieren wir die* Ordnung *von* g *als* $o(g) := |\langle g \rangle|$*, und wenn* G *endlich ist, dann ist* $o(g)$ *ein Teiler von* $|G|$*.*

Bemerkung 4.12
Ist G eine Gruppe und $g \in G$, dann folgt aus aus Aufgabe 1.55

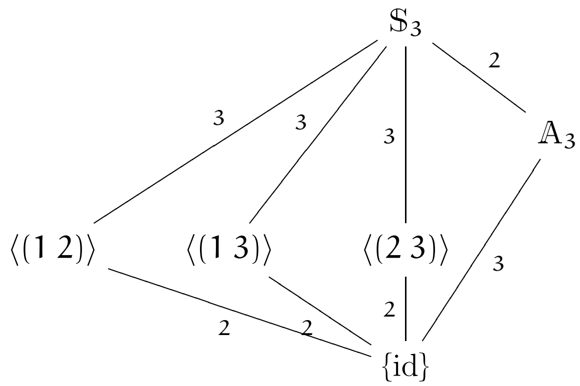
$$o(g) = \inf\{k > 0 \mid g^k = e\} \in \mathbb{N} \cup \{\infty\}.$$

Wir wollen die Nützlichkeit des Satzes von Lagrange an einem Beispiel verdeutlichen.

Beispiel 4.13
Sei $U \leq \mathbb{S}_3$, dann gilt $|U| \in \{1, 2, 3, 6\}$ wegen des Satzes von Lagrange und da $|\mathbb{S}_3| = 3! = 6$.

1. **Fall: $|U| = 1$:** Dann ist notwendig $U = \{\text{id}\}$, da das neutrale Element von $\mathbb{S}_3$ in U liegt.
2. **Fall: $|U| = 6$:** Da U eine Teilmenge von $\mathbb{S}_3$ ist muß mithin $U = \mathbb{S}_3$ gelten.
3. **Fall: $|U| = 2$:** Es gibt ein Element $\text{id} \neq \sigma \in U$ und damit gilt $o(\sigma) \neq 1$. Aus Korollar 4.11 wissen wir, daß $o(\sigma)$ ein Teiler von $|U| = 2$ ist. Da 2 eine Primzahl ist, folgt mithin $o(\sigma) = 2$ und $U = \langle \sigma \rangle$ ist von σ erzeugt. Also gilt $\sigma \in \{(1\ 2), (1\ 3), (2\ 3)\}$ und wir erhalten drei Untergruppen der Ordnung 2:
$$U = \{\text{id}, (1\ 2)\} \text{ oder } U = \{\text{id}, (1\ 3)\} \text{ oder } U = \{\text{id}, (2\ 3)\}.$$
4. **Fall: $|U| = 3$:** Wie im dritten Fall gibt es ein $\text{id} \neq \sigma \in U$ und $1 \neq o(\sigma) \mid |U| = 3$. Da auch 3 eine Primzahl ist gilt $o(\sigma) = 3$ und $U = \langle \sigma \rangle$. Dann ist aber $\sigma \in \{(1\ 2\ 3), (1\ 3\ 2)\}$ und
$$U = \langle (1\ 2\ 3) \rangle = \langle (1\ 3\ 2) \rangle = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\} = \mathbb{A}_3.$$

Wir kennen mithin alle Untergruppen der $\mathbb{S}_3$ und können sie in folgendem *Untegruppendiagramm* festhalten:



Die Striche zwischen zwei Gruppen deuten an, daß die weiter oben stehende die weiter unten stehende enthält, und die Zahlen an den Strichen geben den Index der kleineren Gruppe in der größeren an.

Bemerkung 4.14
Wir haben die Äquivalenzklassen bezüglich der in Proposition 4.2 eingeführten Äquivalenzrelation *Links*nebenklassen genannt, weil sie die Form gU haben, die definierende Untergruppe also von *links* mit dem Repräsentanten g multipliziert wird. Analog dazu könnte man die folgende Relation betrachten:

$$g \sim h \iff hg^{-1} \in U.$$

Auch dies definiert eine Äquivalenzrelation. Die zu g gehörende Äquivalenzklasse ist Ug und wird eine *Rechtsnebenklasse* von U in G genannt. Das Analogon von Lemma 4.9 gilt natürlich auch für Rechtsnebenklassen, und damit kann man dann auch das Analogon des Satzes von Lagrange zeigen, daß nämlich in einer endlichen Gruppe G für eine Untergruppe U mit m paarweise verschiedenen Rechtsnebenklassen notwendig die Beziehung $|G| = |U| \cdot m$ gilt. Aber damit folgt schließlich, daß $m = |G : U|$, oder anders ausgedrückt, daß die Anzahl an Rechtsnebenklassen gleich der Anzahl an Linksnebenklassen ist.

Es gilt im allgemeinen jedoch nicht $gU = Ug$, wie man sich am Beispiel $G = \mathbb{S}_3$, $U = \{\mathrm{id}, (1\ 2)\}$ und $g = (1\ 3)$ leicht verdeutlichen kann. Untergruppen, für die stets $gU = Ug$ gilt, wollen wir im folgenden Abschnitt näher betrachten. □

Aufgabe 4.15 (Produktformel)
Es seien $U, V \leq G$ Untergruppen der Gruppe $(G, \cdot)$.

a. Zeige, daß durch
$$(u, v) \sim (u', v') \iff u \cdot v = u' \cdot v'$$
eine Äquivalenzrelation auf der Menge $U \times V$ definiert wird.

b. Zeige, daß die Äquivalenzklasse von $(u, v) \in U \times V$ die Gestalt
$$\overline{(u, v)} = \left\{ \left(u \cdot y, y^{-1} \cdot v\right) \mid y \in U \cap V \right\}$$
besitzt und die Mächtigkeit $|U \cap V|$ hat.

c. Beweise, wenn U und V endlich sind, so gilt die Produktformel
$$|U \cdot V| = \frac{|U| \cdot |V|}{|U \cap V|}.$$

Bemerkung 4.16
Die Formel in obiger Aufgabe ist besonders nützlich, wenn die Menge $U \cdot V$ eine Untergruppe von G ist. Das ist aber nicht immer der Fall, wie wir mit dem Satz von Lagrange leicht sehen können: das Produkt der Untergruppen $\langle (1\ 2) \rangle$ und $\langle (1\ 3) \rangle$ von $\mathbb{S}_3$ ist wegen der Aufgabe eine Teilmenge der Mächtigkeit 4 und kann nach dem Satz von Lagrange deshalb keine Untergruppe von $\mathbb{S}_3$ sein. Wir werden im folgenden Abschnitt (siehe Lemma 4.29) eine Bedingung kennen lernen, die V erfüllen muß, damit $U \cdot V$ eine Untergruppe von G wird.

Aufgabe 4.17
Ist $(G, \cdot)$ eine Gruppe und $|G|$ eine Primzahl, so ist G zyklisch.

Aufgabe 4.18
Bestimme alle Untergruppen der Gruppe $\mathbb{D}_8 = \langle(1\ 2\ 3\ 4), (2\ 4)\rangle$.

Aufgabe 4.19
Bestimme alle Untergruppen der Gruppe $\mathbb{D}_{10} = \langle(1\ 2\ 3\ 4\ 5), (1\ 5) \circ (2\ 4)\rangle$.

B) **Normalteiler**

Im Kapitel über Äquivalenzrelationen haben wir gesehen, daß eine Äquivalenzrelation genau das richtige Mittel ist, um Ordung in eine Menge zu bringen, indem wir ihre Elemente nach vorgegebenen Gesichtspunkten zu größeren Einheiten zusammenfassen. Kurz gesagt, man verwendet Äquivalenzrelationen auf Mengen, um deren Elemente zu klassifizieren. Man erhält bei diesem Prozess wieder eine Menge, nämlich die Menge der Äquivalenzklassen. In dieser Vorlesung wollen wir uns aber stets mit Mengen beschäftigen, die eine zusätzliche Struktur tragen, und da ist es eine naheliegende Frage, ob sich die Struktur denn von der ursprünglichen Menge auf die neue Menge, die der Äquivalenzklassen, übertragen läßt. Ganz konkret, wenn G eine Gruppe ist und U eine Untergruppe von G, kann man dann auf *natürliche* Weise G/U zu einer Gruppe machen?

Dabei soll *natürlich* bedeuten, daß die Idee zur Definition der Gruppenoperation sofort ins Auge springt. Wir haben zwei Linksnebenklassen gU und hU, diese sind Teilmengen von G und das Produkt von Teilmengen von G wurde bereits in Notation 4.1 eingeführt. Natürlicher hätte man es sicher nicht definieren können. Allerdings soll dieses Produkt auch wieder eine Linksnebenklasse sein, das heißt wir müssen einen Repräsentanten davon angeben, und wenn unsere Definition des Produktes wirklich *natürlich* ist, dann sollte dieser Repräsentant sich aus den Repräsentanten der gegebenen Linksnebenklassen ergeben, d.h. wir wünschen uns, daß $gU \cdot hU = ghU$ gilt. Dies gilt leider nicht für alle Untergruppen und führt deshalb zu folgender Definition.

Definition 4.20
Eine Untergruppe $U \leq G$ von G heißt *normal* oder *Normalteiler*, falls für alle $g \in G$ und $u \in U$ gilt

$$gug^{-1} \in U. \tag{26}$$

Wir schreiben in diesem Falle $U \trianglelefteq G$.

Bemerkung 4.21
Um zu zeigen, daß eine *Teilmenge* $U \subseteq G$ ein Normalteiler ist, reicht es *nicht* die Eigenschaft (26) für alle $g \in G$ und $u \in U$ zu überprüfen. Zunächst muß gezeigt werden, daß U eine *Untergruppe* von G ist! Daß dies ein wesentlicher Bestandteil der Definition des Begriffs Normalteiler ist, wird von Studienanfängern häufig übersehen.

Beispiel 4.22
Ist G eine Gruppe, so sind die Untergruppen $\{e\}$ und G stets Normalteiler. Man nennt sie deshalb auch die *trivialen* Normalteiler.

Lemma 4.23
Ist G eine abelsche Gruppe, so ist jede Untergruppe von G ein Normalteiler.

Beweis: Für $g \in G$ und $u \in U \leq G$ gilt $gug^{-1} = gg^{-1}u = eu = u \in U$. □

Aus diesem Lemma ergibt sich sofort folgendes Beispiel.

Beispiel 4.24
Für jedes $n \in \mathbb{Z}$ ist die Untergruppe $n\mathbb{Z}$ von $(\mathbb{Z}, +)$ ein Normalteiler.

Proposition 4.25
Es sei G eine Gruppe und $U \leq G$ eine Untergruppe. Die folgenden Aussagen sind äquivalent:[24]

a. $U \trianglelefteq G$ *ist ein Normalteiler von* G.
b. $gUg^{-1} = U$ *für alle* $g \in G$.
c. $gU = Ug$ *für alle* $g \in G$.
d. $(gU) \cdot (hU) = ghU$ *für alle* $g, h \in G$.

Beweis: Wir überlassen den Beweis dem Leser als Übungsaufgabe.

□

Beispiel 4.26
Die Untergruppe $U := \{\mathrm{id}, (1\ 2)\} \subset \mathbb{S}_3$ ist kein Normalteiler der $\mathbb{S}_3$, denn für $\sigma = (2\ 3) \in \mathbb{S}_3$ gilt

$$\sigma \circ (1\ 2) \circ \sigma^{-1} = (2\ 3) \circ (1\ 2) \circ (2\ 3) = (1\ 3) \not\in U.$$

Eine gute Quelle zum Auffinden von Normalteilern sind Gruppenhomomorphismen.

Proposition 4.27
Ist $\alpha : G \to H$ ein Gruppenhomomorphismus, dann ist $\mathrm{Ker}(\alpha) \trianglelefteq G$.

Beweis: Wir wissen bereits aus Proposition 1.51, daß $\mathrm{Ker}(\alpha) \leq G$ eine Untergruppe von G ist. Sei nun $u \in \mathrm{Ker}(\alpha)$ und $g \in G$, dann gilt

$$\alpha\big(gug^{-1}\big) = \alpha(g) \cdot \alpha(u) \cdot \alpha\big(g^{-1}\big) \overset{u \in \mathrm{Ker}(\alpha)}{=} \alpha(g) \cdot e_H \cdot \alpha\big(g^{-1}\big) = \alpha(g) \cdot \alpha\big(g^{-1}\big) = \alpha\big(gg^{-1}\big) = \alpha(e_G) = e_H.$$

Aber damit ist $gug^{-1} \in \mathrm{Ker}(\alpha)$ und $\mathrm{Ker}(\alpha) \trianglelefteq G$. □

[24] Um die Äquivalenz von mehreren Aussagen zu zeigen, kann man einen sogenannten Ringschluß machen. Es reicht zu zeigen: “a. ⇒ b. ⇒ c. ⇒ d. ⇒ a.”, denn aus “a. ⇒ b.” und “b. ⇒ c.” folgt z.B. “a. ⇒ c.”, d.h. die scheinbar noch fehlenden Implikationen ergeben sich von selbst.

Beispiel 4.28
Betrachten wir den surjektiven Gruppenhomomorphismus (vgl. Bemerkung 3.20)

$$\mathrm{sgn} : \mathbb{S}_n \to \{-1, 1\},$$

dann gilt $\mathrm{Ker}(\mathrm{sgn}) = \mathbb{A}_n$ ist ein Normalteiler von $\mathbb{S}_n$.

Im allgemeinen ist das Produkt von zwei Untergruppen keine Untergruppe mehr. Betrachtet man etwa die Gruppe $G = \mathbb{S}_3$ sowie die Untergruppen $U = \{\mathrm{id}, (1\ 2)\}$ und $V = \{\mathrm{id}, (1,\ 3)\}$, so ist $UV = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 2\ 3)\}$ und kann wegen des Satzes von Lagrange keine Untergruppe von G sein, da $|UV| = 4$ kein Teiler von $|G| = 6$ ist. Ist aber eine der beiden Untergruppen ein Normalteiler, sieht die Welt anders aus. Normalteiler sind also durchaus nützlich.

Lemma 4.29
Es sei G eine Gruppe, $U \leq G$ und $N \trianglelefteq G$. Dann gilt:

a. $UN \leq G$.

b. $N \trianglelefteq UN$.

c. $U \cap N \trianglelefteq U$.

Beweis: Da N ein Normalteiler ist gilt nach Proposition 4.25

$$(UN) \cdot (UN) = U \cdot (NU) \cdot N = U \cdot (UN) \cdot N = (UU) \cdot (NN) = UN,$$

da $UU = U$ und $NN = N$. Damit gilt aber insbesondere, daß $g \cdot h \in UN$ für alle $g, h \in UN$.

Sei nun $g = un \in UN$ mit $u \in U$ und $n \in N$, dann ist

$$g^{-1} = n^{-1}u^{-1} \in NU \overset{\text{Prop. 4.25}}{=} UN.$$

Da ferner $e = e \cdot e \in UN$ und also UN nicht leer ist, ist UN eine Untergruppe nach dem Untergruppenkriterium.

Damit ist Teil a. gezeigt. Die beiden andere Aussagen überlassen wir dem Leser als Übungsaufgabe. □

Beispiel 4.30
Wir betrachten die Untergruppen $U = \langle(1\ 2)\rangle$ und $V = \langle(2\ 3)\rangle$ von $\mathbb{S}_3$. Dann gilt

$$U \cdot U' = \{\mathrm{id}, (1\ 2), (2\ 3), (1\ 2\ 3)\}$$

und wegen des Satzes von Lagrange kann dieses Produkt keine Untergruppe von $\mathbb{S}_3$ sein. Dies zeigt, daß die Bedinung $N \trianglelefteq G$ in Lemma 4.29 wesentlich ist.

Aufgabe 4.31
Beweise Proposition 4.25.

Aufgabe 4.32
Beweise Teil b. und c. von 4.29.

Aufgabe 4.33
Es sei G eine endliche Gruppe und $U \leq G$ eine Untergruppe vom Index $|G : U| = 2$. Zeige, U ist ein Normalteiler von G.

Aufgabe 4.34
Es sei G eine Gruppe und $N \leq G$ die einzige Untergruppe von G mit Ordnung $|N| = n$. Zeige, dann ist $N \trianglelefteq G$ ein Normalteiler.

Aufgabe 4.35
Bestimme alle Normalteiler der Gruppe $\mathbb{D}_8 = \langle (1\,2\,3\,4), (2\,4) \rangle$.

Aufgabe 4.36
Bestimme alle Normalteiler der Gruppe $\mathbb{D}_{10} = \langle (1\,2\,3\,4\ ), (1\,5) \circ (2\,4) \rangle$.

C) **Faktorgruppe**

Jetzt sind wir in der Lage, den Satz zu formulieren, der der Faktorgruppe, d.h. der Gruppenoperation auf G/U, ans Licht der Welt verhilft. In der Hoffnung, daß die Notation $\overline{g}$ für die Linksnebenklasse gU einer Untergruppe das Rechnen mit den Elementen der Faktorgruppe leichter macht, indem er verschleiert, daß das *Element* $\overline{g} = gU$ eigentlich eine *Menge* ist, werden wir den Satz mit dieser Notation formulieren.

Satz 4.37
Es sei $(G, \cdot)$ *eine Gruppe und* $U \trianglelefteq G$ *ein Normalteiler von* G. *Dann gilt*[25]

$$\overline{g} \cdot \overline{h} = \overline{g \cdot h}, \qquad \textit{für } \overline{g}, \overline{h} \in G/U. \tag{27}$$

Bezüglich der durch diese Multiplikation gegebenen zweistelligen Operation auf G/U *ist* G/U *eine Gruppe. Das* neutrale Element *von* $(G/U, \cdot)$ *ist die Linksnebenklasse* $\overline{e} = U$*, und das zu* $\overline{g} = gU \in G/U$ *existierende* Inverse *Element ist die Linksnebenklasse* $\overline{g^{-1}} = g^{-1}U$.

Außerdem ist die Restklassenabbildung

$$\pi : G \to G/U : g \mapsto \overline{g}$$

ein Epimorphismus mit $\mathrm{Ker}(\pi) = U$.

Man nennt G/U *die* Faktorgruppe *von* G *nach* U.

Beweis: Die Gleichheit in (27) folgt aus 4.25, da U ein Normalteiler ist:

$$\overline{g} \cdot \overline{h} = gU \cdot hU = ghU = \overline{gh}.$$

Zeigen wir nun, daß G/U mit dieser Operation eine Gruppe ist.

Für $\overline{g}, \overline{h}, \overline{k} \in G/U$ folgt mittels der Assoziativität der Multiplikation in G:

$$\left(\overline{g} \cdot \overline{h}\right) \cdot \overline{k} = \overline{gh} \cdot \overline{k} = \overline{(gh)k} = \overline{g(hk)} = \overline{g} \cdot \overline{hk} = \overline{g} \cdot \left(\overline{h} \cdot \overline{k}\right).$$

[25]Dabei ist mit $\overline{g} \cdot \overline{h} = gU \cdot hU$ einfach das Produkt von Teilmengen von G gemeint, wie es in Notation 4.1 eingeführt wurde.

Außerdem ist $\overline{e} \cdot \overline{g} = \overline{eg} = \overline{g}$, so daß $\overline{e}$ das Neutrale von G/U ist, und es gilt

$$\overline{g^{-1}} \cdot \overline{g} = \overline{g^{-1} \cdot g} = \overline{e},$$

und somit besitzt $\overline{g}$ ein Inverses, nämlich $\overline{g}^{-1} = \overline{g^{-1}}$. Also ist G/U eine Gruppe und die bezüglich des neutralen Elementes bzw. der Inversen getroffenen Aussagen sind ebenfalls gezeigt.

Zudem folgt aus der Definition von π

$$\pi(gh) = \overline{gh} \overset{(27)}{=} \overline{g} \cdot \overline{h} = \pi(g) \cdot \pi(h)$$

und

$$\mathrm{Ker}(\pi) = \{g \in G \mid \pi(g) = \overline{e}\} = \{g \in G \mid \overline{g} = \overline{e}\} = \overline{e} = U,$$

so daß π ein Gruppenhomomorphismus mit $\mathrm{Ker}(\pi) = U$ ist. □

Bemerkung 4.38

a. Wir haben für den Beweis des Satzes ausgenutzt, daß das Produkt $\overline{g} \cdot \overline{h}$ ein Produkt von Teilmengen der Gruppe G ist. Diesen Umstand wollen wir nun tunlichst wieder *vergessen*! Wir merken uns nur: jedes Element $\overline{g}$ von G/U ist uns gegeben durch eine Repräsentanten und alle Operationen werden mittels dieser Repräsentanten ausgeführt. D.h. wir müssen uns nur folgende Regeln merken, um mit der Faktorgruppe rechnen zu können:
   (i) $\overline{g} \cdot \overline{h} = \overline{g \cdot h}$,
   (ii) $\overline{g}^{-1} = \overline{g^{-1}}$,
   (iii) $e_{G/U} = \overline{e} = \overline{u}$, wann immer $u \in U$.

b. Ist die Gruppe $(G, \cdot)$ abelsch und $U \trianglelefteq G$, so ist auch $(G/U, \cdot)$ abelsch, da

$$\overline{g} \cdot \overline{h} = \overline{gh} = \overline{hg} = \overline{h} \cdot \overline{g}.$$

c. Satz 4.37 zeigt, daß die Multiplikation der Linksnebenklassen auf der Menge G/U der Linksnebenklassen eine Gruppenoperation liefert, wenn U ein Normalteiler ist. Beachtet man zudem, daß das Produkt der Linksnebenklassen gU und hU auf alle Fälle das Element $gh = gehe$ enthält, so sieht man mit Proposition 4.25, daß es, wenn U kein Normalteiler ist, zwei Elemente $g, h \in G$ gibt, so daß das Produkt von gU mit hU keine Linksnebenklasse mehr ist. Das heißt, wenn U kein Normalteiler ist, kann G/U mit der obigen Multiplikation keine Gruppe sein. Es sind genau die Normalteiler, für die das Verfahren funktioniert.

Als unmittelbare Folgerung erhalten wir den Spezialfall $\mathbb{Z}_n$, da $n\mathbb{Z}$ ein Normalteiler von $(\mathbb{Z}, +)$ ist.

Korollar 4.39

Für $n \in \mathbb{Z}$ *ist* $(\mathbb{Z}_n, +)$ *eine abelsche Gruppe, wobei* $\overline{x} + \overline{y} = \overline{x + y}$ *für* $x, y \in \mathbb{Z}$.

Bemerkung 4.40
Das Rechnen in $\mathbb{Z}_n$ für ausgewählte n ist uns seit unseren Kindertagen vertraut. Wenn unsere Uhr neun Uhr anzeigt, so wissen wir, daß es in fünf Stunden zwei Uhr ist. Wir rechnen dabei in $\mathbb{Z}_{12}$:

$$\overline{9}+\overline{5}=\overline{14}=\overline{2+1\cdot 12}=\overline{2}.$$

Wer eine Uhr mit 24-Stundenrythmus bevorzugt, rechnet in $\mathbb{Z}_{24}$. Ist es jetzt neun Uhr, so war es vor 55 Stunden zwei Uhr:

$$\overline{9}-\overline{55}=\overline{-46}=\overline{2-2\cdot 24}=\overline{2}.$$

Numeriert man die Wochentag von eins (Montag) bis sieben (Sonntag), so ist die Frage danach, welcher Wochentag in 51 Tagen ist, wenn heute Montag ist, eine Rechnung in $\mathbb{Z}_7$:

$$\overline{1}+\overline{51}=\overline{52}=\overline{2+7\cdot 7}=\overline{2}.$$

In 51 Tagen ist also Dienstag.

Um sich mit dem Rechnen in $\mathbb{Z}_n$ vertraut zu machen, empfehle ich, ein wenig mit Uhrzeiten und Wochentagen unter diesem Gesichtspunkt zu rechnen. □

Beispiel 4.41
Für Gruppen kleiner Ordnung, d. h. mit wenig Elementen, ist es sinnvoll sog. Verknüpfungstafeln aufzustellen, aus denen zu je zwei gegebenen Elementen die Verknüpfung der beiden Elemente abgelesen werden kann. Im Falle von $\mathbb{Z}_n$ erhalten wir für $n=2,3,4$ die folgenden Verknüpfungstafeln:

$$\begin{array}{c|cc} + & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \end{array} \qquad \begin{array}{c|ccc} + & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{1} & \overline{2} & \overline{0} \\ \overline{2} & \overline{2} & \overline{0} & \overline{1} \end{array} \qquad \begin{array}{c|cccc} + & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\ \overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\ \overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2} \end{array}$$

□

Wenn für einen Normalteiler $N \trianglelefteq G$ die Menge der Linksnebenklassen G/N eine Gruppe ist, dann stellt sich die Frage, ob wir aus der Kenntnis der Untergruppen von G Rückschlüsse auf die Untergruppen von G/N ziehen können. In der Tat gibt es eine natürliche Eins-zu-Eins-Beziehung zwischen den Untergruppen einer Faktorgruppe G/N und den Untergruppen von G, die N enthalten. Entsprechendes gilt für die Normalteiler.

Bemerkung 4.42
Sei $(G,\cdot)$ eine Gruppe und $N \trianglelefteq G$ ein Normalteiler, dann sind die folgenden Abbildungen *bijektiv*:

$$\{U \leq G \mid N \subseteq U\} \longrightarrow \{\overline{U} \mid \overline{U} \leq G/N\} : U \mapsto U/N$$

und

$$\{M \trianglelefteq G \mid N \subseteq M\} \longrightarrow \{\overline{M} \mid \overline{M} \trianglelefteq G/N\} : M \mapsto M/N.$$

Der Nachweis der Aussagen ist einfach und wir überlassen ihn dem Leser als Übung.

Aus Proposition 1.38 wissen wir, daß die Untergruppen von $(\mathbb{Z}, +)$ die Form $m\mathbb{Z}$ für eine nicht-negative Zahl m haben und aus Beispiel 1.30 wissen wir, daß $m\mathbb{Z}$ genau dann in $n\mathbb{Z}$ enthalten ist, wenn n ein Teiler von m ist. Wir erhalten also unmittelbar folgendes Korollar.

Korollar 4.43
Ist $n \in \mathbb{Z}_{>0}$ eine positive ganze Zahl, so gilt

$$\overline{U} \leq \mathbb{Z}_n \quad \Longleftrightarrow \quad \exists\, m \in \{1, \ldots, n\} \text{ mit } m \text{ teilt } n \;:\; \overline{U} = m\mathbb{Z}/n\mathbb{Z} = \langle \overline{m}_n \rangle.$$

Insbesondere ist jede Untergruppe von $\mathbb{Z}_n$ zyklisch.

Beweis: Wegen Bemerkung 4.42 reicht es, die Untergruppen U von $\mathbb{Z}$ zu bestimmen mit $n\mathbb{Z} \subseteq U$. Nach Proposition 1.38 hat eine solche Untergruppe die Form $U = m\mathbb{Z}$ für eine ganze Zahl $m \geq 0$. Die Bedingung $n\mathbb{Z} \subseteq m\mathbb{Z}$ bedingt nach Beispiel 1.30, daß n ein Vielfaches von m ist, d.h. m muß zwischen 1 und n liegen und m ist ein Teiler von n. □

Wir wollen als nächstes die Ordnung eines Elementes $\overline{m} \in \mathbb{Z}_n$ für positive ganze Zahlen m und n bestimmen. Dazu führen wir zunächst folgende Notation ein.

Notation 4.44
Für zwei ganze Zahlen $a, b \in \mathbb{Z}$ sei

$$\operatorname{kgv}(a, b) := \begin{cases} \min\{z > 0 \mid a \text{ und } b \text{ teilen } z\}, & \text{falls } a, b \neq 0, \\ 0, & \text{falls } a = 0 \text{ oder } b = 0. \end{cases}$$

Wir werden später (vgl. Aufgabe 7.11) sehen, daß $\operatorname{kgv}(a, b)$ ein *kleinstes gemeinsames Vielfaches* von a und b im Sinne der Definition 7.4 ist.

Korollar 4.45
Es seien $m, n \in \mathbb{Z}_{>0}$. Dann ist

$$o(\overline{m}) = \frac{\operatorname{kgv}(m, n)}{m}$$

die Ordnung von $\overline{m} \in \mathbb{Z}_n$.

Beweis: Da $(\mathbb{Z}_n, +)$ eine endliche additive Gruppe ist, nimmt der Ausdruck zur Bestimmung der Ordnung von $\overline{m}$ in Bemerkung 4.12 folgende Form an:

$$\begin{aligned}
o(\overline{m}) &= \min\left\{k > 0 \mid k \cdot \overline{m} = \overline{0}\right\} \\
&= \min\left\{k > 0 \mid n \text{ teilt } k \cdot m\right\} \\
&= \frac{m \cdot \min\{k > 0 \mid n \text{ teilt } k \cdot m\}}{m} \\
&= \frac{\min\left\{m \cdot k \mid k > 0, n \text{ teilt } k \cdot m\right\}}{m} \\
&= \frac{\min\left\{l > 0 \mid n \text{ und } m \text{ teilen } l\right\}}{m} \\
&= \frac{\mathrm{kgv}(m, n)}{m}.
\end{aligned}$$

□

Aufgabe 4.46
Beweise Bemerkung 4.42.

Aufgabe 4.47
Bestimme alle Untergruppen von $(\mathbb{Z}_{33}, +)$.

Aufgabe 4.48
Betrachte für $m, n, a, b \in \mathbb{Z}_{>0}$ das Element $\left(\overline{a}_m, \overline{b}_n\right) \in \mathbb{Z}_m \times \mathbb{Z}_n$ in der Gruppe $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$. Die Ordnung dieses Elementes läßt sich wie folgt berechnen

$$o\Big(\left(\overline{a}_m, \overline{b}_n\right)\Big) = \mathrm{kgv}\left(o\left(\overline{a}_m\right), o\left(\overline{b}_n\right)\right) = \mathrm{kgv}\left(\frac{\mathrm{kgv}(a, m)}{a}, \frac{\mathrm{kgv}(b, n)}{b}\right)$$

und ist ein Teiler von $\mathrm{kgv}(m, n)$. Insbesondere ist $\mathbb{Z}_m \times \mathbb{Z}_n$ nicht zyklisch, wenn m und n nicht teilerfremd sind.

Aufgabe 4.49
Berechne die Ordnung von $\left(\overline{6}_{21}, \overline{9}_{33}\right) \in \mathbb{Z}_{21} \times \mathbb{Z}_{33}$.

Aufgabe 4.50
Es sei σ und π zwei disjunkte Zyklen in $\mathbb{S}_n$ der Länge k bzw. l. Zeige, daß $o(\sigma \circ \pi) = \mathrm{kgv}(k, l)$.

D) **Der Homomorphiesatz**

Gibt es einen Gruppenisomorphismus von einer Gruppe G in eine Gruppe H, so sind diese vom Standpunkt der Gruppentheorie nicht mehr wirklich unterscheidbar. Denn jede gruppentheoretische Eigenschaft der einen Gruppe findet sich automatisch auch in der anderen, da der Gruppenisomorphismus die Struktur erhält und bijektiv ist. Will man also eine der Gruppen studieren, so kann man genausogut auch die andere dazu betrachten, je nachdem ob einem die eine Repräsentation besser gefällt oder die andere. In diesem Sinne ist es interessant, Prinzipien kennenzulernen, die es erlauben festzustellen, wann zwei Gruppen isomorph sind und ggf. auch den Isomorphismus angeben zu können. In diesem Kapitel wollen wir die grundlegendste Methode dazu kennenlernen.

Satz 4.51 (Homomorphiesatz)
Ist $\alpha : G \to H$ *ein Gruppenhomomorphismus, dann ist die durch* α *induzierte Abbildung*

$$\widetilde{\alpha} : G/\operatorname{Ker}(\alpha) \to \operatorname{Im}(\alpha) : \overline{g} \mapsto \alpha(g)$$

wohldefiniert[26] *und ein Isomorphismus. Insbesondere gilt also*

$$G/\operatorname{Ker}(\alpha) \cong \operatorname{Im}(\alpha).$$

Beweis: Wir zeigen zunächst, daß $\widetilde{\alpha}$ wohldefiniert ist. Sei dazu $\overline{g} = \overline{h} \in G/\operatorname{Ker}(\alpha)$ gegeben. Dann gilt also $g^{-1}h \in \operatorname{Ker}(\alpha)$ und damit

$$e_H = \alpha\big(g^{-1}h\big) = \alpha\big(g^{-1}\big)\alpha(h) = \big(\alpha(g)\big)^{-1}\alpha(h).$$

Mithin gilt $\alpha(g) = \alpha(h)$, und $\widetilde{\alpha}$ ist somit wohldefiniert.

Für $\overline{g}, \overline{h} \in G/\operatorname{Ker}(\alpha)$ gilt ferner

$$\widetilde{\alpha}\big(\overline{g} \cdot \overline{h}\big) = \widetilde{\alpha}\big(\overline{gh}\big) = \alpha(gh) = \alpha(g)\alpha(h) = \widetilde{\alpha}\big(\overline{g}\big) \cdot \widetilde{\alpha}\big(\overline{h}\big).$$

Also ist $\widetilde{\alpha}$ ein Gruppenhomomorphismus.

$\widetilde{\alpha}$ ist offensichtlich surjektiv. Bleibt also noch zu zeigen, daß $\widetilde{\alpha}$ injektiv ist. Seien dazu $\overline{g}, \overline{h} \in G/\operatorname{Ker}(\alpha)$ mit $\alpha(g) = \widetilde{\alpha}\big(\overline{g}\big) = \widetilde{\alpha}\big(\overline{h}\big) = \alpha(h)$, so gilt

$$e_H = \big(\alpha(g)\big)^{-1}\alpha(h) = \alpha\big(g^{-1}\big)\alpha(h) = \alpha\big(g^{-1}h\big).$$

D. h. $g^{-1}h \in \operatorname{Ker}(\alpha)$, also $\overline{g} = \overline{h}$. Mithin ist $\widetilde{\alpha}$ injektiv. □

Beispiel 4.52
Betrachte die Gruppen $(\mathbb{Z}, +)$ der ganzen Zahlen mit der Addition und $(\mathbb{C} \setminus \{0\}, \cdot)$

[26] Der Begriff *wohldefiniert* meint im Prinzip nur, daß die getroffene Definition überhaupt eine solche ist (siehe auch Definition B.5 und Bemerkung B.6). Doch wo ist das Problem dabei? Die Elemente von $G/\operatorname{Ker}(\alpha)$ sind nach Definition Linksnebenklassen (auch wenn wir uns bemühen wollen, das zu vergessen), und als solche besitzen sie Repräsentanten, die wir wie immer zum Rechnen und so auch zum Definieren von Abbildungen wie oben verwenden wollen. Nur besitzt für gewöhnlich jede Nebenklasse sehr viele Repräsentanten, und in einer Definition wie oben ist es a priori überhaupt nicht klar, daß die oben getroffene Zuordnung $\overline{g} \mapsto \alpha(g)$ nicht von der Wahl des Repräsentanten abhängt. D.h. wenn h ein anderer Repräsentant der gleichen Linksnebenklasse ist, also $\overline{g} = \overline{h}$, ist dann auch $\alpha(g) = \alpha(h)$? Alles andere wäre nicht gut, denn wir haben ja in unserer *Definition* nicht gesagt, welcher Repräsentant von der Linksnebenklasse verwendet werden soll! Für die *Wohldefiniertheit* der Abbildung müssen wir genau diesen Sachverhalt prüfen: $\overline{g} = \overline{h} \implies \alpha(g) = \alpha(h)$, oder bereits mit obiger Notation ausgedrückt

$$\overline{g} = \overline{h} \implies \widetilde{\alpha}(\overline{g}) = \widetilde{\alpha}(\overline{h}).$$

Dies erinnert verdächtig an die Injektivität einer Abbildung, aber Vorsicht, für diese war genau die andere Implikation zu zeigen.

der komplexen Zahlen mit der Multiplikation. Aus der Vorlesung Grundlagen der Mathematik ist bekannt, daß

$$\alpha : \mathbb{Z} \longrightarrow \mathbb{C} \setminus \{0\} : z \mapsto e^{\frac{i \cdot \pi}{2} \cdot z}$$

ein Gruppenhomomorphismus ist, da das Potenzgesetz

$$e^{\frac{i \cdot \pi}{2} \cdot (z+z')} = e^{\frac{i \cdot \pi}{2} \cdot z} \cdot e^{\frac{i \cdot \pi}{2} \cdot z'}$$

gilt. Eine einfache Rechnung zeigt, daß

$$\mathrm{Im}(\alpha) = \{1, -1, i, -i\}$$

und

$$\mathrm{Ker}(\alpha) = 4 \cdot \mathbb{Z},$$

da $e^{\frac{i \cdot \pi}{2} \cdot z} = 1$ genau dann gilt, wenn $\frac{z}{2}$ ein Vielfaches von 2 ist. Aus dem Homomorphiesatz folgt mithin

$$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/\operatorname{Ker}(\alpha) \cong \mathrm{Im}(\alpha) = \{1, -1, i, -i\},$$

wobei die Gruppenoperation auf der linken Seite die Addition und auf der rechten Seite die Multiplikation ist.

Um die *Wohldefiniertheit* der Abbildung $\widetilde{\alpha}$ im Homomorphiesatz an einem Beispiel zu verstehen, sollte man folgendes beachten. In $\mathbb{Z}/4\mathbb{Z}$ sind die Nebenklassen $\overline{2}$ und $\overline{6}$ identisch. Mithin muß für die Abbildung

$$\widetilde{\alpha} : \mathbb{Z}/4\mathbb{Z} \longrightarrow \{1, -1, i, -i\} : \overline{z} \mapsto e^{\frac{i \cdot \pi}{2} \cdot z}$$

auch $\widetilde{\alpha}(\overline{2}) = \widetilde{\alpha(\overline{6})}$ gelten, und aufgrund der Definition von $\widetilde{\alpha}$ bedeutet das, daß notwendig $\alpha(2) = \alpha(6)$ gelten muß. Das tut's, da sich 2 und 6 um 4 unterscheiden und $e^{\frac{i \cdot \pi}{2} \cdot 4} = 1$.

Bemerkung 4.53
Betrachten wir für $n \geq 2$ wieder den surjektiven Gruppenhomomorphismus (vgl. Bemerkung 3.20)

$$\mathrm{sgn} : \mathbb{S}_n \longrightarrow \{-1, 1\}.$$

Aus dem Homomorphiesatz 4.51 folgt insbesondere $|\mathbb{S}_n/\mathbb{A}_n| = |\{-1, 1\}| = 2$. Da nach dem Satz von Lagrange 4.10 zudem $|\mathbb{S}_n/\mathbb{A}_n| = \frac{|\mathbb{S}_n|}{|\mathbb{A}_n|}$ gilt, erhalten wir mit Proposition 3.11 die folgende Gleichung:

$$|\mathbb{A}_n| = \frac{n!}{2}.$$

Die beiden folgenden Isomorphiesätze sind leichte Anwendungen des obigen Homomorphiesatzes.

Satz 4.54 (1. Isomorphiesatz)
Ist G *eine Gruppe,* $U \leq G$ *und* $N \trianglelefteq G$*. Dann ist*

$$U/U \cap N \cong UN/N.$$

Beweis: Wir überlassen den Beweis dem Leser als Übungsaufgabe.

□

Satz 4.55 (2. Isomorphiesatz)
Es seien G *eine Gruppe,* $M \subseteq N \subseteq G$ *zwei Normalteiler von* G*. Dann ist auch* N/M *ein Normalteiler von* G/M *und es gilt*

$$(G/M)/(N/M) \cong G/N.$$

Beweis: Wir betrachten nun folgende Abbildung

$$\beta : G/M \to G/N : gM \mapsto gN,$$

und zeigen, sie ist ein Epimorphismus mit Kern N/M. Damit haben wir dann insbesondere gezeigt, daß N/M ein Normalteiler von G/M ist.[27]

Da β mittels des Repräsentanten einer Linksnebenklasse definiert ist, müssen wir zunächst wieder die Wohldefiniertheit zeigen.

***Schritt 0*:** β ist wohldefiniert.

Seien also $g, h \in G$ zwei Repräsentanten der gleichen Linksnebenklasse von M in G, d.h. $gM = hM$. Dann gilt nach Definition

$$g^{-1}h \in M \subseteq N,$$

so daß auch $gN = hN$. Die Abbildung ist also wohldefiniert.

***Schritt 1*:** β ist ein Homomorphismus.

Seien $gM, g'M \in G/M$, dann gilt

$$\beta\big(gM \cdot g'M\big) = \beta\big(gg'M\big) = gg'N = gN \cdot g'N = \beta(gM) \cdot \beta\big(g'M\big).$$

***Schritt 2*:** β ist surjektiv.

Sei $gN \in G/N$, dann ist $gN = \beta(gM) \in \mathrm{Im}(\beta)$, so daß β surjektiv ist.

***Schritt 3*:** $\mathrm{Ker}(\beta) = N/M$.

$$gM \in \mathrm{Ker}(\beta) \;\Leftrightarrow\; gN = N \;\Leftrightarrow\; g \in N \;\Leftrightarrow\; gM \in N/M.$$

Die Behauptung folgt also wieder mittels des Homomorphiesatzes:

$$(G/M)/(N/M) = (G/M)/\mathrm{Ker}(\beta) \cong \mathrm{Im}(\beta) = G/N.$$

□

Aufgabe 4.56
Beweise Satz 4.54

[27]Beachte, daß M offenbar ein Normalteiler von N ist und somit der Quotient N/M auch tatsächlich definiert und identisch mit der Menge der Linksnebenklassen von M in G der Form nM mit $n \in N$ ist.

Mit Hilfe des Homomorphiesatzes und des Satze von Lagrange kann man folgende Aufgabe lösen.

Aufgabe 4.57
Es seien $(G, \cdot)$ und $(H, *)$ zwei endliche Gruppen teilerfremder Ordnung. Zeige, es gibt genau einen Gruppenhomomorphismus $\alpha : G \longrightarrow H$.

Aufgabe 4.58
Es sei $(G, \cdot)$ eine Gruppe. Zeige:

a. Sind $g, h \in G$ mit $o(g) = o(h) = p$, wobei p eine Primzahl ist, dann gilt $\langle g \rangle = \langle h \rangle$ oder $\langle g \rangle \cap \langle h \rangle = \{e\}$.

b. Falls $|G| = 10$, so gibt es zwei Elemente $g, h \in G$ mit:
- $o(g) = 2$,
- $o(h) = 5$,
- $\langle h \rangle \trianglelefteq G$,
- $\langle g \rangle \cdot \langle h \rangle = G$.

Hinweis, führe in Teil b. zunächst die folgenden beiden folgenden Möglichkeiten zum Widerspruch: 1. $o(k) = 2$ für alle $e \neq k \in G$, 2. $o(k) = 5$ für alle $e \neq k \in G$.

Eine Gruppe G wie in Aufgabe 4.58 b. nennt man das semidirekte Produkt von $\langle g \rangle$ und $\langle h \rangle$. Man kann zeigen, falls $g \cdot h = h \cdot g$, so ist G isomorph zu $\mathbb{Z}_{10}$, andernfalls ist G isomorph zu $\mathbb{D}_{10}$.

Aufgabe 4.59
Bestimme alle Gruppenhomomorphismen $\alpha : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_n$ mit $n \in \{6, 13\}$.

E) Zyklische Gruppen

Wir wollen das Kapitel mit der Klassifikation zyklischer Gruppen abschließen.

Satz 4.60
Es sei $G = \langle g \rangle$ *eine zyklische Gruppe.*

a. *Ist* $|G| = \infty$*, so haben wir den Gruppenisomorphismus*

$$\alpha : \mathbb{Z} \xrightarrow{\cong} G : z \mapsto g^z.$$

b. *Ist* $|G| = n < \infty$*, so haben wir den Gruppenisomorphismus*

$$\overline{\alpha} : \mathbb{Z}_n \xrightarrow{\cong} G : \overline{z} \mapsto g^z.$$

Beweis: Für die Abbildung

$$\alpha : \mathbb{Z} \xrightarrow{\cong} G : z \mapsto g^z$$

und zwei ganze Zahlen $x, y \in \mathbb{Z}$ gilt

$$\alpha(x + y) = g^{x+y} = g^x \cdot g^y = \alpha(x) \cdot \alpha(y).$$

α ist also ein Gruppenhomomorphismus, und es gilt

$$\mathrm{Im}(\alpha) = \{g^z \mid z \in \mathbb{Z}\} = \langle g \rangle = G,$$

d.h. α ist surjektiv.

Ist $|G| = o(g) = \infty$, so ist

$$\{0\} = \{z \in \mathbb{Z} \mid g^z = e\} = \mathrm{Ker}(\alpha)$$

nach Bemerkung 4.12, d.h. α ist in diesem Fall auch injektiv.

Ist $|G| = o(g) = n < \infty$, so ist nach Aufgabe 1.55

$$\mathrm{Ker}(\alpha) = \{z \in \mathbb{Z} \mid g^z = e\} = n\mathbb{Z}.$$

Aus dem Homomorphiesatz folgt mithin, daß die Abbildung $\overline{\alpha}$ ein Gruppenisomorphismus ist. □

Die Klassifikation zyklischer Gruppen kann nun genutzt werden, um aus der Ordnung eines Elementes g die Ordnung all seiner Potenzen abzuleiten.

Korollar 4.61
Ist $(G, \cdot)$ *eine Gruppe,* $g \in G$ *mit* $o(g) < \infty$ *und* $0 \neq m \in \mathbb{Z}$. *Dann gilt*

$$o\big(g^m\big) = \frac{\mathrm{kgv}\,\big(m, o(g)\big)}{|m|}.$$

Beweis: Es sei $n = o(g)$, dann ist

$$\overline{\alpha} : \mathbb{Z}_n \longrightarrow \langle g \rangle : \overline{z} \mapsto g^z$$

nach Satz 4.60 ein Gruppenisomorphismus. Aus Aufgabe 1.61 folgt dann

$$o\big(g^m\big) = o\Big(\overline{\alpha}(\overline{m})\Big) = o\big(\overline{m}\big).$$

Ist $m > 0$, so folgt die Behauptung aus Korollar 4.45. Ist $m < 0$, so ist $-m > 0$ und es folgt analog

$$o\big(g^{-m}\big) = \frac{\mathrm{kgv}(-m, n)}{-m} = \frac{\mathrm{kgv}(m, n)}{|m|}.$$

Da zudem die Ordnung eines Elementes und seines Inversen übereinstimmen, folgt die Behauptung auch im Fall $m < 0$. □

Korollar 4.62
Ist $G = \langle g \rangle$ *eine zyklische Gruppe der Ordnung* $|G| = n < \infty$, *dann gilt*

$$U \leq G \quad \Longleftrightarrow \quad \exists\, m \in \{1, \ldots, n\} \textit{ mit } m \textit{ teilt } n \;:\; U = \big\langle g^m \big\rangle.$$

Für eine solche Untergruppe gilt zudem

$$\big|\big\langle g^m \big\rangle\big| = \frac{n}{m}.$$

Insbesondere hat G *für jeden Teiler von* n *genau eine Untergruppe dieser Ordnung.*

Beweis: Nach Satz 4.60 ist die Abbildung

$$\overline{\alpha} : \mathbb{Z}_n \longrightarrow G : \overline{z} \mapsto g^z$$

ein Gruppenisomorphismus, so daß die erste Aussage aus Korollar 4.43 folgt. Die Aussage zur Ordnung erhalten wir aus Korollar 4.61, da $\mathrm{kgv}(m, n) = n$. Schließlich beachte man noch, daß mit m auch $\frac{n}{m}$ alle Teiler von n durchläuft. □

Da die Untergruppen von $\mathbb{Z}$ zyklisch sind nach Proposition 1.38 erhalten wir mit Satz 4.60 und Korollar 4.43 folgende Aussage.

Korollar 4.63
Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Aufgabe 4.64
Ist $(G, \cdot)$ eine Gruppe und $p = |G|$ eine Primzahl, so ist G isomorph zu $(\mathbb{Z}_p, +)$.

Aufgabe 4.65
Es sei $(G, \cdot)$ eine Gruppe, $g \in G$ und $n \in \mathbb{Z}_{>0}$. Zeige, genau dann gibt es einen Gruppenhomomorphismus $\alpha : \mathbb{Z}_n \longrightarrow G$ mit $\alpha\big(\overline{1}\big) = g$, wenn die Ordnung von g ein Teiler von n ist.

Aufgabe 4.66
Bestimme alle Automorphismen der Gruppe $(\mathbb{Z}_{10}, +)$.

5 Prüfzifferkodierung

In der Einleitung haben wir uns mit **EAN-13** Strichcodes beschäftigt, und dabei festgehalten, daß die ersten 12 Ziffern eines solchen Codes das Produkt, das ihn trägt, identifizieren. Welche Ziffern dabei welche Bedeutung haben, ist für unsere Belange nicht wichtig. Denn uns geht es letztlich nur darum, daß die 13. Ziffer des Codes nicht der Identifikation des Produktes, sondern der Absicherung des Codes gegen falsches Einscannen oder Abschreiben dient, und ob dieses sinnvoll gemacht wurde. Man nennt diese zusätzliche Ziffer auch *Prüfziffer*. Es ist ganz offensichtlich,

5 901234 123457

Abbildung 2. Ein EAN-13 Strichcode

daß eine einzige zusätzliche Ziffer nicht ausreichen kann, um alle möglichen Fehler zu erkennen. Wenn man also ein *sinnvolles* Verfahren sucht, dann ist zunächst eine Analyse der häufigsten Fehler nötig, die beim Einscannen oder Abschreiben eines Codes auftreten. Das haben glücklicherweise bereits andere für uns erledigt, und eine solche Analyse zeigt, daß etwa 90% der Fehler in folgende beiden Kategorien fallen:

Typ I: "Einzelfehler" – d.h. nur eine einzelne Ziffer ist falsch erkannt. Das sind etwa 80% der auftretenden Fehler.

Typ II: "Nachbartransposition" – d.h. zwei benachbarte Ziffern sind vertauscht. Das sind etwa 10% der auftretenden Fehler.

Alle übrigen Fehlertypen, lagen bei weniger als 1%. Aufgrund dieser Analyse sollte eine gute Prüfziffer auf alle Fälle erkennen, wenn eine einzige Ziffer unter den ersten zwölfen falsch ist, und ihr sollte optimalerweise auch noch die Vertauschung zweier benachbarter Ziffern auffallen.

Die Ziffern, die in einem Strichcode verwendet werden, sind auf den ersten Blick Elemente der Menge

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\},$$

aber der geübte Teilnehmer der Vorlesung Algebraische Strukturen erkennt sofort, daß eine bloße *Menge* viel zu wenig Struktur hat, um damit etwas anfangen zu können, und daß man die 10 Ziffern doch viel besser als Elemente der Menge

$$\mathbb{Z}_{10} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\right\}$$

auffassen sollte. Auf diese Weise haben wir auf der Menge unserer Ziffern, die wir von jetzt an unser *Alphabet* nennen wollen, eine zusätzliche Struktur, nämlich eine

Addition bezüglich derer das Alphabet eine Gruppe ist. Diese Addition kann man ausnutzen, um die Prüfziffer mittels einer *möglichst guten* Formel aus den übrigen Ziffern zu errechnen.

Auf das konkrete Beispiel des **EAN-13** Strichcodes kommen wir später zurück. Zunächst wollen wir den Ansatz allgemeiner betrachten und für den allgemeineren Ansatz die Eigenschaften bezüglich der Fehlererkennung analysieren. Danach können wir dann schauen, ob die tatsächliche Kodierung des **EAN-13** den notwendigen Anforderungen genügt, und falls nicht, wie man ihn verbessern könnte. Die Grundidee des allgemeineren Ansatzes ist, statt $\mathbb{Z}_{10}$ eine beliebige Gruppe als Alphabet zuzulassen. Dann sollte man aber vielleicht nicht mehr von den Ziffern des Codes sprechen, sondern eher von den *Buchstaben* des Codes.

Als erste Idee für ein Verfahren zur Berechnung der Prüfziffer über $\mathbb{Z}_{10}$ könnte die *Quersumme* der ersten 12 Ziffern in $\mathbb{Z}_{10}$ dienen. Ein solches Verfahren würde aber ganz sicher keine Nachbartranspositionen erkennen, da die Gruppenoperation kommutativ ist. Diesem Mangel kann man begegnen, indem man die Elemente noch ein wenig abändert, d.h. *permutiert*, bevor man sie addiert. Dieser Gedanke führt zu folgender Definition.

Definition 5.1
Es sei $(G, \cdot)$ eine Gruppe, $g_0 \in G$ fest gegeben, und $\pi_1, \ldots, \pi_n \in \mathrm{Sym}(G)$ seien Permutationen von G.

a. Wir nennen

$$C = C_G(\pi_1, \ldots, \pi_n, g_0) = \big\{(g_1, \ldots, g_n) \in G^n \;\big|\; \pi_1(g_1) \cdots \pi_n(g_n) = g_0\big\}$$

einen *Prüfziffercode* der *Länge* n auf dem *Alphabet* G.

b. Wir sagen, daß $C = C_G(\pi_1, \ldots, \pi_n, g_0)$ *Fehler vom Typ I erkennt*, falls für alle $(g_1, \ldots, g_n) \in C$ und $g_i' \in G$ mit $g_i' \neq g_i$ gilt $(g_1, \ldots, g_{i-1}, g_i', g_{i+1}, \ldots, g_n) \notin C$.

c. Wir sagen, daß $C = C_G(\pi_1, \ldots, \pi_n, g_0)$ *Fehler vom Typ II erkennt*, falls für alle $(g_1, \ldots, g_n) \in C$ und $i \in \{1, \ldots, n-1\}$ mit $g_i \neq g_{i+1}$ gilt $(g_1, \ldots, g_{i-1}, g_{i+1}, g_i, g_{i+2}, \ldots, g_n) \notin C$.

Wir wollen nun zunächst zeigen, daß der **EAN-13** Strichcode in dieses Schema paßt.

Beispiel 5.2 (EAN-13)
Wir überlassen es dem Leser, zu zeigen, daß die Abbildung

$$\mu_3 : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_{10} : \overline{k} \mapsto 3 \cdot \overline{k} = \overline{k} + \overline{k} + \overline{k}$$

eine Permutation von $\mathbb{Z}_{10}$ ist, d.h. daß sie bijektiv ist. Man kann diese Aussage leicht verifizieren, indem man die Bilder der 10 Elemente von $\mathbb{Z}_{10}$ ausrechnet. Sie folgt allerdings auch leicht aus der Tatsache, daß die Zahlen 10 und 3 teilerfremd sind, wie wir später sehen werden.

Wir betrachten nun die Situation $(G,\cdot) = (\mathbb{Z}_{10},+)$, $g_0 = \overline{0}$, $n = 13$, $\pi_i = \mathrm{id}_{\mathbb{Z}_{10}}$ falls i ungerade ist und $\pi_i = \mu_3$ falls i gerade ist. Dann ist

$$C = C_{\mathbb{Z}_{10}}\big(\pi_1,\pi_2,\ldots,\pi_{13},\overline{0}\big)$$

der Prüfziffercode, der zu **EAN-13** gehört.

Wie läßt sich damit die 13. Ziffer aus den ersten zwölfen bestimmen? Nach Voraussetzung gilt für ein zulässiges Codewort $z_1z_2\ldots z_{12}z_{13} \in C$:

$$\overline{z_1} + 3\cdot\overline{z_2} + \overline{z_3} + \ldots + 3\cdot\overline{z_{12}} + \overline{z_{13}} = \overline{0},$$

und mithin

$$\overline{z_{13}} = -\overline{z_1} - 3\cdot\overline{z_2} - \overline{z_3}\ldots - 3\cdot\overline{z_{12}}.$$

Will man also z_{13} ermitteln, so führt man die Rechnung auf der rechten Seite des Gleichheitszeichens in $\mathbb{Z}_{10}$ durch, wählt den eindeutig bestimmten Repräsentanten $z_{13} \in \{0,1,\ldots,9\}$ der Linksnebenklasse in $\mathbb{Z}_{10}$ die man erhält.

Man kann das Verfahren auch ohne Gruppen beschreiben als: "*man berechne die abwechselnd mit* 1 *und* 3 *gewichtete Quersumme der ersten zwölf Ziffern, nenne* x *die letzte Ziffer dieser Quersumme und wähle die letzte Ziffer von* $10-x$ *als* z_{13}.". Aber die Fehlererkennungseigenschaften lassen sich mit der Gruppennotation leichter analysieren.

Betrachten wir ganz konkret das Beispiel in Figur 2, d.h. die ersten zwölf Ziffern sind 590123412345, so daß die Prüfziffer $z_{13} = 7$ sich ergibt aus

$$-\overline{5} - 3\cdot\overline{9} - \overline{0} - 3\cdot\overline{1} - \overline{2} - 3\cdot\overline{3} - \overline{4} - 3\cdot\overline{1} - \overline{2} - 3\cdot\overline{3} - \overline{4} - 3\cdot\overline{5} = \overline{-83} = \overline{7},$$

bzw. alternativ, daß sich $(5,9,0,1,2,3,4,1,2,3,4,5,7) \in C$ ergibt aus:

$$\overline{5} + 3\cdot\overline{9} + \overline{0} + 3\cdot\overline{1} + \overline{2} + 3\cdot\overline{3} + \overline{4} + 3\cdot\overline{1} + \overline{2} + 3\cdot\overline{3} + \overline{4} + 3\cdot\overline{5} + \overline{7} = \overline{0}.$$

Man beachte im Übrigen, daß $C = \mathrm{Ker}(\alpha)$ der Kern des folgenden Gruppenhomomorphismus ist,

$$\alpha : \mathbb{Z}_{10}^{13} \longrightarrow \mathbb{Z}_{10} : (z_1,\ldots,z_{13}) \mapsto z_1 + 3z_2 + z_3 + \ldots + 3z_{12} + z_{13},$$

wobei $\mathbb{Z}_{10}^{13}$ eine Gruppe bezüglich komponentenweiser Addition ist. □

Nachdem wir nun Prüfzifferkodierungen über beliebigen Gruppen eingeführt haben, sollten wir deren Fehlererkennungseigenschaften untersuchen.

Proposition 5.3 (Fehlererkennungseigenschaft)
Es sei G *eine Gruppe und* $C = C_G(\pi_1,\ldots,\pi_n,g_0)$ *ein Prüfziffercode über dem Alphabet* G.

a. C *erkennt Fehler vom Typ I.*

b. *Für* $n \geq 3$ *erkennt* C *Fehler vom Typ II genau dann, wenn*

$$g\cdot\big(\pi_{i+1}\circ\pi_i^{-1}\big)(h) \neq h\cdot\big(\pi_{i+1}\circ\pi_i^{-1}\big)(g) \tag{28}$$

für alle $i = 1,\ldots,n-1$ *und für alle* $g,h \in G$ *mit* $g \neq h$.

Beweis: a. Sei $(g_1, \ldots, g_n) \in C$ und $g_i' \in G$ mit $g_i' \neq g_i$. Angenommen $(g_1, \ldots, g_i', \ldots, g_n) \in C$, dann gilt

$$\pi_1(g_1) \cdots \pi_n(g_n) = g_0 = \pi_1(g_1) \cdots \pi_i\big(g_i'\big) \cdots \pi_n(g_n).$$

Wenden wir die Kürzungsregel auf beiden Seiten der Gleichung mehrfach an, so erhalten wir

$$\pi_i(g_i) = \pi_i\big(g_i'\big).$$

Da nach Voraussetzung π_i eine Permutation, also insbesondere injektiv ist, folgt $g_i = g_i'$ im Widerspruch zur Voraussetzung. Mithin ist $(g_1, \ldots, g_i', \ldots, g_n) \notin C$, und C erkennt Fehler vom Typ I.

b. Gehen wir zunächst davon aus, daß die Bedingung (28) erfüllt ist, und schließen daraus, daß C Fehler vom Typ II erkennt. Sei dafür $(g_1, \ldots, g_n) \in C$ gegeben mit $g_i \neq g_{i+1}$ für ein $1 \leq i \leq n-1$. Wir setzen $g = \pi_i(g_i)$ und $h = \pi_i(g_{i+1})$. Da π_i injektiv ist, gilt $g \neq h$. Aus (28) folgt damit:

$$\pi_i(g_i) \cdot \pi_{i+1}(g_{i+1}) = g \cdot \big(\pi_{i+1} \circ \pi_i^{-1}\big)(h) \neq h \cdot \big(\pi_{i+1} \circ \pi_i^{-1}\big)(g) = \pi_i(g_{i+1}) \cdot \pi_{i+1}(g_i).$$

Multiplizieren wir beide Seiten mit jeweils den gleichen Elementen aus G von links bzw. von rechts, so bleibt die Gleichheit erhalten. Auf dem Wege gilt also:

$$\pi_1(g_1) \cdots \pi_i(g_i) \cdot \pi_{i+1}(g_{i+1}) \cdots \pi_n(g_n) \neq \pi_1(g_1) \cdots \pi_i(g_{i+1}) \cdot \pi_{i+1}(g_i) \cdots \pi_n(g_n).$$

Das bedeutet aber, daß C Fehler vom Typ II erkennt.

Gehen wir nun umgekehrt davon aus, daß C Fehler vom Typ II erkennt, und zeigen, daß dann die Bedingung (28) erfüllt ist. Dazu seien $g, h \in G$ mit $g \neq h$ gegeben. Wir setzen $g_i = \pi_i^{-1}(g)$ und $g_{i+1} = \pi_i^{-1}(h)$. Da π_i bijektiv ist, folgt aus $g \neq h$, daß auch $g_i \neq g_{i+1}$. Wir wählen nun $g_j \in G$, $j \neq i, i+1$ so, daß $(g_1, \ldots, g_n) \in C$ – beachte, daß wir hier $n \geq 3$ benötigen. Nach Voraussetzung gilt dann aber

$$(g_1, \ldots, g_{i+1}, g_i, \ldots, g_n) \notin C,$$

und mithin

$$\pi_1(g_1) \cdots \pi_n(g_n) = g_0 \neq \pi_1(g_1) \cdots \pi_i(g_{i+1}) \cdot \pi_{i+1}(g_i) \cdots \pi_n(g_n).$$

Wir können nun wieder die Kürzungsregel auf beiden Seiten der Gleichung mehrfach anwenden und erhalten:

$$g \cdot \big(\pi_{i+1} \circ \pi_i^{-1}\big)(h) = \pi_i(g_i) \cdot \pi_{i+1}(g_{i+1}) \neq \pi_i(g_{i+1}) \cdot \pi_{i+1}(g_i) = h \cdot \big(\pi_{i+1} \circ \pi_i^{-1}\big)(g).$$

Damit ist die Aussage bewiesen.

□

Beispiel 5.4

Aus Proposition 5.3 folgt, daß **EAN-13** alle Fehler vom Typ I erkennt. Wie sieht es mit Fehlern vom Typ II aus? Wir erinnern uns, daß $\pi_1 = \mathrm{id}_{\mathbb{Z}_{10}}$ und $\pi_2 = \mu_3$, die Multiplikation mit 3, ist. Mithin gilt für $g = \overline{0} \neq \overline{5} = h$

$$g + \left(\pi_2 \circ \pi_1^{-1}\right)(h) = \overline{0} + 3 \cdot \overline{5} = \overline{5} = \overline{5} + 3 \cdot \overline{0} = h + \left(\pi_2 \circ \pi_1^{-1}\right)(g).$$

Damit folgt aber aus Proposition 5.3, daß **EAN-13** nicht alle Fehler vom Typ II erkennt.

Natürlich stellt sich die Frage, welche Nachbarvertauschungen von **EAN-13** erkannt werden, und welche nicht. Eine kurze Überlegung führt zu folgender Erkenntnis: Sind $z, z' \in \{0, 1, 2, \ldots, 9\}$ zwei Ziffern, so daß $|z - z'| = 5$ gilt, dann gilt

$$2 \cdot (z - z') \equiv 0 \pmod{10} \tag{29}$$

und mithin

$$\overline{z} + 3 \cdot \overline{z'} = \overline{z'} + 3 \cdot \overline{z}. \tag{30}$$

Gilt umgekehrt (30), so gilt auch (29) und damit $|z - z'| = 5$.

Folglich erkennt **EAN-13** genau dann die Vertauschung zweier verschiedener benachbarter Ziffern nicht, wenn diese sich um 5 unterscheiden. Beim Beispiel in Figur 2 würden also auch Fehler vom Typ II erkannt. □

Proposition 5.3 hilft uns bei der Entscheidung, ob ein Prüfziffercode *alle* Fehler vom Typ II erkennt, ist dies nicht der Fall, so sagt sie aber nichts darüber aus, ob *sehr viele* solcher Fehler nicht erkannt werden, oder sehr wenige. Im Fall von **EAN-13** haben wir durch eine Zusatzüberlegung gesehen, daß vergleichsweise wenig Fehler vom Typ II übersehen werden. Könnte man die Qualität von **EAN-13** durch die Wahl anderer Gewichte, d.h. anderer Permutationen, verbessern, so daß *alle* Fehler vom Typ II erkannt werden? Dazu wollen wir zunächst einmal festhalten, daß die Gruppe $(\mathbb{Z}_{10}, +)$ abelsch ist, und daß sich für eine *abelsche* Gruppe $(G, \cdot)$ die Gleichung (28) schreiben läßt als

$$g \cdot \left(\mathrm{inv} \circ \pi_{i+1} \circ \pi_i^{-1}\right)(g) \neq h \cdot \left(\mathrm{inv} \circ \pi_{i+1} \circ \pi_i^{-1}\right)(h), \tag{31}$$

wobei

$$\mathrm{inv} : G \to G : g \mapsto g^{-1}$$

die Inversionsabbildung ist. Da inv bijektiv ist, ist $\mathrm{inv} \circ \pi_{i+1} \circ \pi_i^{-1} \in \mathrm{Sym}(G)$ eine Permutation von G. Betrachtet man nun (31), so scheint wegen Proposition 5.3 die Erkennung von Fehlern des Typs II mit Abbildungen der Form

$$g \mapsto g \cdot \pi(g)$$

zusammenzuhängen, wobei $\pi \in \mathrm{Sym}(G)$. Wir wollen diesen deshalb einen Namen geben.

Definition 5.5
Ist G eine Gruppe und $\pi \in \mathrm{Sym}(G)$ eine Permutation von G, so nennen wir π eine *vollständige Abbildung* wenn die Abbildung

$$\pi^* : G \to G : g \mapsto g \cdot \pi(g)$$

bijektiv ist.

Bislang konnten wir nur für einen gegebenen Prüfziffercode entscheiden, ob er Fehler vom Typ II erkennt oder nicht. Die folgende Proposition gibt uns nun ein Kriterium, anhand dessen wir für *abelsche* Gruppen entscheiden können, ob es mit ihnen als Alphabet überhaupt eine Prüfzifferkodierung geben *kann*, die alle Fehler vom Typ II erkennt. Der Beweis ist *konstruktiv* in dem Sinn, daß es reicht eine *vollständige Abbildung* auf der Gruppe zu kennen, um eine solche Prüfzifferkodierung hinschreiben zu können.

Korollar 5.6
Es sei G *eine endliche* abelsche *Gruppe und* $n \geq 3$. *Genau dann gibt es auf* G *einen Prüfziffercode der Länge* n, *der Fehler vom Typ II erkennt, wenn es auf* G *eine vollständige Abbildung gibt.*

Beweis: Wir setzen zunächst voraus, daß es auf G eine vollständige Abbildung $\pi \in \mathrm{Sym}(G)$ gibt. Definieren wir $g_0 = e_G$ und $\pi_i = (\mathrm{inv} \circ \pi)^i$ für $i = 1, \ldots, n$, dann wollen wir zeigen, daß $C = C_G(\pi_1, \ldots, \pi_n, g_0)$ Fehler vom Typ II erkennt.

Dazu müssen wir nur überprüfen, ob die Gleichung (31) erfüllt ist. Seien $g, h \in G$ mit $g \neq h$ gegeben, dann gilt

$$\begin{aligned} g \cdot \big(\mathrm{inv} \circ \pi_{i+1} \circ \pi_i^{-1}\big)(g) &= g \cdot \big(\mathrm{inv} \circ (\mathrm{inv} \circ \pi)^{i+1-i}\big)(g) = g \cdot \pi(g) = \pi^*(g) \\ &\neq \pi^*(h) = h \cdot \pi(h) = h \cdot \big(\mathrm{inv} \circ (\mathrm{inv} \circ \pi)^{i+1-i}\big)(h) = h \cdot \big(\mathrm{inv} \circ \pi_{i+1} \circ \pi_i^{-1}\big)(h). \end{aligned}$$

Mithin ist die Gleichung (31) erfüllt und C erkennt Fehler vom Typ II.

Setzen wir nun umgekehrt voraus, daß es auf G einen Prüfziffercode $C_G(\pi_1, \ldots, \pi_n, g_0)$ gibt, der Fehler vom Typ II erkennt. Es reicht zu zeigen, daß $\pi = \mathrm{inv} \circ \pi_2 \circ \pi_1^{-1} \in \mathrm{Sym}(G)$ eine vollständige Abbildung ist. Seien dazu $g, h \in G$ mit $g \neq h$. Aufgrund von Gleichung (31) gilt

$$\pi^*(g) = g \cdot \pi(g) = g \cdot \big(\mathrm{inv} \circ \pi_2 \circ \pi_1^{-1}\big)(g) \neq h \cdot \big(\mathrm{inv} \circ \pi_2 \circ \pi_1^{-1}\big)(h) = h \cdot \pi(h) = \pi^*(h).$$

Mithin ist π^* injektiv und damit auch bijektiv, da G endlich ist. Also ist π eine vollständige Abbildung. □

Bemerkung 5.7

a. Wenn $|G| = 2 \cdot m$ mit m ungerade, dann gibt es *keine* vollständige Abbildung auf G.[28] Insbesondere gibt es auf $\mathbb{Z}_{10}$ also keinen Prüfziffercode, der alle Fehler vom Typ II erkennt.

b. Wenn $|G|$ ungerade ist, dann ist die Identität id_G eine vollständige Abbildung.

c. **Problem:** Es gibt keinen Prüfziffercode auf $(\mathbb{Z}_{10}, +)$, der alle Fehler vom Typ II erkennt. Wie können wir diesem Problem begegnen, wenn wir es nicht einfach hinnehmen wollen?

[28] Der Beweis ist elementar, aber etwas länglich. Wir verweisen den Leser deshalb auf [Sie81].

Lösung 1: Man verwende eine ungerade Anzahl an Ziffern, d.h. man ersetze $\mathbb{Z}_{10}$ durch $\mathbb{Z}_m$ für ein ungerade Zahl m.

Diese Methode wendete z.B. der ISBN-Code bis 2007 an. Er arbeitete mit $(\mathbb{Z}_{11},+)$ als Alphabet und die *Ziffer* $\overline{10} = 10 + 11\mathbb{Z}$ wurde in einem ISBN-Code mit X bezeichnet. Dabei tauchte das X in den tatsächlich auf Büchern verwendeten ISBN-Nummern nur als Prüfziffer auf. Der ISBN-Code war der Prüfziffercode

$$C_{\mathbb{Z}_{11}}\big(\pi_1, \ldots, \pi_{10}, \overline{0}\big),$$

wobei

$$\pi_i : \mathbb{Z}_{11} \to \mathbb{Z}_{11} : \overline{a} \mapsto (11 - i) \cdot \overline{a}.$$

Wir überlassen es dem Leser zu überprüfen, daß der Code tatsächlich Fehler vom Typ II erkennt. Es reicht zu zeigen, daß die Gleichung (31) erfüllt ist.

Lösung 2: Man verwende eine *nicht-abelsche* Gruppe mit zehn Elementen. Für diese gibt die Nicht-Existenz einer vollständigen Abbildung keinerlei Hinweis auf die Fehlererkennungseigenschaft von Prüfziffercodes.

Beispiel 5.8 (Seriennummern deutscher Währung)
Die Prüfziffer der Seriennummern der DM-Scheine waren kodiert mittels

$$C_{\mathbb{D}_{10}}\big(\pi^1, \ldots, \pi^{10}, \mathrm{id}_{\mathbb{D}_{10}}, (1)\big),$$

wobei

$$\mathbb{D}_{10} = \big\langle (1\ 2\ 3\ 4\ 5), (1\ 5)(2\ 4) \big\rangle \leq \mathbb{S}_5 = \mathrm{Sym}\big(\{1, \ldots, 5\}\big)$$

die *Diëdergruppe* der Ordnung 10 ist und die Permutation π weiter unten definiert wird. Wir schreiben hier das neutrale Element der $\mathbb{D}_{10}$ als Einszyklus (1) und nicht als $\mathrm{id}_{\{1,\ldots,5\}}$, um Verwechslungen mit der Permutation $\mathrm{id}_{\mathbb{D}_{10}}$ vorzubeugen.

Wie für die Gruppe $\mathbb{D}_8$ zeigt man, daß mit $\sigma = (1\ 2\ 3\ 4\ 5)$ und $\tau = (1\ 5)(2\ 4)$ die Gruppe $\mathbb{D}_{10}$ geschrieben werden kann als

$$\mathbb{D}_{10} = \big\{\sigma^0 = (1), \sigma^1, \ldots, \sigma^4, \tau \circ \sigma^0 = \tau, \tau \circ \sigma^1, \ldots, \tau \circ \sigma^4\big\}.$$

Die Gruppe ist nicht abelsch, da $\tau \circ \sigma = \sigma^{-1} \circ \tau \neq \sigma \circ \tau$.

Verhoeff hat in [Ver75] gezeigt, daß die Permutation $\pi : \mathbb{D}_{10} \to \mathbb{D}_{10}$ mit

x	σ^0	σ^1	σ^2	σ^3	σ^4	$\tau\circ\sigma^0$	$\tau\circ\sigma^1$	$\tau\circ\sigma^2$	$\tau\circ\sigma^3$	$\tau\circ\sigma^4$
$\pi(x)$	σ^1	$\tau\circ\sigma^0$	$\tau\circ\sigma^2$	$\tau\circ\sigma^1$	σ^2	$\tau\circ\sigma^3$	σ^3	σ^0	$\tau\circ\sigma^4$	σ^4

folgende Eigenschaft hat:

$$g \circ \pi(h) \neq h \circ \pi(g) \quad \text{für alle } g, h \in \mathbb{D}_{10} \text{ mit } g \neq h.$$

Aus Proposition 5.3 folgt dann, daß $C_{\mathbb{D}_{10}}\big(\pi^1, \ldots, \pi^{10}, \mathrm{id}_{\mathbb{D}_{10}}, (1)\big)$ Fehler vom Typ II erkennt.

Natürlich hat man bei den Seriennummern der DM-Scheine keine Symbole wie σ verwendet. Stattdessen wurden die 10 Ziffern sowie zusätzlich 10 Buchstaben verwendet, die dann vermittels folgender Tabelle mit den Elementen der $\mathbb{D}_{10}$ identifiziert wurden:

σ^0	σ^1	σ^2	σ^3	σ^4	$\tau\circ\sigma^0$	$\tau\circ\sigma^1$	$\tau\circ\sigma^2$	$\tau\circ\sigma^3$	$\tau\circ\sigma^4$
0	1	2	3	4	5	6	7	8	9
A	D	G	K	L	N	S	U	Y	Z.

Wollte man überprüfen, ob eine Seriennummer zulässig ist, mußte man die Ziffern und Buchstaben durch die entsprechenden Elemente der $\mathbb{D}_{10}$ ersetzen und nachrechnen, ob das Ergebnis in der Menge $C_{\mathbb{D}_{10}}\big(\pi^1,\ldots,\pi^{10},\mathrm{id}_{\mathbb{D}_{10}},(1)\big)$ liegt.

Aufgabe 5.9
Überprüfe ob $AA6186305Z2$ eine zulässige Seriennummer für einen DM-Schein ist.

Bemerkung 5.10
Hätte man noch eine andere Gruppe mit 10 Elementen als Alphabet verwenden können?

Nicht wirklich! Für das Alphabet kommt es nur auf den Isomorphietyp der Gruppe an, und jede Gruppe der Ordnung 10 ist entweder isomorph zu $(\mathbb{Z}_{10},+)$ oder zu $(\mathbb{D}_{10},\circ)$. Der Beweis dieser Aussage ist mit den Mitteln, die wir bislang zur Verfügung haben, etwas länglich, aber durchaus machbar.

Aufgabe 5.11
Beweise Teil b. von Bemerkung 5.7.

6 Ringe und Körper

A) Ringe und Körper

In Kapitel 1 haben wir die mathematische Struktur der *Gruppe* eingeführt, und unsere ersten Beispiele waren die additiven Gruppen $(\mathbb{Z},+)$ und $(\mathbb{Q},+)$ der ganzen bzw. der rationalen Zahlen. Auf diesen Mengen haben wir aber neben der Addition jeweils noch eine zweite zweistellige Operation, die Multiplikation, bezüglich derer in beiden Mengen wiederum interessante Rechenregeln gelten. So ist die Menge $(\mathbb{Q}\setminus\{0\},\cdot)$ wieder eine Gruppe, während $(\mathbb{Z}\setminus\{0\},\cdot)$ zu dieser Eigenschaft (nur) die multiplikativen Inversen fehlen. Wir wollen diese Beispiele nun verallgemeinern und führen dazu folgende Definition ein.

Definition 6.1

a. Ein *Ring mit Eins* ist ein Tripel $(R,+,\cdot)$ bestehend aus einer Menge R zusammen mit zwei zweistelligen Operationen

$$+ : R\times R\to R : (a,b)\mapsto a+b, \qquad (\text{“}\textit{Addition}\text{”})$$

und

$$\cdot : R\times R\to R : (a,b)\mapsto a\cdot b, \qquad (\text{“}\textit{Multiplikation}\text{”})$$

so, daß folgende Axiome erfüllt sind:

(i) $(R,+)$ ist eine abelsche Gruppe (mit neutralem Element 0_R).

(ii) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ für alle $a,b,c\in R$. (“*Assoziativität der Multiplikation*”)

(iii) Es gibt ein Element $1_R\in R$ mit $1_R\cdot a=a\cdot 1_R=a$ für alle $a\in R$. (“*Einselement*”)

(iv) $a\cdot(b+c)=a\cdot b+a\cdot c$ und $(b+c)\cdot a=b\cdot a+c\cdot a$ für alle $a,b,c\in R$. (“*Distributivität*”)

b. Ein Ring mit Eins $(R,+,\cdot)$ heißt *kommutativ*, falls $a\cdot b=b\cdot a$ für alle $a,b\in R$.

c. Ist $(R,+,\cdot)$ ein Ring mit Eins, dann heißt $a\in R$ eine *Einheit* oder *invertierbar* in R, falls es ein $a'\in R$ gibt mit $a\cdot a'=a'\cdot a=1_R$. Wir bezeichnen mit

$$R^* = \{a\in R \mid a \text{ ist Einheit}\}$$

die Menge der Einheiten von R.

d. Ein kommutativer Ring mit Eins $(R,+,\cdot)$ heißt *Körper*, falls $1_R\in R^*=R\setminus\{0\}$.

Bemerkung 6.2

Wir werden in Ringen für die Addition stets das Zeichen $+$ und für die Multiplikation das Zeichen $\cdot$ verwenden, auch wenn wir gleichzeitig verschiedene Ringe betrachten. Wir verzichten im Folgenden deshalb darauf, die Ringoperationen jeweils anzugeben und nennen verkürzend die dem Ring $(R,+,\cdot)$ zugrunde liegende Menge R einen Ring. Zudem werden wir statt $a\cdot b$ oft auch nur ab schreiben.

Das neutrale Element von $(R, +)$ werden wir mit 0_R oder einfach mit 0 bezeichnen und das *Nullelement* von R nennen; das Einselement bezeichnen wir mit 1_R oder 1.

Ist R ein Ring und sind $a, b \in R$, so schreiben wir statt $a + (-b)$ auch kurz $a - b$.

Das Einselement in R ist eindeutig bestimmt, denn wenn $1_R, 1'_R \in R$ zwei Elemente mit der Eigenschaft des Einselementes sind, dann folgt $1_R = 1_R \cdot 1'_R = 1'_R$.

Ist $a \in R$ eine Einheit und $a', a'' \in R$ mit $a \cdot a' = a' \cdot a = 1_R$ und $a \cdot a'' = a'' \cdot a = 1_R$, so gilt

$$a' = 1_R \cdot a' = (a'' \cdot a) \cdot a' = a'' \cdot (a \cdot a') = a'' \cdot 1_R = a''.$$

Das Inverse a' zu a ist also eindeutig bestimmt und wird mit a^{-1} oder $\frac{1}{a}$ bezeichnet.

Beachte, aus der Definition folgt unmittelbar, daß $(R^*, \cdot)$ eine Gruppe ist, die sogenannte *Einheitengruppe* des Ringes R.

Unter Beachtung der Rechenregeln 6.5 kann man leicht zeigen, daß eine Tripel $(K, +, \cdot)$ genau dann ein *Körper* ist, wenn gilt:

a. $(K, +)$ ist eine abelsche Gruppe.

b. $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

c. Für alle $a, b, c \in K$ gilt $a \cdot (b + c) = a \cdot b + a \cdot c$.

$\square$

Beispiel 6.3

a. $(\mathbb{Z}, +, \cdot)$ mit der üblichen Addition und Multiplikation ist ein kommutativer Ring mit Eins, der kein Körper ist.

b. $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ mit der üblichen Addition und Multiplikation sind Körper.

c. In der Vorlesung Grundlagen der Mathematik wurden auf der Menge $\mathbb{C} = \{(x, y) \mid x, y \in \mathbb{R}\}$ die beiden zweistelligen Operationen

$$+ : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} : \big((x, y), (x', y')\big) \mapsto (x + x', y + y')$$

und

$$\cdot : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} : \big((x, y), (x', y')\big) \mapsto (x \cdot x' - y \cdot y', x \cdot y' + x' \cdot y)$$

eingeführt, und es wurde gezeigt, daß $(\mathbb{C}, +, \cdot)$ ein Körper ist – *Körper der komplexen Zahlen* Für die Elemente von $\mathbb{C}$ hat sich die Schreibweise $(x, y) = x + iy$ mit $i^2 = -1$ eingebürgert. Wir werden im weiteren Verlauf der Vorlesung die komplexen Zahlen und ihre Eigenschaften so, wie sie in der Vorlesung Grundlagen der Mathematik gezeigt wurden, als bekannt voraussetzen. Der Vollständigkeit halber haben wir die wichtigsten Eigenschaften im Anhang zusammengetragen.

d. Ist M eine beliebige Menge und $(R, +, \cdot)$ ein Ring mit Eins, so ist

$$R^M := \{f \mid f : M \to R \text{ ist eine Abbildung}\}$$

mit den punktweise definierten Operationen

$$+ : R^M \times R^M \to R^M : (f, g) \mapsto \big(f + g : M \to R : x \mapsto f(x) + g(x)\big),$$

und

$$\cdot : R^M \times R^M \to R^M : (f, g) \mapsto \big(f \cdot g : M \to R : x \mapsto f(x) \cdot g(x)\big),$$

ein Ring mit der Nullfunktion $0 : M \to R : x \mapsto 0_R$ als neutralem Element der Addition und der Einsfunktion $1 : M \to R : x \mapsto 1_R$ als Einselement, wie man mit etwas Fleiß nachprüft.

e. In Aufgabe 1.21 haben wir die Menge

$$\mathrm{Mat}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R} \right\}$$

der reellen 2×2-Matrizen eingeführt und für zwei Matrizen

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R})$$

ihr Produkt als

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a \cdot a' + b \cdot c' & a \cdot b' + b \cdot d' \\ c \cdot a' + d \cdot c' & c \cdot b' + d \cdot d' \end{pmatrix}$$

definiert. Setzen wir zudem

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix},$$

so rechnet man mit etwas Geduld nach, daß $(\mathrm{Mat}_2(\mathbb{R}), +, \cdot)$ ein Ring mit Einselement

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ist. Dieser Ring ist nicht-kommutativ, da

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

In der Vorlesung Grundlagen der Mathematik wird dieses Beispiel verallgemeinert auf Matrizen der Größe $n \times n$ für $n \geq 1$ über einem beliebigen Körper K, und der Nachweis, daß auf diesem Wege ein nicht-kommutativer Ring mit Eins entsteht, wird dort auf weit geschickterem Weg als durch langatmiges Nachrechnen geführt.

Beispiel 6.4
Es seien $(R,+,\cdot)$ und $(S,+,\cdot)$ zwei kommutative Ringe mit Eins. Dann wird das kartesische Produkt $R \times S$ durch die komponentenweisen Operationen

$$(r,s)+(r',s') := (r+r', s+s')$$

und

$$(r,s)\cdot(r',s') := (r\cdot r', s\cdot s')$$

zu einem kommuativen Ring mit Eins $(1_R, 1_S)$. Das Nachrechnen der Axiome ist eine einfache Anwendung der Definition.

Für die Einheiten in $R \times S$ gilt

$$(R\times S)^* = R^* \times S^*,$$

da

$$(1_R, 1_S) = (r,s)\cdot(r',s') = (r\cdot r', s\cdot s') \iff 1_R = r\cdot r' \text{ und } 1_S = s\cdot s'.$$

Auf die gleiche Weise wird das kartesische Produkt von einer beliebigen Anzahl kommutativer Ringe mit Eins wieder ein kommutativer Ring mit Eins, und die Einheiten des kartesischen Produktes sind wieder durch das kartesische Produkt der Einheitengruppen gegeben.

Wir wollen nun einige Rechenregeln für das Rechnen in Ringen aufstellen.

Lemma 6.5 (Rechenregeln)
Es sei R ein Ring mit Eins. Für $a, b, c \in R$ gelten:

a. $-(-a) = a$.

b. $a + b = c \Leftrightarrow a = c - b$.

c. $-(a+b) = -a - b$.

d. $0 \cdot a = a \cdot 0 = 0$.

e. $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$.

f. $(-a)\cdot(-b) = a\cdot b$.

g. $a\cdot(b-c) = a\cdot b - a\cdot c$.

h. *Für $a \in R^*$ ist $a^{-1} \in R^*$ und $\left(a^{-1}\right)^{-1} = a$.*

i. *Ist $1_R = 0_R$, so ist $R = \{0_R\}$ der* Nullring.

Beweis: Die Aussagen a., b. und c. folgen unmittelbar aus Lemma 1.6.

d. Für $a \in R$ gilt $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$, also folgt $0\cdot a = 0$ mittels der Kürzungsregeln in $(R,+)$. Analog sieht man $a\cdot 0 = 0$.

e. Für $a, b \in R$ gilt wegen d.:

$$a\cdot b + (-a)\cdot b = (a-a)\cdot b = 0\cdot b = 0,$$

also $-(a \cdot b) = (-a) \cdot b$. Die Gleichheit des Ausdrucks zu $a \cdot (-b)$ folgt analog.

f. Für $a, b \in R$ folgt unter Zuhilfenahme von a. und e.:

$$(-a) \cdot (-b) = -\big(a \cdot (-b)\big) = -\big(-(a \cdot b)\big) = a \cdot b.$$

g. Für $a, b, c \in R$ impliziert e.:

$$a \cdot (b - c) = a \cdot b + a \cdot (-c) = a \cdot b + \big(-(a \cdot c)\big) = a \cdot b - a \cdot c.$$

h. Ist $a \in R^*$ eine Einheit mit Inversem a^{-1}. Dann ist nach Definition a ein Inverses von a^{-1}, und insbesondere ist a^{-1} eine Einheit. Aus der Eindeutigkeit des Inversen (siehe Bemerkung 6.2) folgt dann, daß $a = (a^{-1})^{-1}$.

i. Ist $a \in R$, so gilt $a = 1_R \cdot a = 0_R \cdot a = 0_R$.

$\square$

Eine wichtige Klasse kommutativer Ringe mit Eins stellen die sogenannten formalen Potenzreihenringe dar, die wir in folgenden Definition einführen wollen.

Definition 6.6

Sei R ein kommutativer Ring mit Eins. Ist $a_k \in R$ für $k \in \mathbb{N}$, so bezeichnen wir die Funktion

$$\mathbb{N} \longrightarrow R : k \mapsto a_k$$

durch den Ausdruck $\sum_{k=0}^{\infty} a_k \cdot t^k$, so daß

$$R[[t]] := \left\{ \sum_{k=0}^{\infty} b_k \cdot t^k \;\middle|\; b_k \in R \right\}$$

die Menge aller Funktionen von $\mathbb{N}$ nach R bezeichnet. Wir nennen die Elemente von $R[[t]]$ *formale Potenzreihen*, und $R[[t]]$ heißt der *Ring der formalen Potenzreihen* über R in der Unbestimmten t.

Für zwei formale Potenzreihen $\sum_{i=0}^{\infty} a_i \cdot t^i, \sum_{j=0}^{\infty} b_j \cdot t^j \in R[[t]]$ definieren wir ferner

$$\sum_{i=0}^{\infty} a_i \cdot t^i \;+\; \sum_{i=0}^{\infty} b_i \cdot t^i \;:=\; \sum_{i=0}^{\infty} (a_i + b_i) \cdot t^i \in R[[t]]$$

und

$$\sum_{i=0}^{\infty} a_i \cdot t^i \;\cdot\; \sum_{j=0}^{\infty} b_j \cdot t^j \;:=\; \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \cdot b_j \right) \cdot t^k \in R[[t]].$$

Man beachte, daß aus der Definition unmittelbar folgt, daß

$$\sum_{i=0}^{\infty} a_i \cdot t^i \;=\; \sum_{i=0}^{\infty} b_i \cdot t^i \quad\Longleftrightarrow\quad a_i = b_i \;\forall\, i \in \mathbb{N}.$$

Gilt $a_i = 0$ für $i \geq n$, so schreiben wir auch abkürzend

$$\sum_{i=0}^{n} a_i \cdot t^i = \sum_{i=0}^{\infty} a_i \cdot t^i.$$

Bemerkung 6.7
Die Definition der Multiplikation in $R[[t]]$ entspringt dem Bedürfnis, eine Art verallgemeinertes Distributivgesetz für diese *unendlichen Summen* zu haben:

$$\left(\sum_{i=0}^{\infty} a_i \cdot t^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j \cdot t^j\right) = \sum_{i=0}^{\infty} \left(a_i \cdot t^i \cdot \left(\sum_{j=0}^{\infty} b_j \cdot t^j\right)\right) =$$

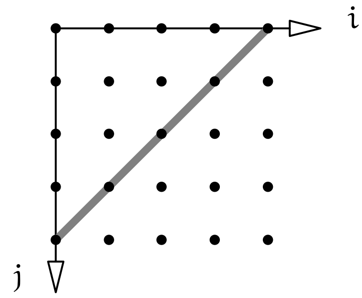
$$\sum_{i=0}^{\infty} \left(\left(\sum_{j=0}^{\infty} a_i \cdot t^i \cdot b_j \cdot t^j\right)\right) = \sum_{i=0}^{\infty} \left(\left(\sum_{j=0}^{\infty} a_i \cdot b_j \cdot t^{i+j}\right)\right). \quad (32)$$

Wenn die eben durchgeführten Operationen in $R[[t]]$ korrekt sind, d.h. wenn alle Gleichungen korrekt sind, dann ist unsere Notation der Elemente von $R[[t]]$ als unendliche Summen eine nützliche Notation. Der Ausdruck auf der rechten Seite in (32) ist in der angegebenen Form aber noch nicht als formale Potenzreihe, d.h. als Element von $R[[t]]$, erkennbar. Viele der t^{i+j} stimmen für verschiedene Werte von i und j überein; z.B. kann man t^2 durch $(i,j) = (2,0)$ und $(i,j) = (1,1)$ und $(i,j) = (0,2)$ erhalten. Der Koeffizient zu t^2 der Potenzreihe in (32) sollte also die Summe der $a_i \cdot b_j$ für diese (i,j) sein, d.h. $a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2$.

Gibt es eigentlich für jedes k nur endlich viele Paare (i,j), so daß $i + j = k$? Ja! Denn wir setzen für i und j ja voraus, daß es nicht-negative ganze Zahlen sind. Da mit der Vorgabe von k und durch die Wahl von i die Zahl j bereits als $j = k - i$ festgelegt ist und da i und j zwischen 0 und k liegen müssen, damit sowohl i als auch j nicht-negativ sind, gibt es genau die folgenden $k+1$ Möglichkeiten:

$$(k,0),\ \ (k-1,1),\ \ (k-2,2),\ \ \dots\ \ ,\ \ (1,k-1),\ \ (0,k).$$

Am deutlichsten kann man sich die Paare (i,j), deren Summe ein festes k ergibt, verdeutlichen, indem man sie als Punkte in ein Koordinatensystem mit den Achsen i und j einträgt:



Genau die Paare (i,j) auf der Diagonalen von $(k,0)$ nach $(0,k)$ haben die Eigenschaft, daß die Summe $i+j$ den Wert k ergibt. Der Koeffizient zu t^k in der rechten Seite von (32) muß deshalb

$$\sum_{i+j=k} a_i \cdot b_j = \sum_{i=0}^{k} a_i \cdot b_{k-i}$$

sein. Man spricht wegen der angegebenen graphischen Darstellung auch vom *Cantorschen Diagonalverfahren* der Multiplikation zweier Potenzreihen.

Satz 6.8
Ist R *ein kommutativer Ring mit Eins, so ist der formale Potenzreihenring* $(R[[t]], +, \cdot)$ *ein kommutativer Ring mit Eins* $1_{R[[t]]} = t^0$.

Beweis: Nach Definition sind $+$ und $\cdot$ zwei zweistellige Operationen auf $R[[t]]$. Seien also $\sum_{i=0}^{\infty} a_i \cdot t^i, \sum_{i=0}^{\infty} b_i \cdot t^i, \sum_{i=0}^{\infty} c_i \cdot t^i \in R[[t]]$ gegeben. Dann gilt wegen der Assoziativität der Addition in R

$$\left(\sum_{i=0}^{\infty} a_i \cdot t^i + \sum_{i=0}^{\infty} b_i \cdot t^i\right) + \sum_{i=0}^{\infty} c_i \cdot t^i = \sum_{i=0}^{\infty} \big((a_i + b_i) + c_i\big) \cdot t^i$$
$$= \sum_{i=0}^{\infty} \big(a_i + (b_i + c_i)\big) \cdot t^i = \sum_{i=0}^{\infty} a_i \cdot t^i + \left(\sum_{i=0}^{\infty} b_i \cdot t^i + \sum_{i=0}^{\infty} c_i \cdot t^i\right)$$

und wegen der Kommutativität der Addition in R

$$\sum_{i=0}^{\infty} a_i \cdot t^i + \sum_{i=0}^{\infty} b_i \cdot t^i = \sum_{i=0}^{\infty} (a_i + b_i) \cdot t^i$$
$$= \sum_{i=0}^{\infty} (b_i + a_i) \cdot t^i = \sum_{i=0}^{\infty} b_i \cdot t^i + \sum_{i=0}^{\infty} a_i \cdot t^i.$$

Zudem gilt für die Nullfunktion $0_{R[[t]]} = \sum_{i=0}^{\infty} 0 \cdot t^i$

$$0_{R[[t]]} + \sum_{i=0}^{\infty} a_i \cdot t^i = \sum_{i=0}^{\infty} (0 + a_i) \cdot t^i = \sum_{i=0}^{\infty} a_i \cdot t^i,$$

und für $\sum_{i=0}^{\infty} (-a_i) \cdot t^i \in R[[t]]$ gilt

$$\sum_{i=0}^{\infty} (-a_i) \cdot t^i + \sum_{i=0}^{\infty} a_i \cdot t^i = \sum_{i=0}^{\infty} (-a_i + a_i) \cdot t^i = 0_{R[[t]]},$$

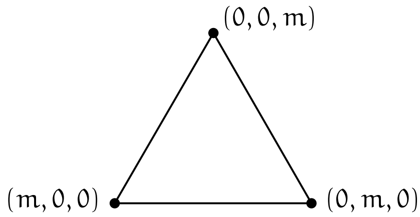
so daß $(R[[t]], +)$ eine abelsche Gruppe mit der Nullfunktion als neutralem Element ist.

Man beachte nun, daß

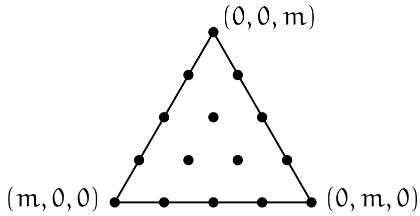
$$\sum_{k+l=m} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot c_l = \sum_{i+j+l=m} a_i \cdot b_j \cdot c_l = \sum_{i+k=m} \left(a_i \cdot \sum_{j+l=k} b_j \cdot c_l\right), \qquad (33)$$

da unter jeder der Summen jedes der Tripel (i, j, l) natürlicher Zahlen mit der Eigenschaft $i + j + l = m$ genau einmal vor kommt[29] und da in R das Assoziativgesetz

[29] Man kann sich dies auch geometrisch veranschaulichen. Fassen wir (i, j, l) als Koordinaten des dreidimensionalen Raumes $\mathbb{R}^3$ auf, so bestimmt die Gleichung $i + j + l = m$ bei vorgegebenem m eine Ebene im Raum, nämlich die Ebene, die durch die drei Punkte $(m, 0, 0)$, $(0, m, 0)$ und $(0, 0, m)$ aufgespannt wird. Verbinden wir diese drei Punkte in dieser Ebene, so erhalten wir ein Dreieck:



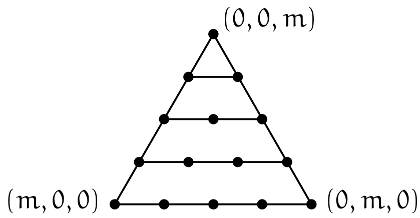
Die Punkte mit ganzzahligen Koordinaten in diesem Dreieck sind genau die Tripel nicht-negativer ganzer Zahlen, deren Summe m ist:



In der linken Seite von (33) zerlegen wir diese Menge wie folgt:

$$\bigcup_{l=0}^{m} \bigcup_{i+j=m-l} \{(i, j, l)\}.$$

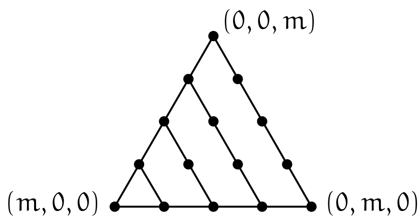
In der inneren Summe werden also diejenigen ganzzahligen (i, j, l) in dem Dreieck zusammen gefaßt, für die die Koordinate l konstant ist und für die $i + j = m - l$ ist, d.h. die Punkte liegen auf einer Geraden parallel zur Geraden durch $(m, 0, 0)$ und $(0, m, 0)$:



In der rechten Seite von (33) zerlegen wir diese Menge wie folgt:

$$\bigcup_{i=0}^{m} \bigcup_{j+l=m-i} \{(i, j, l)\}.$$

In der inneren Summe werden also diejenigen ganzzahligen (i, j, l) in dem Dreieck zusammen gefaßt, für die die Koordinate i konstant ist und für die $j + l = m - i$ ist, d.h. die Punkte liegen auf einer Geraden parallel zur Geraden durch $(0, m, 0)$ und $(0, 0, m)$:



In beiden Fällen wird jedes ganzzahlige Tripel (i, j, l) im Dreieck genau einmal betrachtet.

der Multiplikation und das Distributivgesetz gelten. Damit gilt aber

$$\begin{aligned}
\left(\sum_{i=0}^{\infty} a_i \cdot t^i \ \cdot \ \sum_{j=0}^{\infty} b_j \cdot t^j\right) \ \cdot \ \sum_{l=0}^{\infty} c_l \cdot t^l &= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot t^k \ \cdot \ \sum_{l=0}^{\infty} c_l \cdot t^l \\
&= \sum_{m=0}^{\infty} \left(\sum_{k+l=m} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot c_l\right) \cdot t^m \\
&= \sum_{m=0}^{\infty} \left(\sum_{i+k=m} a_i \cdot \sum_{j+l=k} b_j \cdot c_l\right) \cdot t^m \\
&= \sum_{i=0}^{\infty} a_i \cdot t^i \ \cdot \ \sum_{k=0}^{\infty} \left(\sum_{j+l=k} b_j \cdot c_l\right) \cdot t^k \\
&= \sum_{i=0}^{\infty} a_i \cdot t^i \ \cdot \ \left(\sum_{j=0}^{\infty} b_j \cdot t^j \ \cdot \ \sum_{l=0}^{\infty} c_l \cdot t^l\right),
\end{aligned}$$

so daß die Multiplikation auf $R[[t]]$ assoziativ ist. Ferner folgt aus der Kommutativität der Multiplikation auf R unmittelbar

$$\begin{aligned}
\sum_{i=0}^{\infty} a_i \cdot t^i \ \cdot \ \sum_{j=0}^{\infty} b_j \cdot t^j &= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot t^k \\
&= \sum_{k=0}^{\infty} \left(\sum_{j+i=k} b_j \cdot a_i\right) \cdot t^k = \sum_{j=0}^{\infty} b_j \cdot t^j \ \cdot \ \sum_{i=0}^{\infty} a_i \cdot t^i.
\end{aligned}$$

Und schließlich gilt für $1_{R[[t]]} = t^0 = \sum_{j=0}^{\infty} e_j \cdot t^j$ mit $e_0 = 1$ und $e_j = 0$ für $j \geq 1$:

$$1_{R[[t]]} \cdot \sum_{i=0}^{\infty} a_i \cdot t^i = \sum_{k=0}^{\infty} \left(\sum_{j+i=k} e_j \cdot a_i\right) \cdot t^k = \sum_{k=0}^{\infty} a_k \cdot t^k,$$

so daß t^0 unter Ausnutzung der Kommutativität der Multiplikation das Einselement von $R[[t]]$ ist.

Es bleibt nur, die Distributivität zu zeigen:

$$\begin{aligned}
\sum_{i=0}^{\infty} a_i \cdot t^i \cdot \ \left(\sum_{j=0}^{\infty} b_j \cdot t^j \ + \ \sum_{j=0}^{\infty} c_j \cdot t^j\right) &= \sum_{i=0}^{\infty} a_i \cdot t^i \ \cdot \ \sum_{j=0}^{\infty} (b_j + c_j) \cdot t^j \\
&= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \cdot (b_j + c_j)\right) \cdot t^k \\
&= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} (a_i \cdot b_j + a_i \cdot c_j)\right) \cdot t^k \\
&= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot t^k + \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \cdot c_j\right) \cdot t^k \\
&= \sum_{i=0}^{\infty} a_i \cdot t^i \ \cdot \ \sum_{j=0}^{\infty} b_j \cdot t^j \ + \ \sum_{i=0}^{\infty} a_i \cdot t^i \ \cdot \ \sum_{j=0}^{\infty} c_j \cdot t^j.
\end{aligned}$$

Das zweite Distributivgesetz folgt mittels der Kommutativität der Multiplikation.

Damit haben wir gezeigt, daß $(R[[t]], +, \cdot)$ ein kommutativer Ring mit Eins ist. □

Bemerkung 6.9
Die Definition der formalen Potenzreihen bereitet Studienanfängern für gewöhnlich einige Probleme. In der Analysis lernt man Potenzreihen als Funktionen eines Intervalls $(a-\varepsilon, a+\varepsilon)$ in die reellen Zahlen kennen, indem man die Unbestimmte t durch eine reelle Zahl aus dem Intervall $(a-\varepsilon, a+\varepsilon)$ ersetzt. Der Ausdruck $\sum_{k=0}^{\infty} a_k \cdot t^k$ stellt in der Analysis mithin eine Funktionsvorschrift dar, bei der t variabel ist. Damit das Einsetzen von Werten für t zu einem sinnvollen Ergebnis führen kann, benötigt man den Begriff der Konvergenz von Folgen und Reihen reeller Zahlen. Diesen Begriff wollen und können wir nicht so ohne weiteres auf andere Ringe oder Körper verallgemeinern, so daß wir uns davor hüten müssen, eine Potenzreihe als Funktionvorschrift aufzufassen, bei der für t irgendwelche Werte eingesetzt werden!

Dennoch haben wir Potenzreihen als Funktionen eingeführt, als Funktionen von $\mathbb{N}$ in den Ring R, über dem wir die Potenzreihen betrachten. Will man eine solche Funktion f beschreiben, so kann man dies durch eine Wertetabelle tun:

k	0	1	2	3	$\ldots$
$f(k)$	a_0	a_1	a_2	a_3	$\ldots$

Die Potenzreihe $\sum_{k=0}^{\infty} a_k \cdot t^k$ ist letztlich nichts anderes als eine kompakte Schreibweise für diese Wertetabelle. Die Spalte

3
a_3

wird dabei ersetzt durch den Ausdruck $a_3 \cdot t^3$, und der Zusatz $\cdot t^3$ dient dazu festzuhalten, daß es sich um die vierte Spalte der Wertetabelle handelt. Und statt die Spalten der Tabelle durch senkrechte Balken zu trennen, verbindet man sie mit Summenzeichen:

$$a_0 \cdot t^0 + a_1 \cdot t^1 + a_2 \cdot t^2 + a_3 \cdot t^3 + \ldots .$$

Ist also $f = \sum_{k=0}^{\infty} a_k \cdot t^k \in R[[t]]$ eine Potenzreihe, so ist $f(k) = a_k$ nach Definition.

Weshalb wählt man nun diese Schreibweise?

Wir haben oben eine Addition und eine Multiplikation von Potenzreihen, d.h. von Funktionen von $\mathbb{N}$ nach R, eingeführt. Diese lassen sich mit Hilfe der neuen Schreibweise auf angenehme Weise ausdrücken. Mehr steckt nicht dahinter.

Um im Potenzreihenring rechnen zu können, reicht es, die Rechenregeln aus Definition 6.6 zu kennen. Dabei kann man $f = \sum_{k=0}^{\infty} a_k \cdot t^k$ als einen formalen Ausdruck ohne tiefere Bedeutung betrachten, den man nach den vorgegebenen Regeln manipulieren kann. Man kann dabei getrost vergessen, daß f eine Funktion repräsentiert, solange man die Regeln kennt. □

Aufgabe 6.10
Es sei R ein kommutativer Ring mit Eins und $f = \sum_{k=0}^{\infty} a_k \cdot t^k \in R[[t]]$ eine formale Potenzreihe über R. Zeige, f ist genau dann eine Einheit in $R[[t]]$, wenn a_0 eine Einheit in R ist.

Hinweis, wenn a_0 eine Einheit in R ist, so ist eine Reihe $g = \sum_{k=0}^{\infty} b_k \cdot t^k$ mit $f \cdot g = t^0$ gesucht. Multipliziere die linke Seite der Gleichung aus und löse die Gleichungen, die sich für die Koeffizienten ergeben rekursiv.

B) **Unterringe**

Definition 6.11
Sei R ein Ring mit Eins und $S \subseteq R$. S heißt ein *Unterring* von R, wenn

a. $1_R \in S$,

b. $a + b \in S$ für alle $a, b \in S$,

c. $-a \in S$ für alle $a \in S$, und

d. $a \cdot b \in S$ für alle $a, b \in S$.

Ist R ein Körper und S ein Unterring von R für den zusätzlich $a^{-1} \in S$ für alle $a \in S \setminus \{0\}$ gilt, so nennen wir S auch einen *Unterkörper* oder *Teilkörper* von R.

Man beachte, daß ein Unterring S von R insbesondere selbst wieder Ring ist bezüglich der Einschränkung der Addition und Multiplikation von R auf S, und daß entsprechend ein Teilkörper selbst ein Körper ist.

Beispiel 6.12
$\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$. $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$ und $\mathbb{C}$. $\mathbb{R}$ ist ein Teilkörper von $\mathbb{C}$.

Das neben den ganzen Zahlen wichtigste Beispiel eines kommutativen Ringes mit Eins in dieser Vorlesung ist der Polynomring, den wir als Unterring des formalen Potenzreihenringes erhalten.

Definition 6.13
Ist R ein kommutativer Ring, so nennen wir

$$\begin{aligned} R[t] &:= \left\{ \sum_{k=0}^{\infty} a_k \cdot t^k \in R[[t]] \;\middle|\; \text{nur endlich viele } a_k \text{ sind ungleich null} \right\} \\ &= \left\{ \sum_{k=0}^{n} a_k \cdot t^k \in R[[t]] \;\middle|\; n \in \mathbb{N}, a_0, \ldots, a_n \in R \right\} \end{aligned}$$

den *Polynomring* über R in der Unbestimmten t und die Elemente von $R[t]$ heißen *Polynome*. Für $0 \neq f = \sum_{k=0}^{\infty} a_k \cdot t^k \in R[t]$ nennen wir

$$\deg(f) = \max\{k \mid a_k \neq 0\}$$

den *Grad* des *Polynoms* f und $\mathrm{lc}(f) := a_{\deg(f)}$ seinen *Leitkoeffizienten*. Ferner setzen wir $\deg(0) = -\infty$ und $\mathrm{lc}(0) := 0$.

Beachte, daß aufgrund der in Definition 6.6 getroffenen Konvention jedes Polynom in $R[t]$ die Form

$$\sum_{k=0}^{n} a_k \cdot t^k$$

für ein $n \in \mathbb{N}$ hat.

Beispiel 6.14
$3 \cdot t^4 - t^2 + 5 \cdot t^0 \in \mathbb{Z}[t]$ ist ein Polynom vom Grad $\deg(f) = 4$ und mit Leitkoeffizient $\mathrm{lc}(f) = 3$.

Da $R[t]$ abgeschlossen ist bezüglich Addition, Negativen und Multiplikation und da $1_{R[[t]]} = t^0 \in R[t]$ erhalten wir folgenden Satz.

Satz 6.15
Ist R ein kommutativer Ring mit Eins, so ist $R[t]$ ein Unterring von $R[[t]]$. Insbesondere ist $R[t]$ selbst ein kommutativer Ring mit Eins.

Beweis: Seien $f = \sum_{k=0}^{m} a_k \cdot t^k, g = \sum_{k=0}^{n} b_k \cdot t^k \in R[t]$ gegeben (wobei zugelassen ist, daß alle a_k oder b_k Null sind), so ist

$$f + g = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) \cdot t^k \in R[t], \tag{34}$$

$$-f = \sum_{k=0}^{m} (-a_k) \cdot t^k \in R[t]$$

und

$$f \cdot g = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) \cdot t^k \in R[t], \tag{35}$$

wobei wir die Konvention verwenden, daß $a_k = 0$ für $k > m$ und $b_k = 0$ für $k > n$. Um zu sehen, daß in (35) keine Terme vom Grad größer als $n+m$ nötig sind, beachte man einfach, daß der Koeffizient von t^k für $k > n + m$ die Form

$$\sum_{i=0}^{m} a_i \cdot b_{k-i} + \sum_{i=m+1}^{k} a_i \cdot b_{k-i}$$

hat. Die zweite Summe ist Null, da alle a_i dort Null sind, während die erste Summe Null ist, da dort alle b_{k-i} Null sind. $\square$

Die folgenden Gradformeln für Polynome ergeben sich unmittelbar aus dem obigen Beweis. Dabei verwenden wir die Konvention $m + -\infty = -\infty$ und $\max\{m, -\infty\} = m$ für alle $m \in \mathbb{N} \cup \{-\infty\}$.

Proposition 6.16 (Gradformeln)
Es sei R ein kommutativer Ring mit Eins und $f, g \in R[t]$ seien zwei Polynome. Dann gelten:

a. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.

b. $\deg(f \cdot g) \leq \deg(f) + \deg(g)$.

c. $\deg(f \cdot g) = \deg(f) + \deg(g)$ *genau dann, wenn* $\mathrm{lc}(f) \cdot \mathrm{lc}(g) \neq 0$.
In diesem Fall gilt auch $\mathrm{lc}(f \cdot g) = \mathrm{lc}(f) \cdot \mathrm{lc}(g)$.

Beweis: Ist $f = 0$ oder $g = 0$, so sind die Aussagen offenbar korrekt und wir können deshalb $f \neq 0 \neq g$ annehmen. Dann folgt a. unmittelbar aus (34) und b. aus (35). Für c. beachte man, daß in (35) der Koeffizient von t^{m+n} gerade $a_m \cdot b_n = \mathrm{lc}(f) \cdot \mathrm{lc}(g)$ ist. □

Aufgabe 6.17 a. Es sei R ein kommutativer Ring mit Eins und $S \subset R$ ein nichtleere Teilmenge für die gilt:

- $x + y \in S$ für alle $x, y \in S$,
- $-x \in S$ für alle $x \in S$,
- $x \cdot y \in S$ für alle $x, y \in S$ und
- $1_R \in S$.

Zeige, S ist ein kommutativer Ring mit Eins bezüglich der Einschränkung der Addition und der Multiplikation von R auf S.

b. Zeige, $\mathbb{Z}[i] := \{a + i \cdot b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ ist ein kommutativer Ring mit Eins, wobei die Addition und die Multiplikation einfach die Addition und Multiplikation komplexer Zahlen sein sollen. Man nennt diesen Ring den *Ring der ganzen Gaußschen Zahlen*.

c. Bestimme die Einheitengruppe $\mathbb{Z}[i]^*$ des Ringes $\mathbb{Z}[i]$.

Aufgabe 6.18
Für $\omega \in \mathbb{Z}$, $\omega \geq 2$, bezeichnen wir mit $\sqrt{-\omega}$ die komplexe Zahl $i \cdot \sqrt{\omega}$.

a. Zeige, $\mathbb{Z}\left[\sqrt{-\omega}\right] := \{a + b \cdot \sqrt{-\omega} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ ist ein kommutativer Ring mit Eins, wobei die Addition und die Multiplikation einfach die Addition und Multiplikation komplexer Zahlen sein sollen.

b. Zeige, $\mathbb{Z}\left[\sqrt{-\omega}\right]^* = \{1, -1\}$.

C) Ringhomomorphismen

Mit einer neuen Struktur definieren wir auch gleich die strukturerhaltenden Abbildungen. Man beachte hierbei, daß zur Struktur eines Ringes mit *Eins* neben der Addition und der Multiplikation auch das Vorhandensein eines Einselementes zählt. Wir werden deshalb fordern, daß eine strukturerhaltende Abbildung verträglich ist mit der Addition und der Multiplikation und daß sie zudem das Einselement respektiert.

Definition 6.19
Es seien R und S zwei Ringe mit Eins. Eine Abbildung $\varphi : R \to S$ heißt *Ringhomomorphismus*, falls

a. $\varphi(a+b) = \varphi(a) + \varphi(b)$ für alle $a, b \in R$,

b. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ für alle $a, b \in R$ und

c. $\varphi(1_R) = 1_S$.

Ist φ ein Ringhomomorphismus, dann nennen wir φ einen

- *Monomorphismus*, falls φ injektiv ist;
- *Epimorphismus*, falls φ surjektiv ist;
- *Isomorphismus*, falls φ bijektiv ist.

Wir nennen zwei Ringe R und S *isomorph*, falls es einen Isomorphismus von R nach S gibt. Wir schreiben dann kurz $R \cong S$.

Beispiel 6.20
Ist $S \subseteq R$ ein Unterring des Ringes R, so ist die kanonische Inklusion $i_S : S \to R$ ein Ringhomomorphismus.

Lemma 6.21
Ist $\varphi : R \to S$ ein bijektiver Ringhomomorphismus, dann ist auch $\varphi^{-1} : S \to R$ ein Ringhomomorphismus.

Beweis: Daß φ^{-1} mit der Addition verträglich ist, folgt aus Proposition 1.51 c., da φ ein Homomorphismus von der abelschen Gruppe $(R, +)$ nach $(S, +)$ ist. Für die Verträglichkeit mit der Multiplikation kopiere man den dortigen Beweis. Schließlich gilt $\{x \in R \mid \varphi(x) = 1_S\} = \{1_R\}$ wegen der Bijektivität von φ und da $\varphi(1_R) = 1_S$, und mithin ist $\varphi^{-1}(1_S) = 1_R$. □

Lemma 6.22
Ist $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, so ist $\mathrm{Im}(\varphi)$ ein Unterring von S.

Beweis: Nach Proposition 1.51 ist $\mathrm{Im}(\varphi)$ eine Untergruppe von $(S, +)$, so daß $\mathrm{Im}(\varphi)$ abgeschlossen ist bezüglich Addition und Negativen. Zudem gilt

$$1_S = \varphi(1_R) \in \mathrm{Im}(\varphi)$$

und für $\varphi(a), \varphi(b) \in \mathrm{Im}(\varphi)$ gilt

$$\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b) \in \mathrm{Im}(\varphi).$$

□

Da ein Ringhomomorphismus $\varphi : R \longrightarrow S$ nach Definition ein Gruppenhomomorphismus von $(R, +)$ nach $(S, +)$ ist, folgt aus Lemma 1.52 unmittelbar folgendes Kriterium für die Injektivität von φ, wobei $\mathrm{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0_S\}$.

Lemma 6.23
Ein Ringhomomorphismus $\varphi : R \longrightarrow S$ ist genau dann ein Monomorphismus, wenn $\mathrm{Ker}(\varphi) = \{0_R\}$.

Bemerkung 6.24
Ist R ein kommutativer Ring mit Eins, so ist die Abbildung

$$\iota : R \longrightarrow R[t] : a \mapsto a \cdot t^0$$

ein Ringmonomorphismus, und somit ist R isomorph zum Unterring $\mathrm{Im}(\iota) = \{a \cdot t^0 \mid a \in R\}$. Wir werden diesen Isomorphismus in Zukunft nutzen und die Elemente von R mit den konstanten Polynomen identifizieren, d.h. wir schreiben z.B. $2t^2 + 3$ anstatt $2t^2 + 3t^0$.

Aufgabe 6.25
Es seien K ein Körper, R ein kommutativer Ring mit $1_R \neq 0_R$ und $\varphi : K \longrightarrow R$ ein Ringhomomorphismus. Zeige, φ ist ein Monomorphismus.

Aufgabe 6.26
Es sei S ein kommutativer Ring mit Eins, $R \subseteq S$ ein Unterring und $b \in S$.

a. Wir definieren

$$f(b) = \sum_{k=0}^{n} a_k \cdot b^k \in S$$

für $f = \sum_{k=0}^{n} a_k \cdot t^k \in R[t]$. Zeige, daß die Abbildung

$$\varphi_b : R[t] \longrightarrow S : f \mapsto f(b)$$

ein Ringhomomorphismus ist. Wir nennen φ_b einen *Einsetzhomomorphismus*.

b. Ist b Nullstelle des Polynoms $g = t^n + \alpha_{n-1} \cdot t^{n-1} + \ldots + \alpha_1 \cdot t + \alpha_0 \in R[t]$, so ist

$$\mathrm{Im}(\varphi_b) = \left\{ a_0 + a_1 \cdot b + a_2 \cdot b^2 + \ldots + a_{n-1} \cdot b^{n-1} \;\middle|\; a_0, \ldots, a_{n-1} \in R \right\}.$$

Wir bezeichnen diesen Unterring von S mit $R[b] = \mathrm{Im}(\varphi_b)$.

D) Ideale

Ist R ein kommutativer Ring mit Eins und S ein Unterring von R, so ist insbesondere $(S, +)$ ein Normalteiler der abelschen Gruppe $(R, +)$. Wir können mithin die Faktorgruppe $(R/S, +)$ bilden, wobei für zwei Nebenklassen $\overline{a}, \overline{b} \in R/S$ die Summe definiert ist als $\overline{a} + \overline{b} = \overline{a + b}$. Wir würden gerne auch die zweite Operation, die wir auf R und S haben, auf die Faktorgruppe R/S fortsetzen durch $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ und so R/S zu einem kommutativen Ring mit Eins machen. Das geht aber schief! Denn das Nullelement von R/S muß notwendig $\overline{0}$ sein, und für ein beliebiges $\overline{a} \in R/S$ und $b \in S$ muß dann

$$S = \overline{0} = \overline{a \cdot 0} = \overline{a} \cdot \overline{b} = \overline{a \cdot b} = (a \cdot b) + S$$

gelten. Also ist $a \cdot b \in S$, d.h. S ist abgeschlossen bezüglich der Multiplikation mit beliebigen Elementen aus R. Da nach Voraussetzung $1_R \in S$, müßte für ein beliebiges $a \in R$

$$a = a \cdot 1_R \in S$$

gelten und somit $S = R$. D.h. der einzige Unterring, für den die zugehörige Faktorgruppe $(R/S, +)$ auf diesem Weg zu einem Ring mit Eins gemacht werden könnte, wäre der Ring R selbst. Dann wäre aber R/S der Nullring, und wir könnten uns die Mühe sparen.

Es bleibt uns nichts anderes übrig, als den Begriff des Unterrings durch einen anderen Begriff zu ersetzen, der es uns erlaubt, Faktorstrukturen zu bilden. Wir haben bereits gesehen, daß es wünschenswert wäre, daß es sich bei dieser neu zu definierenden Unterstruktur um eine Untergruppe von $(R, +)$ handelt, die bezüglich der Multiplikation mit beliebigen Elementen aus R abgeschlossen ist. Dies führt zu folgender Definition, bei der wir uns wie für den Rest des Kapitels auf *kommutative* Ringe mit Eins beschränken.

Definition 6.27
Es sei R ein kommutativer Ring mit Eins und $\emptyset \neq I \subseteq R$ eine nicht-leere Teilmenge. I heißt ein *Ideal* von R, falls

(1) $a + b \in I$ für alle $a, b \in I$ und

(2) $r \cdot a \in I$ für alle $r \in R$ und $a \in I$.

Wir schreiben in diesem Fall $I \trianglelefteq R$, da Ideale für Ringe die Analoga von Normalteilern für Gruppen sind.

Bemerkung 6.28
Es sei R ein kommutativer Ring mit Eins und $I \trianglelefteq R$. Dann ist $(I, +)$ eine Untergruppe von $(R, +)$. Dies folgt aus dem Untergruppenkriterium 1.28, da mit $-1_R \in R$ und für $a \in I$ auch $-a = -1_R \cdot a \in I$.

Beachte auch, daß aus der Definition eines Ideals per Induktion unmittelbar

$$\sum_{k=1}^{n} r_k \cdot a_k \in I$$

für alle $r_k \in R$ und $a_k \in I$ folgt.

Beispiel 6.29

a. Ist R ein kommutativer Ring mit Eins, dann sind $\{0_R\}$ und R die *trivialen* Ideale von R.

b. $n\mathbb{Z}$ ist ein Ideal in $\mathbb{Z}$ für jedes $n \in \mathbb{Z}$, da die Menge abgeschlossen bezüglich $+$ und bezüglich Multiplikation mit ganzen Zahlen ist.

Da jedes Ideal von $(\mathbb{Z}, +, \cdot)$ insbesondere eine Untergruppe von $(\mathbb{Z}, +)$ ist folgt aus obigem Beispiel und der Klassifikation der Untergruppen von $(\mathbb{Z}, +)$ in Proposition 1.38 folgendes Korollar.

Korollar 6.30
Für eine Teilmenge $U \subseteq \mathbb{Z}$ sind die folgenden Aussagen äquivalent:

a. U *ist ein Ideal von* $(\mathbb{Z}, +, \cdot)$.

b. U *ist eine Untergruppe von* $(\mathbb{Z},+)$.

c. $U = n\mathbb{Z}$ *für eine ganze Zahl* $n \geq 0$.

Wie bei Untergruppen wollen wir auch bei Idealen wieder wissen, wie sie sich bezüglich bestimmter mengentheoretischer Operationen verhalten.

Proposition 6.31
Ist R *ein kommutativer Ring mit Eins und sind* $I_\lambda \trianglelefteq R$ *Ideale für* $\lambda \in \Lambda$, *dann ist* $\bigcap_{\lambda\in\Lambda} I_\lambda \trianglelefteq R$ *ein Ideal.*

Beweis: Seien $a, b \in \bigcap_{\lambda\in\Lambda} I_\lambda$ und $r \in R$. Dann ist $a + b \in I_\lambda$ und $r \cdot a \in I_\lambda$, da I_λ ein Ideal ist. Mithin ist auch

$$a + b, r \cdot a \in \bigcap_{\lambda\in\Lambda} I_\lambda.$$

Zudem ist $0_R \in I_\lambda$, da $(I_\lambda, +)$ eine Untergruppe von $(R, +)$ ist, und mithin ist $0_R \in \bigcap_{\lambda\in\Lambda} I_\lambda$, so daß die Menge nicht leer ist. □

Definition 6.32
Es sei R ein kommutativer Ring und $M \subseteq R$ eine Teilmenge. Wir definieren das *Erzeugnis* von M als

$$\langle M\rangle_R = \bigcap_{M\subseteq I\trianglelefteq R} I,$$

den Schnitt aller Ideale von R, die M enthalten.

Proposition 6.33
Es sei R *ein kommutativer Ring mit Eins und* $\emptyset \neq M \subseteq R$. *Dann ist das Erzeugnis*

$$\langle M\rangle_R = \left\{ \sum_{k=1}^{n} r_k \cdot a_k \;\middle|\; a_k \in M, r_k \in R, n \geq 1 \right\} \trianglelefteq R$$

von M *die Menge aller endlichen* Linearkombinationen *von Elementen in* M *mit Koeffizienten in* R.

Beweis: Wir setzen

$$J = \left\{ \sum_{k=1}^{n} r_k \cdot a_k \mid a_k \in M, r_k \in R, n \geq 1 \right\}$$

und zeigen zunächst, daß J ein Ideal von R ist.

Da M nicht die leere Menge ist, ist auch J nicht leer. Sind nun $\sum_{k=1}^{n} r_k \cdot a_k, \sum_{k=1}^{m} s_k \cdot b_k \in J$ mit $r_k, s_k \in R$ und $a_k, b_k \in M$, so setzen wir einfach $r_k = s_{k-n}$ und $a_k = b_{k-n}$ für $k = n+1, \ldots, n+m$ und erhalten

$$\sum_{k=1}^{n} r_k \cdot a_k + \sum_{k=1}^{m} s_k \cdot b_k = \sum_{k=1}^{n+m} r_k \cdot a_k \in J.$$

Da zudem für $r \in R$ auch $r \cdot r_k \in R$ gilt auch

$$r \cdot \sum_{k=1}^{n} r_k \cdot a_k = \sum_{k=1}^{n} (r \cdot r_k) \cdot a_k \in J.$$

Also ist J ein Ideal von R.

Zudem ist $M \subset J$, da $a = 1_R \cdot a \in J$ für alle $a \in M$. Also gilt nach Definition

$$\langle M \rangle_R = \bigcap_{M \subseteq I \trianglelefteq R} I \subseteq J.$$

Andererseits gilt für $\sum_{k=1}^{n} r_k \cdot a_k \in J$ mit $r_k \in R$ und $a_k \in M$, daß

$$\sum_{k=1}^{n} r_k \cdot a_k \in I$$

für jedes Ideal $I \trianglelefteq R$, das M enthält, wegen Bemerkung 6.28. Mithin gilt auch

$$J \subseteq \bigcap_{M \subseteq I \trianglelefteq R} I = \langle M \rangle_R.$$

$\square$

Beispiel 6.34
Ist R ein kommutativer Ring mit Eins und $a, b \in R$, dann gelten

$$\langle a \rangle_R = \{r \cdot a \mid r \in R\}$$

und

$$\langle a, b \rangle_R = \{r \cdot a + s \cdot b \mid r, s \in R\}.$$

Insbesondere gilt $n\mathbb{Z} = \langle n \rangle_{\mathbb{Z}}$.

Aufgabe 6.35
Zeige, daß

$$I = \{f \in \mathbb{Z}[t] \mid f(5) = 0\}$$

ein Ideal von $\mathbb{Z}[t]$ ist.

Aufgabe 6.36
Es sei R ein kommutativer Ring. R ist genau dann ein Körper, wenn R genau zwei Ideale besitzt.

Aufgabe 6.37
Es sei R ein Ring und $I_k \trianglelefteq R$, $k \in \mathbb{N}$, seien Ideale mit der Eigenschaft

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots,$$

d.h. $I_k \subseteq I_{k+1}$ für alle $k \in \mathbb{N}$. Zeige, daß dann auch

$$\bigcup_{k \in \mathbb{N}} I_k \trianglelefteq R$$

ein Ideal in R ist.

E) Faktorringe

Satz 6.38
Es sei R *ein kommutativer Ring mit Eins und* $I \trianglelefteq R$ *ein Ideal. Dann wird auf der abelschen Gruppe* $(R/I, +)$ *durch*

$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

für $\overline{a}, \overline{b} \in R/I$ *eine zweistellige Operation definiert, und* $(R/I, +, \cdot)$ *ist ein kommutativer Ring mit Einselement* $1_{R/I} = \overline{1_R}$. *Wir nennen* R/I *den* Faktorring *von* R *nach* I.

Beweis: Wir müssen zunächst zeigen, daß die Operation wohldefiniert ist, also nicht von der Wahl der Repräsentanten der Nebenklassen abhängt. Seien dazu $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, dann gilt nach Definition $a = a' + c$ und $b = b' + d$ mit $c, d \in I$. Damit folgt dann

$$a \cdot b = (a' + c) \cdot (b' + d) = a' \cdot b' + \big(a' \cdot d + c \cdot b' + c \cdot d\big)$$

mit $a' \cdot d + c \cdot b' + c \cdot d \in I$. Also gilt

$$\overline{a \cdot b} = a \cdot b + I = a' \cdot b' + I = \overline{a' \cdot b'},$$

und die Multiplikation ist wohldefiniert. Die Assoziativität und die Kommutativität der Multiplikation folgen dann aus den entsprechenden Eigenschaften der Multiplikation auf R. Zudem ist $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}$ für alle $\overline{a} \in R/I$, so daß $(R/I, +, \cdot)$ ein kommutativer Ring mit Eins $\overline{1}$ ist. □

Beispiel 6.39
$(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring mit Eins vermittels

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{und} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

für alle $a, b \in \mathbb{Z}$ und $n \geq 0$.

Beachte, in $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ ist offenbar jedes Element ungleich $\overline{0}$ eine Einheit, so daß $(Z_2, +, \cdot)$ ein Körper ist. Da zudem jeder Körper K mindestens zwei Elemente, nämlich $0_K \neq 1_K$ enthalten muß, ist $\mathbb{Z}_2$ der kleinst mögliche Körper.

Aufgabe 6.40
Welcher der folgenden Ringe ist ein Körper?

a. $\mathbb{Z}_4$.

b. $\mathbb{Z}_7$.

Beweise Deine Vermutung.

Aufgabe 6.41
Für eine positive ganze Zahl n definieren wir die Abbildung

$$\phi_n : \mathbb{Z}[t] \longrightarrow \mathbb{Z}_n[t] : \sum_{k=0}^{n} a_k \cdot t^k \mapsto \sum_{k=0}^{n} \overline{a_k} \cdot t^k.$$

Zeige, daß ϕ_n ein Ringepimorphismus ist. Wir nennen ϕ_n *Reduktion modulo* n.

Aufgabe 6.42

a. Bestimme $\mathbb{Z}_6^*$.

b. Bestimme $\mathbb{Z}_8^*$.

c. Bestimme $\mathbb{Z}_{15}^*$.

d. Stelle eine Vermutung auf, wann eine Element $\overline{z} \in \mathbb{Z}_n$ für $n \geq 2$ eine Einheit ist.

e. Zeige, für alle $n \geq 2$ ist $\overline{n-1} \in \mathbb{Z}_n$ eine Einheit.

F) Homomorphiesatz

Satz 6.43 (Homomorphiesatz)
Es sei $\varphi : R \longrightarrow S$ *ein Ringhomomorphismus zwischen kommutativen Ringen mit Eins. Dann ist* $\mathrm{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0\} \trianglelefteq R$ *ein Ideal und*

$$\overline{\varphi} : R/\,\mathrm{Ker}(\varphi) \longrightarrow \mathrm{Im}(\varphi)$$

ein Isomorphismus. Insbesondere gilt $R/\,\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.

Beweis: Nach Proposition 1.51 ist $(\mathrm{Ker}(\alpha), +)$ eine Untergruppe von $(R, +)$, also insbesondere nicht leer und abgeschlossen bezüglich der Addition. Sei nun $a \in \mathrm{Ker}(\alpha)$ und $r \in R$. Dann gilt

$$\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0.$$

Also ist $r \cdot a \in \mathrm{Ker}(\alpha)$ und $\mathrm{Ker}(\alpha)$ ist ein Ideal. Aus dem Homomorphiesatz 4.51 folgt dann, daß $\overline{\varphi}$ ein Isomorphismus abelscher Gruppen ist. Da zudem

$$\overline{\varphi}\big(\overline{a} \cdot \overline{b}\big) = \overline{\varphi}\big(\overline{a \cdot b}\big) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \overline{\varphi}\big(\overline{a}\big) \cdot \overline{\varphi}\big(\overline{b}\big)$$

und $\overline{\varphi}\big(\overline{1}\big) = \varphi(1) = 1$ gilt, ist $\overline{\varphi}$ ein Isomorphismus von Ringen. $\square$

Aufgabe 6.44

a. Finde alle Ringhomomorphismen $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_6$.

b. Finde alle Ringhomomorphismen $\varphi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}$.

c. Finde alle Ringhomomorphismen $\varphi : \mathbb{Q} \longrightarrow \mathbb{R}$.

7 Teilbarkeit in Ringen

Wir haben im vorigen Kapitel den Begriff des kommutativen Ringes mit Eins eingeführt. Als Modell für diesen Begriff haben uns die ganzen Zahlen gedient, und sie sollen auch das Leitbild für die in diesem Kapitel betrachteten Eigenschaften von Ringen und ihren Elementen sein.

A) **Integritätsbereiche**

Der zentrale Begriff wird der der Teilbarkeit sein. Eine uns vertraute Eigenschaft der natürlichen Zahlen ist, daß das Produkt zweier Zahlen nur dann Null ergeben kann, wenn eine der Zahlen bereits Null ist. Dies gilt in beliebigen Ringen nicht mehr. Betrachtet man etwa den Ring $\mathbb{Z}_4$, so ist die Restklasse $\overline{2} \neq \overline{0}$, aber $\overline{2}\cdot\overline{2} = \overline{4} = \overline{0}$. Dies hat unangenehme Folgen, denn $\overline{0}$ läßt sich somit auf mehrere Weisen als Vielfaches von $\overline{2}$ schreiben:

$$\overline{2} \cdot \overline{2} = \overline{0} = \overline{0} \cdot \overline{2}.$$

In einem solchen Ring gelten ganz offensichtlich die Kürzungsregeln für die Multiplikation nicht mehr. Diese sind aber für den Begriff der Teilbarkeit von zentraler Bedeutung, schließlich wollen wir einen *Teiler* auch *wegkürzen* können. Wir führen deshalb einen neuen Begriff für solche Ringe ein, die sich in dieser Beziehung vernünftig verhalten.

Definition 7.1
Es sei R ein kommutativer Ring mit Eins und $a \in R$.

a. a heißt ein *Nullteiler*, falls es ein $0 \neq b \in R$ gibt mit $a \cdot b = 0$.

b. R heißt *Integritätsbereich* oder *nullteilerfrei*, falls 0 der einzige Nullteiler in R ist.

Beispiel 7.2

a. Ist R nicht der Nullring, so ist 0 ein Nullteiler, da $0 \cdot 1 = 0$ und $1 \neq 0$.

b. Ist $a \in R^*$ eine Einheit, so ist a kein Nullteiler.

   Denn da a ein Inverses $a^{-1} \in R$ besitzt, folgt aus $a \cdot b = 0$ unmittelbar

$$b = 1 \cdot b = \left(a^{-1} \cdot a\right) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

c. Aus b. folgt, daß jeder Körper ein Integritätsbereich ist, da 0 das einzige Element ist, das keine Einheit ist. Insbesondere sind $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ Integritätsbereiche.

d. Jeder Unterring eines Integritätsbereichs ist ein Integritätsbereich. Insbesondere sind also $\mathbb{Z}$ und

$$\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b \cdot \sqrt{-5} \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z}\right\}$$

   Integritätsbereiche.

e. Ist R ein Integritätsbereich, so ist $R[t]$ ein Integritätsbereich und $R[t]^* = R^*$.

Denn sind $f, g \in R[t] \setminus \{0\}$, so ist $\deg(f), \deg(g) \geq 0$ und $\mathrm{lc}(f) \neq 0 \neq \mathrm{lc}(g)$. Aufgrund der Gradformeln für Polynome 6.16 folgt deshalb

$$\deg(f \cdot g) = \deg(f) + \deg(g) \geq 0, \tag{36}$$

da $\mathrm{lc}(f) \cdot \mathrm{lc}(g) \neq 0$ im Integritätsbereich R, und somit ist $f \cdot g \neq 0$. Also ist $R[t]$ ein Integritätsbereich. Ist $f \in R[t]^*$ eine Einheit und g das zugehörige Inverse, so gilt $f \cdot g = t^0 = 1$ und aus (36) folgt, daß $\deg(f) = 0 = \deg(g)$. D.h. f und g sind konstante Polynome und mithin gilt $f, g \in R^*$. Ist umgekehrt $f \in R^* \subseteq R[t]$, so gibt es ein $g \in R \subseteq R[t]$ mit $f \cdot g = 1 = t^0$ und somit $f \in R[t]^*$.

f. $\mathbb{Z}_4$ ist kein Integritätsbereich, da $\overline{2}$ wegen $\overline{2} \cdot \overline{2} = \overline{0}$ ein Nullteiler ist.

Lemma 7.3 (Kürzungsregeln)
Ist R ein Integritätsbereich, so gelten die Kürzungsregeln der Multiplikation, d.h. für alle $a, b, c \in R$ mit $a \neq 0$ gilt

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c$$

und

$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c.$$

Beweis: Wegen der Kommutativität der Multiplikation reicht es, eine der Kürzungsregeln zu zeigen. Seien dazu $a, b, c \in R$ mit $ab = ac$. Dann gilt

$$0 = ab - ac = a \cdot (b - c). \tag{37}$$

Da $a \neq 0$ und R ein Integritätsbereich ist, ist a kein Nullteiler. Mithin folgt aus (37), daß $b - c = 0$ und somit $b = c$ gilt. □

Nun können wir den Begriff der Teilbarkeit für Elemente eines Integritätsbereiches einführen. Dabei sollten wir beachten, daß wir in einem Integritätsbereich zunächst nur die Operationen der Addition und der Multiplikation haben, nicht aber eine Division. Wir müssen also mit ersteren auskommen um Teilbarkeit zu definieren.

Definition 7.4
Sei R ein Integritätsbereich und $a, b \in R$.

a. Wir sagen b *teilt* a, falls es ein $c \in R$ gibt mit $a = b \cdot c$. Wir schreiben in diesem Fall $b \mid a$.

b. Wir nennen $g \in R$ einen *größten gemeinsamen Teiler* von a und b, falls die folgenden beiden Eigenschaften erfüllt sind:
   (1) $g \mid a$ und $g \mid b$.
   (2) Für alle $h \in R$ mit $h \mid a$ und $h \mid b$ gilt $h \mid g$.

Wir bezeichnen mit

$$\mathrm{ggT}(a, b) = \{g \in R \mid g \text{ ist größter gemeinsamer Teiler von } a \text{ und } b\}$$

die Menge der größten gemeinsamen Teiler von a und b.

c. Wir nennen $k \in R$ ein *kleinstes gemeinsames Vielfaches* von a und b, falls die folgenden beiden Eigenschaften erfüllt sind:
   (1) $a \mid k$ und $b \mid k$.
   (2) Für alle $l \in R$ mit $a \mid l$ und $b \mid l$ gilt $k \mid l$.

   Wir bezeichnen mit

$$\mathrm{kgV}(a, b) = \{k \in R \mid k \text{ ist kleinstes gemeinsames Vielfaches von } a \text{ und } b\}$$

die Menge der kleinsten gemeinsamen Vielfachen von a und b.

d. Wir nennen a und b *teilerfremd*, wenn $1 \in \mathrm{ggT}(a, b)$.

Remark 7.5

Bei der Definition eines größten gemeinsamen Teilers g von a und b bedeutet die Bedingung (1), daß g überhaupt ein Teiler von a und von b ist. Die Bedingung (2) dient dazu den Zusatz *größter* zu rechtfertigen. Wie soll man in einem beliebigen Integritätsbereich entscheiden, wann g größer als h ist für $g, h \in R$? In $\mathbb{Z}$ kann man dazu vielleicht die bekannte Ordnungsrelation "$\leq$" heranziehen, indem man zum Beispiel für die Teiler $h = 2$ und $g = 6$ der Zahlen $a = 12$ und $b = 30$ definiert, daß wohl 6 der *größere* Teiler ist. Aber wie sollte man das etwa im Polynomring $\mathbb{Z}[t]$ machen? Ist $t + 2$ größer als t oder kleiner oder kann man sie vielleicht gar nicht vergleichen? Man macht sich deshalb zunutze, daß in den ganzen Zahlen der *größte* gemeinsame Teiler von a und b von allen gemeinsamen Teilern von a und b geteilt wird. In obigem Beispiel etwa sind 1, 2, 3 und 6 die einzigen positiven gemeinsamen Teiler von 12 und 30, und sie alle teilen $g = 6$. Man kann einen Teiler also *kleiner* als einen anderen nennen, wenn ersterer letzteren teilt. In diesem Sinne legt die Bedingung (2) in $\mathbb{Z}$ in der Tat fest, welcher der beiden Teiler g und h größer ist.

Nach Definition ist ein *größter gemeinsamer Teiler* zweier Elemente a und b also ein gemeinsamer Teiler von a und b, der von jedem anderen gemeinsamen Teiler geteilt wird. Analog ist ein *kleinstes gemeinsames Vielfaches* von a und b ein gemeinsames Vielfaches, das jedes andere gemeinsame Vielfache teilt.

Weshalb sprechen wir in der Definition von *einem* größten gemeinsamen Teiler und nicht von *dem* größten gemeinsamen Teiler? Schlicht und ergreifend, weil unsere Definition ihn nicht eindeutig bestimmt! In obigem Beispiel $a = 12, b = 30 \in \mathbb{Z}$ ist zweifellos $g = 6$ ein größter gemeinsamer Teiler von a und b. Aber auch -6 teilt a und b und wird von jedem anderen gemeinsamen Teiler von a und b geteilt. In $\mathbb{Z}$ ist nach unserer Definition ein gemeinsamer Teiler nur bis auf sein Vorzeichen (d.h. bis auf Multiplikation mit einer Einheit in $\mathbb{Z}$) eindeutig bestimmt.

In $\mathbb{Q}[t]$ wird das noch schlimmer. Betrachten wir zwei konstante Polynome $0 \neq a, g \in \mathbb{Q} \subset \mathbb{Q}[t]$, so ist

$$a = g \cdot \frac{a}{g}$$

und somit ist g ein Teiler von a. Zudem gilt für einen Teiler $c \in \mathbb{Q}[t]$ von a, daß es ein $d \in \mathbb{Q}[t]$ gibt mit $a = c \cdot d$, und aus der Gradformel $0 = \deg(a) = \deg(c) + \deg(d)$ folgt dann notwendig, daß $\deg(c) = 0$ und $c \in \mathbb{Q} \setminus \{0\}$. D.h. die Teiler von a sind genau die Elemente aus $\mathbb{Q} \setminus \{0\}$. Betrachten wir in $\mathbb{Q}[t]$ also etwa die konstanten Polynome $a = 2$ und $b = 5$, so sind die rationalen Zahlen $0 \neq q \in \mathbb{Q}$ genau die gemeinsamen Teiler von a und b und, da sie sich gegenseitig teilen, sind sie alle auch größte gemeinsame Teiler von a und b im Sinne der Definition. Da man in diesem Fall von einem größten gemeinsamen Teiler q zu einem anderen p durch Multiplikation mit der rationalen Zahl $\frac{p}{q}$ gelangt, könnte man auch sagen, daß der größte gemeinsamer Teiler nur bis auf Multiplikation mit einer rationalen Zahl ungleich Null bestimmt ist.

In den ganzen Zahlen hat man sich angewöhnt, einen der beiden größten gemeinsamen Teiler zu bevorzugen, nämlich den positiven. Für einen beliebigen Integritätsbereich gibt es dazu aber keinen einsichtigen Grund, so daß für uns jedes Element der Menge $\mathrm{ggT}(a, b)$ gleich gut ist.

Die Betrachtungen zum größten gemeinsamen Teiler lassen sich auch auf ein kleinstes gemeinsames Vielfaches k von a und b übertragen. Bedingung (1) bedeutet, daß k ein Vielfaches sowohl von a als auch von b ist, und (2) rechtfertigt den Zusatz *kleinstes*, da jedes andere Vielfache von a und b von k geteilt wird. In $\mathbb{Z}$ ist ein kleinstes gemeinsames Vielfaches wieder nur bis auf sein Vorzeichen bestimmt. □

Beispiel 7.6

a. Für $f = t - 1 \in \mathbb{Q}[t]$ und $g = t^n - 1 \in \mathbb{Q}[t]$ mit $n \geq 1$ gilt

$$g = f \cdot \left(t^{n-1} + t^{n-2} + \ldots + t + 1\right)$$

und somit $f \mid g$.

b. Betrachten wir die komplexen Zahlen $a = 9$, $b = 2 + \sqrt{-5}$, $c = 2 - \sqrt{-5}$ und $d = 3$ in $\mathbb{Z}\left[\sqrt{-5}\right]$. Wegen

$$a = 9 = \left(2 + \sqrt{-5}\right) \cdot \left(2 - \sqrt{-5}\right) = b \cdot c$$

gilt $b \mid a$.

Wir wollen nun noch zeigen, daß d kein Teiler von b ist. Nehmen wir das Gegenteil an, d.h. $d \mid b$. Dann gibt es ein $e = x + y \cdot \sqrt{-5}$ mit $x, y \in \mathbb{Z}$, so daß

$$b = d \cdot e.$$

Mit Hilfe des Absolutbetrags komplexer Zahlen erhalten wir damit dann aber

$$9 = |b|^2 = |d|^2 \cdot |e|^2 = 9 \cdot \left(x^2 + 5 \cdot y^2\right).$$

Es folgt $x^2 + 5y^2 = 1$, und da x und y ganze Zahlen sind, muß notwendig $y = 0$ und $x \in \{1, -1\}$ gelten. Aber $b \notin \{d, -d\}$, so daß wir einen Widerspruch hergeleitet haben.

c. In $\mathbb{Z}$ gilt $\mathrm{ggT}(6, 8) = \{-2, 2\}$ und $\mathrm{kgV}(6, 8) = \{-24, 24\}$.

Viele Eigenschaften eines Elementes a in einem Integritätsbereich können ausgedrückt werden durch Eigenschaften des von a erzeugten Ideals $\langle a\rangle_R = \{r \cdot a \mid r \in R\}$. Manche Formulierung und manches Argument wird dadurch deutlich verkürzt.

Lemma 7.7

Sei R *ein Integritätsbereich und* $a, b, g, k \in R$.

a. $b \mid a$ *genau dann, wenn* $\langle a\rangle_R \subseteq \langle b\rangle_R$.

b. *Die folgenden Aussagen sind gleichwertig:*
   (i) $a \mid b$ *und* $b \mid a$.
   (ii) $\langle a\rangle_R = \langle b\rangle_R$.
   (iii) *Es gibt eine Einheit* $u \in R^*$ *mit* $a = u \cdot b$.

c. *Genau dann ist* $g \in \mathrm{ggT}(a, b)$, *wenn die folgenden beiden Eigenschaften erfüllt sind:*
   (1) $\langle a, b\rangle_R \subseteq \langle g\rangle_R$.
   (2) *Für alle* $h \in R$ *mit* $\langle a, b\rangle_R \subseteq \langle h\rangle_R$, *gilt* $\langle g\rangle_R \subseteq \langle h\rangle_R$.

d. *Genau dann ist* $k \in \mathrm{kgV}(a, b)$, *wenn die folgenden beiden Eigenschaften erfüllt sind:*
   (1) $\langle k\rangle_R \subseteq \langle a\rangle_R \cap \langle b\rangle_R$.
   (2) *Für alle* $l \in R$ *mit* $\langle l\rangle_R \subseteq \langle a\rangle_R \cap \langle b\rangle_R$, *gilt* $\langle l\rangle_R \subseteq \langle k\rangle_R$.

Beweis: a. Falls $b \mid a$, so gibt es ein $c \in R$ mit $a = b \cdot c$. Mithin gilt für jedes $r \in R$ auch $r \cdot a = (r \cdot c) \cdot b \in \langle b\rangle_R$ und damit $\langle a\rangle_R \subseteq \langle b\rangle_R$. Gilt umgekehrt $\langle a\rangle_R \subseteq \langle b\rangle_R$, so ist $a \in \langle a\rangle_R \subseteq \langle b\rangle_R$ und mithin gibt es ein $c \in R$ mit $a = c \cdot b$. Also wird a von b geteilt.

b. Zunächst können wir ohne Einschränkung annehmen, daß $a \neq 0 \neq b$, da die drei Aussagen sonst offenbar gleichwertig sind. Setzen wir (i) voraus, so folgt (ii) aus Teil a.. Es gelte nun (ii), so daß $a \in \langle b\rangle_R$ und $b \in \langle a\rangle_R$. Es gibt also $u, v \in R$ mit $a = u \cdot b$ und $b = v \cdot a$. Aber dann gilt

$$1 \cdot a = a = u \cdot b = (u \cdot v) \cdot a.$$

Da im Integritätsbereich R die Kürzungsregel gilt und da $a \neq 0$, folgt $1 = u \cdot v$. Da zudem R kommutativ ist, ist $u \in R^*$ eine Einheit und nach Wahl von u gilt $a = u \cdot b$, so daß (iii) erfüllt ist. Setzen wir (iii) voraus, so gilt $a = u \cdot b$ und $b = u^{-1} \cdot a$. Damit gilt aber $b \mid a$ und $a \mid b$, so daß (i) erfüllt ist.

c. Dies ist nur eine Umformulierung der Definition mit Hilfe von Teil a., wenn man beachtet, daß $\langle a, b\rangle_R \subseteq \langle g\rangle_R$ genau dann, wenn $\langle a\rangle_R \subseteq \langle g\rangle_R$ und $\langle b\rangle_R \subseteq \langle g\rangle_R$.

d. Dies ist nur eine Umformulierung der Definition mit Hilfe von Teil a..

□

Eine Verallgemeinerung der Betrachtungen zum ggT und zum kgV in $\mathbb{Z}$ und $\mathbb{Q}[t]$ ist das folgende Lemma. Zwei größte gemeinsame Teiler unterscheiden sich nur durch eine Einheit, und das gleiche gilt für zwei kleinste gemeinsame Vielfache.

Lemma 7.8
Sei R ein Integritätsbereich, $a, b \in R$.

a. *Ist $g \in \mathrm{ggT}(a, b)$, dann ist $\mathrm{ggT}(a, b) = \{u \cdot g \mid u \in R^*\}$, d.h. ein größter gemeinsamer Teiler ist bis auf Multiplikation mit Einheiten eindeutig bestimmt.*

b. *Ist $k \in \mathrm{kgV}(a, b)$, dann ist $\mathrm{kgV}(a, b) = \{u \cdot k \mid u \in R^*\}$, d.h. ein kleinstes gemeinsames Vielfaches ist bis auf Multiplikation mit Einheiten eindeutig bestimmt.*

Beweis: Der Beweis sei dem Leser als Übungsaufgabe überlassen.

□

Aufgabe 7.9
Beweise Lemma 7.8.

Aufgabe 7.10

a. Bestimme die Nullteiler und die Einheiten in $\mathbb{Z}_{24}$. Ist $\mathbb{Z}_{24}$ ein Integritätsbereich?

b. Ist $3 + 4i$ ein Teiler von $7 + i$ in $\mathbb{Z}[i]$?

c. Bestimme alle größten gemeinsamen Teiler von $f = t^2 - 3t + 2$ und $g = t^3 - 2t^2 - t + 2$ in $\mathbb{Z}[t]$.

Die nächste Aufgabe zeigt, daß man in den ganzen Zahlen die Bestandteile *größter* beim größten gemeinsamen Teiler bzw. *kleinster* beim kleinsten gemeinsamen Vielfachen auch mittels der Ordnungsrelation in $\mathbb{Z}$ definieren kann.

Aufgabe 7.11
Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen. In Notation 4.44 haben wir die Zahl

$$\mathrm{kgv}(a, b) := \begin{cases} \min\{z > 0 \mid a \text{ und } b \text{ teilen } z\}, & \text{falls } a, b \neq 0, \\ 0, & \text{falls } a = 0 \text{ oder } b = 0, \end{cases}$$

eingeführt und ergänzen sie nun um die Zahl

$$\mathrm{ggt}(a, b) := \begin{cases} \max\left\{z > 0 \;\middle|\; z \text{ teilt sowohl } a \text{ als auch } b\right\}, & \text{falls } (a, b) \neq (0, 0), \\ 0, & \text{sonst.} \end{cases}$$

Zeige, $\mathrm{ggt}(a, b) \in \mathrm{ggT}(a, b)$ und $\mathrm{kgv}(a, b) \in \mathrm{kgV}(a, b)$.

Aufgabe 7.12
Es sei R ein kommutativer Ring mit Eins, der nur endlich viele Elemente enthält. Zeige, dann ist jedes Element von R entweder eine Einheit oder ein Nullteiler.

Aufgabe 7.13
Es sei R ein Integritätsbereich. Wir definieren eine Äquivalenzrelation auf $R \times (R \setminus \{0\})$ durch

$$(a, b) \sim (a', b') \quad :\Longleftrightarrow \quad a \cdot b' = a' \cdot b.$$

Die Äquivalenzklasse von (a, b) bezeichnen wir mit $\frac{a}{b}$, und die Menge aller Äquivalenzklassen bezeichnen wir mit $\mathrm{Quot}(R)$. Auf dieser Menge definieren wir eine Addition und eine Multiplikation durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Zeige:

a. $\sim$ ist eine Äquivalenzrelation.

b. Die Addition und die Multiplikation sind wohldefiniert.

c. $\big(\mathrm{Quot}(R), +, \cdot\big)$ ist ein Körper, der sogenannte *Quotientenkörper* von R.

B) **Faktorielle Ringe**

Wir haben bislang weder eine Aussage dazu getroffen, ob ein größter gemeinsamer Teiler zweier Elemente in einem Integritätsbereich stets existiert, noch wie man diesen ggf. ausrechnen kann. In der Tat werden wir später sehen, daß es Integritätsbereiche gibt, in denen größte gemeinsame Teiler nicht notwendig existieren. Wir wollen uns aber zunächst dem Problem zuwenden, wie man einen größten gemeinsamen Teiler denn berechnen könnte.

Die in der Schule gängigste Methode zur Berechnung eines größten gemeinsamen Teilers zweier positiver ganzer Zahlen a und b besteht darin, diese als ein Produkt von Primzahlen zu schreiben und festzustellen, welche Primzahlen mit welchen Vielfachheiten sowohl in a, als auch in b vorkommen. Wenn wir dieses Vorgehen adaptieren wollen, müssen wir zunächst den Begriff der *Primzahl* auf beliebige Integritätsbereiche erweitern. Dazu sollten wir uns charakterisierende Eigenschaften des Begriffs Primzahl anschauen. Eine *Primzahl* ist eine *positive* ganze Zahl, die genau *zwei* positive Teiler besitzt. Dies kann man auch etwas anders ausdrücken als, $p \in \mathbb{Z}_{>1}$ ist eine Primzahl genau dann, wenn für $a, b \in \mathbb{Z}_{\geq 0}$ gilt:

$$p = a \cdot b \quad \Longrightarrow \quad a = 1 \ \text{ oder } \ b = 1. \tag{38}$$

Denn $p = a \cdot b$ bedeutet, daß sowohl a als auch b Teiler von p sind, und für eine Primzahl können nicht beide gleich p sein.

Es gibt aber noch eine andere Eigenschaft, die Primzahlen charakterisiert, eine Eigenschaft, die man verwendet, wenn man den größten gemeinsamen Teiler auf obigem Weg ausrechnet. Wenn nämlich eine Primzahl ein Produkt teilt, so teilt sie schon einen der Faktoren. D.h. $p \in \mathbb{Z}_{>1}$ ist eine Primzahl genau dann, wenn für $a, b \in \mathbb{Z}_{\geq 0}$ gilt:

$$p \mid a \cdot b \quad \Longrightarrow \quad p \mid a \;\text{ oder }\; p \mid b. \tag{39}$$

Den Beweis der Gleichwertigkeit der Eigenschaften (38) und (39) liefert Korollar 7.18.

Wir haben mithin zwei Möglichkeiten, den Begriff der Primzahl auf beliebige Integritätsbereiche zu verallgemeinern, und wir werden sehen, daß diese beiden Begriffe nicht notwendig übereinstimmen. Eine vernünftige Theorie der Teilbarkeit erhalten wir aber nur, wenn die beiden Begriffe übereinstimmen, denn nur dann läßt sich die Primfaktorzerlegung, wie wir sie aus den ganzen Zahlen gewohnt sind, verallgemeinern.

Ein Problem bei der Verallgemeinerung der obigen Bedingungen auf beliebige Integritätsbereiche ist das Fehlen einer Ordnungsrelation $>$, die es uns erlauben würde von *positiven* Ringelementen zu sprechen. Das erweist sich bei näherem Hinsehen jedoch als überflüssig, wenn wir in $\mathbb{Z}$ auch negative Zahlen zulassen. Die Bedingung “$= 1$” bzw. “$\neq 1$” kann man dann durch “$\in \mathbb{Z}^*$” bzw. “$\notin \mathbb{Z}^*$” ersetzen.

Definition 7.14
Sei R ein Integritätsbereich.

a. Ein Element $0 \neq p \in R \setminus R^*$ heißt *irreduzibel*, falls aus $p = a \cdot b$ mit $a, b \in R$ folgt, daß $a \in R^*$ oder $b \in R^*$.

b. Ein Element $0 \neq p \in R \setminus R^*$ heißt *prim*, falls aus $p \mid a \cdot b$ mit $a, b \in R$ folgt, daß $p \mid a$ oder $p \mid b$.

c. R heißt ein *faktorieller* Ring[30], falls jedes $0 \neq a \in R \setminus R^*$ sich als Produkt von endlich vielen Primelementen schreiben läßt.

Wir werden weiter unten sehen, daß in einem faktoriellen Ring die Zerlegung in ein Produkt von Primelementen im wesentlichen eindeutig ist.

Beispiel 7.15

a. Wir unterscheiden in $\mathbb{Z}$ zwischen *Primzahlen*, welche nach Definition positiv sind, und *Primelementen*, welche auch negativ sein können. Aufgrund der obigen Vorbetrachtungen ist eine ganze Zahl z genau dann prim, wenn sie irreduzibel ist, und das ist genau dann der Fall, wenn z oder $-z$ eine Primzahl ist. Wie angedeutet, beweisen wir diese Tatsache erst weiter unten in Korollar 7.18.

[30] In der Literatur werden faktorielle Ringe auch *ZPE-Ringe* genannt, wobei ZPE für *eindeutige Primfaktorzerlegung* steht.

b. Ist K ein Körper und $f \in K[t]$ mit $\deg(f) = 1$, so ist f irreduzibel.

Denn $f = g \cdot h$ mit $g, h \in K[t]$ impliziert $1 = \deg(f) = \deg(g) + \deg(h)$. Mithin gilt entweder $\deg(g) = 0$ und $\deg(h) = 1$ oder es gilt $\deg(g) = 1$ und $\deg(h) = 0$. In ersterem Fall ist $g \in K \setminus \{0\} = K^* = K[t]^*$, in letzterem ist $h \in K \setminus \{0\} = K^* = K[t]^*$, wobei die Gleichheit $K \setminus \{0\} = K^*$ gilt, da K ein Körper ist.

c. Das Polynom $f = 2t + 2 \in \mathbb{Z}[t]$ ist nicht irreduzibel, da $f = 2 \cdot (t + 1)$ und weder 2 noch $t + 1$ ist eine Einheit in $\mathbb{Z}[t]$, da $\mathbb{Z}[t]^* = \mathbb{Z}^* = \{1, -1\}$.

d. Ist R ein Integritätsbereich und sind $p, q \in R$ irreduzibel mit $p \mid q$, dann ist $\langle p \rangle_R = \langle q \rangle_R$, d.h. die beiden unterscheiden sich nur um einen Einheit.

Denn $p \mid q$ bedeutet, es gibt ein $c \in R$ mit $q = p \cdot c$. Da q irreduzibel ist und p keine Einheit, muß notwendig c eine Einheit sein. Also unterscheiden sich p und q nur um eine Einheit.

Wir wollen im folgenden den Zusammenhang der Begriffe *prim* und *irreduzibel* untersuchen, und dabei unter anderem zeigen, daß diese im Ring der ganzen Zahlen übereinstimmen.

Lemma 7.16

Ist R *ein Integritätsbereich und* $p \in R$ *prim, so ist* p *irreduzibel.*

Beweis: Seien $a, b \in R$ gegeben mit $p = a \cdot b$, dann gilt insbesondere $p \mid a \cdot b$. Mithin gilt $p \mid a$ oder $p \mid b$. In ersterem Fall gibt es ein $c \in R$ mit $a = p \cdot c$ und somit gilt

$$p \cdot 1 = p = a \cdot b = p \cdot c \cdot b.$$

Da im Integritätsbereich R die Kürzungsregel gilt, folgt unmittelbar, daß $1 = c \cdot b$ und b eine Einheit ist. Analog folgt aus $p \mid b$, daß $a \in R^*$. Somit ist p irreduzibel. □

Beispiel 7.17

a. Wir wollen nun ein Beispiel dafür geben, daß ein irreduzibles Element nicht notwendig prim sein muß.

Dazu betrachten wieder die komplexen Zahlen $a = 9$, $b = 2 + \sqrt{-5}$, $c = 2 - \sqrt{-5}$ und $d = 3$ in $\mathbb{Z}\left[\sqrt{-5}\right]$. Wir haben bereits in Beispiel 7.6 gesehen, daß d kein Teiler von b ist. Analog zeigt man, daß d kein Teiler von c ist. Aber $d = 3$ ist ein Teiler von $d^2 = a = b \cdot c$. Mithin ist d *nicht prim*, da es das Produkt $b \cdot c$, aber keinen der Faktoren teilt.

Sei nun $d = f \cdot g$ mit $f = x + y \cdot \sqrt{-5}$ und $g = u + v \cdot \sqrt{-5}$, $x, y, u, v \in \mathbb{Z}$. Dann gilt

$$9 = |d|^2 = |f|^2 \cdot |g|^2 = \left(x^2 + 5y^2\right) \cdot \left(u^2 + 5v^2\right)$$

mit $x^2 + 5y^2, u^2 + 5v^2 \in \mathbb{N}$. Es folgt, daß $(x^2 + 5y^2, u^2 + 5v^2) \in \{(9, 1), (1, 9)\}$. In ersterem Fall muß $u \in \{1, -1\}$ und $v = 0$ sein, so daß g eine Einheit in

$\mathbb{Z}[\sqrt{-5}]$ ist. In letzterem Fall muß $x \in \{1, -1\}$ und $y = 0$ sein, so daß f eine Einheit in $\mathbb{Z}[\sqrt{-5}]$ ist. Es folgt, daß d *irreduzibel* ist.

b. Ist R faktoriell, so ist jedes irreduzible Element prim.

Denn falls $p \in R$ irreduzibel ist, so ist p nach Voraussetzung ein Produkt $p = q_1 \cdots q_k$ von Primelementen. Nehmen wir $k \geq 2$ an. Da q_k prim ist, ist es keine Einheit und mithin muß $q_1 \cdots q_{k-1}$ eine Einheit sein. Es gibt also ein $a \in R$ mit $1 = q_1 \cdot (q_2 \cdots q_{k-1} \cdot a)$, so daß dann q_1 eine Einheit ist, im Widerspruch zur Voraussetzung q_1 prim. Mithin ist $k = 1$ und $p = q_1$ ist prim.

c. $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, da 3 irreduzibel aber nicht prim ist.

Wir haben bislang nur Körper einen Körper mit nur endlich vielen Elementen kennen gelernt, $\mathbb{Z}_2$. Für Anwendungen in der Kryptographie oder der Kodierungstheorie sind endliche Körper aber von weit größerem Interesse als unendliche. Wir werden nun zeigen, daß das Beispiel $\mathbb{Z}_2$ verallgemeinert werden kann.

Korollar 7.18
Für $0 \neq n \in \mathbb{Z}$ sind die folgenden Aussagen gleichwertig:

a. $\mathbb{Z}_n$ *ist ein Körper.*

b. $\mathbb{Z}_n$ *ist ein Integritätsbereich.*

c. n *ist prim.*

d. n *ist irreduzibel, d.h.* n *ist eine Primzahl.*

Beweis:

a. ⇒ b.: Ist $\mathbb{Z}_n$ ein Körper, so ist $\mathbb{Z}_n$ ein Integritätsbereich nach Beispiel 7.2.

b. ⇒ c.: Gilt $n \mid a \cdot b$ mit $a, b \in \mathbb{Z}$, dann ist

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{0} \in \mathbb{Z}_n.$$

Da nach Voraussetzung $\mathbb{Z}_n$ nullteilerfrei ist, muß $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$ gelten. In ersterem Fall gilt $n \mid a$, in letzterem $n \mid b$. Also ist n prim in $\mathbb{Z}$.

c. ⇒ d.: Dies folgt aus Lemma 7.16.

d. ⇒ a.: Ist I ein Ideal in $\mathbb{Z}_n$, so ist $(I, +)$ eine Untergruppe von $(\mathbb{Z}_n, +)$ und die Ordnung von I ist nach dem Satz von Lagrange ein Teiler der Primzahl $n = |\mathbb{Z}_n|$. Also muß $|I|$ entweder 1 oder n sein, d.h. $I = \{\overline{0}\}$ oder $I = \mathbb{Z}_n$. Da zudem $\{\overline{0}\} \neq \mathbb{Z}_n$, hat $\mathbb{Z}_n$ also genau zwei Ideale und ist nach Aufgabe 6.36 ein Körper.

□

Bemerkung 7.19
Ist R ein faktorieller Ring und $0 \neq a \in R \setminus R^*$, dann ist die Darstellung $a = p_1 \cdots p_r$

als Produkt von Primelementen *im wesentlichen eindeutig*, d.h. sind

$$p_1 \cdot \cdots \cdot p_r = q_1 \cdot \cdots \cdot q_s \tag{40}$$

zwei solche Darstellungen, so gilt $r = s$, und nach Umordnen der q_i unterscheiden sich p_i und q_i nur noch um eine Einheit, d.h. $\langle p_i \rangle_R = \langle q_i \rangle_R$. Dies ist leicht einzusehen: da p_1 prim und ein Teiler der rechten Seite von (40) ist, muss p_1 eines der q_i teilen. Nach Umordnen der q_i können wir $p_1 \mid q_1$ annehmen. Da beide prim sind, sind sie nach Lemma 7.16 auch beide irreduzibel und unterscheiden sich nach Beispiel 7.15 nur um eine Einheit. Nun können wir p_1 aus (40) kürzen und induktiv das gleiche Verfahren auf das verbleibende Produkt anwenden. □

Bemerkung 7.20
Es sei R ein faktorieller Ring und $a = p_1^{m_1} \cdots p_r^{m_r}$ und $b = p_1^{n_1} \cdots p_r^{n_r}$ seien Elemente in $R \setminus \{0\}$ mit $p_1, \ldots, p_r$ prim, $\langle p_i \rangle_R \neq \langle p_j \rangle_R$ für $i \neq j$ und $m_1, \ldots, m_r, n_1, \ldots, n_r \in \mathbb{N}$. Dann sieht man wie für die ganzen Zahlen, daß

$$p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}} \in \mathrm{ggT}(a, b)$$

und

$$p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}} \in \mathrm{kgV}(a, b).$$

Man nennt eine Darstellung von a wie oben auch eine *Primfaktorzerlegung* von a, wenn $m_i > 0$ für alle $i = 1, \ldots, r$. Nach Bemerkung 7.19 ist sie bis auf die Reihenfolge der Faktoren und Multiplikation mit Einheiten eindeutig bestimmt. □

Aufgabe 7.21
Es sei R ein Integritätsbereich und es gebe eine natürliche Zahl $n \geq 1$ so, daß $n \cdot 1_R = \sum_{k=1}^{n} 1_R = 0_R$, d.h. die n-fache Summe des Einselementes ergibt das Nullelement. Zeige, daß die kleinste positive ganze Zahl $p = \min\{m \in \mathbb{Z}_{>0} \mid m \cdot 1_R = 0_R\}$ mit dieser Eigenschaft irreduzibel (d.h. eine Primzahl) ist.

Man nennt diese Zahl p auch die *Charakteristik* des Ringes.

Aufgabe 7.22
Ist $p = x + y \cdot i \in \mathbb{Z}[i]$ so, daß $q := |p|^2 = x^2 + y^2$ eine Primzahl ist, dann ist p ein Primelement in $\mathbb{Z}[i]$. Finde zudem ein Beispiel für eine solche Zahl p.

Aufgabe 7.23
Bestimme alle Polynome f in $\mathbb{Z}_2[t]$ vom Grad 4, deren Leitkoeffizient $\mathrm{lc}(f)$ und deren konstanter Koeffizient $f(0)$ beide $\overline{1}$ sind. Welche dieser Polynome sind irreduzibel?

Aufgabe 7.24

a. Es sei $f \in \mathbb{Z}[t]$ mit $\mathrm{lc}(f) = 1$. Zeige, falls es eine Primzahl $p \in \mathbb{Z}$ gibt, so daß die Reduktion $\phi_p(f)$ von f modulo p irreduzibel in $\mathbb{Z}_p[t]$ ist (siehe Aufgabe 6.41), so ist f irreduzibel in $\mathbb{Z}[t]$.

b. Bestimme alle Polynome f in $\mathbb{Z}_2[t]$ vom Grad $0 \leq \deg(f) \leq 4$ und schreibe sie jeweils als Produkt von möglichst vielen Polynomen vom Grad größer oder gleich 1.

c. Ist $f = t^4 + 187t^3 + 5t^2 - 33t + 3001 \in \mathbb{Z}[t]$ irreduzibel?

C) **Euklidische Ringe**

Faktorielle Ringe verallgemeinern die ganzen Zahlen und wie in Bemerkung 7.20 gesehen, ist die *eindeutige Primfaktorzerlegung* eines Elements sehr nützlich. Allerdings wissen wir bislang von keinem anderen Ring als den ganzen Zahlen, daß er faktoriell ist. Uns fehlt ein gutes Kriterium, dies zu entscheiden, ein Kriterium, das einfacher zu Handhaben ist, als für jedes Element eine Primfaktorzerlegung anzugeben.

Stellen wir dieses Problem einmal hintan und nehmen an, wir wüßten von einem Ring bereits, daß er faktoriell ist. Unser Ausgangspunkt war, aus der Kenntnis von Primfaktorzerlegungen einen größten gemeinsamen Teiler zu bestimmen. Um dies praktisch umzusetzen, fehlt uns mithin noch ein Verfahren, das es uns erlaubt, die Primfaktorzerlegung eines Elementes tatsächlich auszurechnen. Und obwohl dies in der Schulzeit bei den ganzen Zahlen *das* Verfahren war, um den größten gemeinsamen Teiler zweier ganzer Zahlen zu bestimmen, wage ich zu bezweifeln, daß Ihr es auf die folgenden beiden Zahlen anwenden wollt:

$$a = 1234567890987654321234567890987654321$$

und

$$b = 27283950390827160499283950390827065.$$

Selbst mit einem Taschenrechner halte ich das Unterfangen für aussichtslos, und für Anwendungen in der Kryptographie sind diese beiden Zahlen nahezu winzig. Dort sind Zahlen mit 500 und mehr Ziffern notwendig, und die Sicherheit neuerer kryptographischer Verfahren beruht auf der Tatsache, daß es sehr schwer ist, eine Zahl in ihre Primfaktoren zu zerlegen.

Es gibt aber ein sehr einfaches und effizientes Verfahren, um den größten gemeinsamen Teiler zu bestimmen, ohne die Primfaktorzerlegung zu kennen. Dieses Verfahren wollen wir im folgenden beschreiben. Es funktioniert nicht nur für die ganzen Zahlen, sondern für jeden Integritätsbereich, in dem man eine *Division mit Rest* hat.

Definition 7.25

Ein Integritätsbereich R heißt ein *euklidischer Ring,* wenn es eine Funktion

$$\nu : R \setminus \{0\} \longrightarrow \mathbb{N}$$

gibt, so daß es für alle $a, b \in R \setminus \{0\}$ eine *Division mit Rest* der Form

$$a = q \cdot b + r$$

mit $q, r \in R$ gibt, wobei entweder $r = 0$ oder $\nu(r) < \nu(b)$. Wir nennen ν dann eine *euklidische Funktion* von R.

Beispiel 7.26
$\mathbb{Z}$ ist mittels $\nu : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N} : z \mapsto |z|$ und der wohlbekannten Division mit Rest (siehe Bemerkung 1.39) ein euklidischer Ring.

Bevor wir zeigen, wie uns die Division mit Rest hilft, einen größten gemeinsamen Teiler zu bestimmen, wollen wir zeigen, daß es außer den ganzen Zahlen noch andere euklidische Ringe gibt. Das vielleicht wichtigste Beispiel neben $\mathbb{Z}$ sind die Polynomringe über Körpern.

Proposition 7.27 (Division mit Rest im Polynomring)
Ist K ein Körper und sind $0 \neq f, g \in K[t]$, dann gibt es Polynome $q, r \in K[t]$, so daß

$$g = q \cdot f + r \quad \textit{und} \quad \deg(r) < \deg(f).$$

Dabei sind q und r eindeutig bestimmt.

Beweis: Seien $f = \sum_{i=0}^{n} a_i \cdot t^i$ und $g = \sum_{i=0}^{m} b_i \cdot t^i$ mit $m = \deg(g)$ und $n = \deg(f)$. Wir führen den Beweis der Existenz einer solchen Division mit Rest mittels Induktion nach m.

Falls $m = n = 0$, so sind wir fertig mit $q = \frac{b_0}{a_0}$ und $r = 0$, und falls $0 \leq m < n$, so können wir $q = 0$ und $r = g$ wählen. Diese Fälle schließen den Induktionsanfang $m = 0$ ein.

Es reicht nun, den Fall $m > 0$ und $n \leq m$ zu betrachten. Definieren wir

$$g' := g - \frac{b_m}{a_n} \cdot t^{m-n} \cdot f.$$

Dann heben sich in der Differenz die Leitterme auf, so daß $\deg(g') < \deg(g) = m$ gilt. Folglich existieren nach Induktionsannahme Polynome $q', r' \in K[t]$, so daß

$$q' \cdot f + r' = g' = g - \frac{b_m}{a_n} \cdot t^{m-n} \cdot f$$

und $\deg(r') < \deg(f)$. Also

$$g = \left(q' + \frac{b_m}{a_n} \cdot t^{m-n}\right) \cdot f + r',$$

und wir sind fertig mit $q = q' + \frac{b_m}{a_n} \cdot t^{m-n}$ und $r = r'$.

Es bleibt nur noch die Eindeutigkeit der Zerlegung zu zeigen. Nehmen wir dazu an, daß

$$g = q \cdot f + r = q' \cdot f + r'$$

mit $q, q', r, r' \in K[t]$ und $\deg(r), \deg(r') < \deg(f)$. Dann gilt

$$(q - q') \cdot f = r' - r$$

und mithin

$$\deg(q - q') + \deg(f) = \deg(r' - r) \leq \max\{\deg(r), \deg(r')\} < \deg(f).$$

Das ist aber nur möglich, wenn $q - q' = 0$. Also gilt $q = q'$ und dann auch $r = r'$. $\square$

Wir erhalten somit unmittelbar folgendes Korollar.

Korollar 7.28
Ist K *ein Körper, so ist* $K[t]$ *ein euklidischer Ring mit* deg *als euklidischer Funktion.*

Der Beweis von Proposition 7.27 ist konstruktiv, d.h. er liefert uns ein Verfahren, wie wir die Division mit Rest im Polynomring durchführen können.

Beispiel 7.29
Seien $f = t^3 + t + 1, g = t - 1 \in \mathbb{Q}[t]$ gegeben. Wir führen Polynomdivision durch

$$\begin{array}{l}
(t^3 \qquad + \ t + 1) : (t-1) = t^2 + t + 2 + \frac{r}{t-1} \\
\underline{\ t^3 - t^2} \\
\qquad t^2 + \ t \\
\qquad \underline{t^2 - \ t} \\
\qquad\qquad 2t + \ 1 \\
\qquad\qquad \underline{2t - \ 2} \\
\qquad\qquad\qquad 3 \quad =: r
\end{array}$$

und erhalten $f = (t^2 + t + 2) \cdot g + 3$. □

Nun wollen wir den Euklidischen Algorithmus kennen lernen, der es uns erlaubt, in euklidischen Ringen den größten gemeinsamen Teiler auszurechnen. Bevor wir den Algorithmus als Satz formulieren und beweisen, wollen wir ihn beispielhaft in den ganzen Zahlen anwenden, um die Formulierung des Satzes und den Beweis auf dem Weg leichter verständlich zu machen.

Beispiel 7.30
Wir wollen einen größten gemeinsamen Teiler der ganzen Zahlen $r_0 = 66$ und $r_1 = 15$ berechnen. Dazu führen wir Division mit Rest durch

$$r_0 = 66 = 4 \cdot 15 + 6 = q_1 \cdot r_1 + r_2$$

und erhalten den Rest $r_2 = 6$. Sodann teilen wir r_1 durch r_2 mit Rest,

$$r_1 = 15 = 2 \cdot 6 + 3 = q_2 \cdot r_2 + r_3,$$

und erhalten den Rest $r_3 = 3$. Dann teilen wir r_2 durch r_3 mit Rest,

$$r_2 = 6 = 2 \cdot 3 + 0 = q_2 \cdot r_3 + r_4,$$

und erhalten den Rest $r_4 = 0$. Das Verfahren bricht ab, da wir r_3 nicht weiter durch $r_4 = 0$ teilen können. Wir erhalten als größten gemeinsamen Teiler von $r_0 = 66$ und $r_1 = 15$

$$r_3 = 3 \in \mathrm{ggT}(66, 15) = \mathrm{ggT}(r_0, r_1),$$

d.h. den letzten Rest der sukkzessiven Division mit Rest, der nicht Null war.

Der folgende Satz begründet, weshalb das obige Verfahren zum Erfolg führen mußte.

Satz 7.31 (Euklidischer Algorithmus)
Sei R *ein euklidischer Ring mit euklidischer Funktion* ν *und seien* $r_0, r_1 \in R \setminus \{0\}$.

Für $k \geq 2$ *definieren wir, solange* $r_{k-1} \neq 0$ *gilt, rekursiv* r_k *als einen Rest der Division mit Rest von* r_{k-2} *durch* r_{k-1}*, d.h. es gibt ein* $q_{k-1} \in R$ *mit*

$$r_{k-2} = q_{k-1} \cdot r_{k-1} + r_k$$

mit

$$r_k = 0 \quad \textit{oder} \quad \nu(r_k) < \nu(r_{k-1}).$$

Dann gibt es ein $n \geq 2$ *so, daß* $r_n = 0$*, und es gilt* $r_{n-1} \in \mathrm{ggT}(r_0, r_1)$.

Beweis: Solange r_{k-1} nicht Null ist, können wir Division mit Rest durchführen und erhalten auf dem Wege $r_k, q_{k-1} \in R$, so daß die obigen Bedingungen erfüllt sind.

Unsere Konstruktion liefert

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, & \nu(r_2) &< \nu(r_1), \\ r_1 &= r_2 q_2 + r_3, & \nu(r_3) &< \nu(r_2), \\ &\vdots \\ r_{k-2} &= r_{k-1} q_{k-1} + r_k, & \nu(r_k) &< \nu(r_{k-1}), \end{aligned}$$

und damit eine streng monoton fallende Folge natürlicher Zahlen

$$\nu(r_1) > \nu(r_2) > \nu(r_3) > \ldots.$$

Das Verfahren muß mithin zwangsläufig abbrechen, und das ist nur der Fall, wenn es ein $n \geq 2$ gibt mit $r_n = 0$.

Wir wollen nun durch Induktion nach n zeigen, daß

$$r_{n-1} \in \mathrm{ggT}(r_0, r_1).$$

Beachte, daß $n - 1$ die Anzahl der Rekursionsschritte des Verfahrens ist, d.h. die Anzahl der Divisionen mit Rest, die berechnet werden müssen, bis sich der Rest Null ergibt.

Induktionsanfang: $n = 2$. Dann ist $r_2 = 0$, also $r_1 \mid r_0$ und $r_1 \in \mathrm{ggT}(r_0, r_1)$.

Induktionsschluß: Sei nun $n \geq 3$ und die Behauptung gelte für alle Paare, für die das Verfahren einen Rekursionsschritt weniger benötigt. Die Betrachtung der letzten $n-3$ Rekursionsschritte liefert mithin durch Anwendung der Induktionsvoraussetzung auf r_1 und r_2:

$$r_{n-1} \in \mathrm{ggT}(r_1, r_2).$$

Insbesondere ist r_{n-1} ein Teiler von r_1 und von r_2. Da nach Voraussetzung $r_0 = q_1 \cdot r_1 + r_2$, ist dann aber r_{n-1} auch ein Teiler von r_0.

Sei nun $r \in R$ ein weiterer Teiler von r_0 und r_1, dann gilt

$$r \mid (r_0 - q_1 \cdot r_1) = r_2,$$

und mithin ist r ein Teiler sowohl von r_1 als auch von r_2. Aber da $r_{n-1} \in \mathrm{ggT}(r_1, r_2)$ gilt dann

$$r \mid r_{n-1},$$

und nach Definition ist deshalb $r_{n-1} \in \mathrm{ggT}(r_0, r_1)$. $\square$

Um den Algorithmus durchführen zu können brauchen wir nur die Division mit Rest. Diese können wir auch im Polynomring über einem Körper durchführen, so daß wir größte gemeinsame Teiler auch im Polynomring ausrechnen können.

Beispiel 7.32
Betrachte $r_0 = t^4 + t^2 \in \mathbb{Q}[t]$ und $r_1 = t^3 - 3t^2 + t - 3 \in \mathbb{Q}[t]$. Division mit Rest liefert im ersten Schritt

$$r_0 = t^4 + t^2 = (t+3) \cdot (t^3 - 3t^2 + t - 3) + (9t^2 + 9) = q_1 \cdot r_1 + r_2$$

mit Rest $r_2 = 9t^2 + 9$. Im nächsten Schritt erhalten wir

$$r_1 = t^3 - 3t^2 + t - 3 = \left(\frac{1}{9} \cdot t - \frac{1}{3}\right) \cdot (9t^2 + 9) + 0 = q_2 \cdot r_2 + r_3$$

mit Rest $r_3 = 0$. Das Verfahren bricht ab und $r_2 = 9t^2 + 9 \in \mathrm{ggT}(r_0, r_1)$ ist ein größter gemeinsamer Teiler. Man kann diesen normieren, indem man das Polynom durch seinen Leitkoeffizienten teilt und erhält dann als normierten größten gemeinsamen Teiler

$$t^2 + 1 \in \mathrm{ggT}\left(t^4 + t^2, t^3 - 3t^2 + t - 3\right).$$

Bemerkung 7.33
Ist R ein euklidischer Ring und $a, b \in R \setminus \{0\}$, so gilt $g \in \mathrm{ggT}(a, b)$ genau dann wenn $\frac{a \cdot b}{g} \in \mathrm{kgV}(a, b)$. Man kann mit Hilfe des Euklidischen Algorithmus in einem euklidischen Ring also auch kleinste gemeinsame Vielfache ausrechnen.

Aufgabe 7.34
Zeige, daß $\mathbb{Z}[i] = \{x + i \cdot y \mid x, y \in \mathbb{Z}\}$ ein euklidischer Ring mit euklidischer Funktion $\nu : \mathbb{Z}[i] \longrightarrow \mathbb{N} : a \mapsto |a|^2$ ist.

Aufgabe 7.35
Betrachte die Polynome

$$f = t^5 + 3t^4 + 2t^3 + 5t^2 + 7t + 2 \in \mathbb{Z}[t]$$

und

$$g = t^3 + t^2 + t + 1 \in \mathbb{Z}[t].$$

a. Bestimme einen größten gemeinsamen Teiler von f und g in $\mathbb{Q}[t]$ mittels des Euklidischen Algorithmus.

b. Betrachte die Koeffizienten von f und g modulo 3 und bestimme einen größten gemeinsamen Teiler der resultierenden Polynome $\phi_3(f)$ und $\phi_3(g)$ in $\mathbb{Z}_3[t]$.

D) **Der Polynomring** $K[t]$

Wir haben im letzten Abschnitt gesehen, wie Polynomdivision funktioniert und daß es sich dabei um eine Division mit Rest handelt, die den Polynomring $K[t]$ über einem Körper K zu einem euklidischen Ring macht. In diesem Abschnitt wollen wir die Division mit Rest ausnutzen, um Nullstellen eines Polynoms als Linearfaktoren abzuspalten. Um von einer Nullstelle eines Polynoms sprechen zu können, müssen wir erlauben, in Polynomen für die Unbestimmte t Werte einzusetzen. Für allgemeine Potenzreihen hatten wir das strikt ausgeschlossen, bei Polynomen können wir es zulassen, da der resultierende Ausdruck nur endlich viele Summanden hat.

Lemma 7.36 (Einsetzhomomorphismus)
Es sei K ein Körper und $b \in K$. Die Abbildung

$$\varphi_b : K[t] \longrightarrow K : f \mapsto f(b)$$

ist ein Ringepimorphismus, wobei

$$f(b) := \sum_{k=0}^{n} a_k \cdot b^k \in K$$

für $f = \sum_{k=0}^{n} a_k \cdot t^k \in K[t]$. Wir nennen φ_b Einsetzhomomorphismus*, und für ein konstantes Polynom $f = a_0$ gilt $\varphi_b(f) = a_0$.*

Beweis: Seien zwei Polynome $f = \sum_{k=0}^{n} a_k \cdot t^k$ und $g = \sum_{k=0}^{m} b_k \cdot t^k$ in $K[t]$ gegeben. Wir können ohne Einschränkung annehmen, daß $m = n$ gilt. Dann gilt

$$\begin{aligned}\varphi_b(f+g) = \varphi_b\left(\sum_{k=0}^{n}(a_k+b_k)\cdot t^k\right) &= \sum_{k=0}^{n}(a_k+b_k)\cdot b^k \\ &= \sum_{k=0}^{n} a_k \cdot b^k + \sum_{k=0}^{n} b_k \cdot b^k = \varphi_b(f) + \varphi_b(g)\end{aligned}$$

und

$$\begin{aligned}\varphi_b(f\cdot g) = \varphi_b\left(\sum_{k=0}^{2n}\sum_{i+j=k}(a_i\cdot b_j)\cdot t^k\right) &= \sum_{k=0}^{2n}\sum_{i+j=k}(a_i\cdot b_j)\cdot b^k \\ &= \sum_{k=0}^{n} a_k \cdot b^k \cdot \sum_{k=0}^{n} b_k \cdot b^k = \varphi_b(f)\cdot\varphi_b(g).\end{aligned}$$

Außerdem gilt für ein konstantes Polynom $a_0 \cdot t^0$

$$\varphi_b(a_0 \cdot t^0) = a_0 \cdot b^0 = a_0.$$

Damit gilt aber insbesondere $\varphi_b(1) = 1$, und φ_b ist ein Ringhomomorphismus. Für die Surjektivität beachten wir nur, daß für $a \in K$ automatisch $a = \varphi_b(a \cdot t^0) \in \operatorname{Im}(\varphi_b)$. $\square$

Bemerkung 7.37
Der Umstand, daß φ_b ein Ringhomomorphismus ist, impliziert

$$(f+g)(b) = f(b) + g(b) \quad \text{und} \quad (f \cdot g)(b) = f(b) \cdot g(b).$$

Beachte auch, daß der Beweis von Aufgabe 6.26 a. trotz der etwas allgemeineren Voraussetzungen im wesentlichen identisch ist mit obigem Beweis.

Wir sind nun in der Lage zu definieren, was eine Nullstelle ist.

Definition 7.38
Sei K ein Körper und $b \in K$. b heißt *Nullstelle* von f, falls $f(b) = \varphi_b(f) = 0$.

Proposition 7.39
Sei K *ein Körper und sei* $b \in K$ *eine Nullstelle des Polynoms* $0 \neq g \in K[t]$*, so gibt es ein* $q \in K[t]$ *mit*

$$g = q \cdot (t - b).$$

Wir nennen $t - b$ *einen* Linearfaktor *des Polynoms* g.

Beweis: Division mit Rest 7.27 angewendet auf g und $f = t - b$ liefert die Existenz zweier Polynome $q, r \in K[t]$ mit

$$g = q \cdot f + r$$

und $\deg(r) < \deg(f) = 1$. Aus der Gradbedingung folgt unmittelbar, daß $r = r_0 \cdot t^0$ ein konstantes Polynom ist. Da $\varphi_b(f) = b - b = 0$ und da b eine Nullstelle von g ist, gilt

$$r_0 = \varphi_b(r) = \varphi_b(g - q \cdot f) = \varphi_b(g) - \varphi_b(q) \cdot \varphi_b(f) = 0.$$

Also ist r das Nullpolynom und $g = q \cdot (t - b)$. $\square$

Korollar 7.40
Ist K *ein Körper und* $0 \neq f \in K[t]$ *ein Polynom vom Grad* $\deg(f) \geq 2$*, das eine Nullstelle in* K *besitzt, so ist* f *nicht irreduzibel.*

Beweis: Ist $b \in K$ eine Nullstelle von f, so gibt es wegen Proposition 7.39 ein $q \in K[t]$ mit $f = q \cdot (t - b)$. Aus der Gradformel folgt

$$\deg(q) = \deg(f) - 1 \geq 1,$$

so daß die beiden Faktoren q und $t - b$ beides keine Einheiten in $K[t]$ sind. Also ist f nicht irreduzibel. $\square$

Beispiel 7.41
Wir wollen nun in zwei Beispielen sehen, wie man mit Hilfe von Polynomdivision Linearfaktoren abspalten kann.

a. Sei $f = t^3 + t^2 - 5t - 2 \in \mathbb{Q}[t]$, dann gilt offenbar $f(2) = 8 + 4 - 10 - 2 = 0$. Polynomdivision liefert:

$$
\begin{array}{l}
(t^3 + t^2 - 5t - 2) : (t-2) = t^2 + 3t + 1. \\
\underline{\;t^3 - 2t^2\;} \\
\qquad\;\; 3t^2 - 5t \\
\qquad\;\; \underline{3t^2 - 6t} \\
\qquad\qquad\quad t - 2 \\
\qquad\qquad\quad \underline{t - 2} \\
\qquad\qquad\qquad -
\end{array}
$$

Also gilt $f = (t^2 + 3t + 1) \cdot (t - 2)$ und f ist nicht irreduzibel.

b. Ist $f = t^5 + t^4 + t^3 + t^2 + t + \overline{1} \in \mathbb{Z}_2[t]$, so gilt

$$f\big(\overline{1}\big) = \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{6} = \overline{0} \in \mathbb{Z}_2.$$

Also ist $\overline{1}$ eine Nullstelle von f und f ist nicht irreduzibel. Wir können den Linearfaktor $t - \overline{1}$ mittels Polynomdivision abspalten. Dabei sollte man beachten, daß $\overline{1} = -\overline{1}$ in $\mathbb{Z}_2$, also $t - \overline{1} = t + \overline{1}$:

$$
\begin{array}{l}
\big(t^5 + t^4 + t^3 + t^2 + t + \overline{1}\big) : \big(t + \overline{1}\big) = t^4 + t^2 + \overline{1} \\
\underline{\;t^5 + t^4 \qquad\qquad\qquad\quad\;} \\
\qquad\qquad t^3 + t^2 + t + \overline{1} \\
\qquad\qquad \underline{t^3 + t^2 \qquad\quad\;} \\
\qquad\qquad\qquad\quad t + \overline{1} \\
\qquad\qquad\qquad\quad \underline{t + \overline{1}} \\
\qquad\qquad\qquad\qquad -
\end{array}
$$

Also gilt $f = \big(t^4 + t^2 + \overline{1}\big) \cdot \big(t + \overline{1}\big)$.

Satz 7.42
Ist K *ein Körper und* $0 \neq f \in K[t]$ *ein Polynom, so hat* f *höchstens* $\deg(f)$ *Nullstellen.*

Beweis: Wir überlassen den Beweis dem Leser als Übungsaufgabe.

□

Beispiel 7.43
Das Polynome $f = t^2 + 1$ hat in $\mathbb{R}$ keine Nullstelle, während es in $\mathbb{C}$ die Nullstellen i und $-i$ hat und sich mithin in $\mathbb{C}[t]$ als Produkt von Linearfaktoren schreiben läßt:

$$f = (t - i) \cdot (t + i).$$

Bemerkung 7.44
Durch die Definition der Einsetzhomomorphismen definiert jedes Polynom $f \in K[t]$ eine Funktion

$$P_f : K \longrightarrow K : b \mapsto f(b),$$

die durch f definierte *Polynomfunktion.* Auf diesem Weg erhalten wir eine Abbildung

$$P : K[t] \longrightarrow K^K : f \mapsto P_f$$

von der Menge der Polynome über K in die Menge der Funktionen von K nach K, die einem Polynom seine Polynomfunktion zuordnet. Aus den Eigenschaften des Einsetzhomomorphismus und der Definition der Ringoperationen in K^K (siehe Beispiel 6.3) folgt

$$P_{f+g}(b) = (f+g)(b) = f(b) + g(b) = P_f(b) + P_g(b) = (P_f + P_g)(b)$$

und

$$P_{f\cdot g}(b) = (f \cdot g)(b) = f(b) \cdot g(b) = P_f(b) \cdot P_g(b) = (P_f \cdot P_g)(b).$$

Damit gilt dann aber $P_{f+g} = P_f + P_g$ und $P_{f\cdot g} = P_f \cdot P_g$. Da zudem P_1 die Einsfunktion, d.h. das Einselement von K^K, ist, ist die Abbildung P ein *Ringhomomorphismus*.

Aus der Schule sind Polynome in aller Regel nur als Polynomfunktionen bekannt, und der obige Ringhomomorphismus erlaubt es uns, unsere Polynome als Polynomfunktionen aufzufassen. Im allgemeinen ist es aber nicht richtig, daß zwei *verschiedene* Polynome auch verschiedene Polynomfunktionen definieren! Sei dazu $K = \mathbb{Z}_2$, $f = t^2 + t \in K[t]$ und $g = \overline{0} \cdot t^0 \in K[t]$. Dann gilt

$$f\big(\overline{1}\big) = \overline{1} + \overline{1} = \overline{0} \quad \text{und} \quad f\big(\overline{0}\big) = \overline{0}.$$

Da $K = \{\overline{0}, \overline{1}\}$ nur die zwei Elemente $\overline{0}$ und $\overline{1}$ enthält ist P_f die Nullfunktion, d.h. $P_f = P_g$, obwohl f nicht das Nullpolynom ist, d.h. $f \neq g$.

Ein Polynom ist im allgemeinen nicht festgelegt durch die Polynomfunktion, die es definiert. Etwas mathematischer ausgedrückt, der Ringhomomorphismus P ist im allgemeinen *nicht injektiv*. Der Ärger in obigem Beispiel rührt daher, daß K nur endlich viele Elemente besitzt und daß es somit ein Polynom ungleich 0 geben kann, daß alle diese Elemente als Nullstelle hat.

Ist hingegen K *ein Körper mit unendlich vielen Elemente, so ist* P *injektiv.*

Dazu müssen wir nur zeigen, daß der Kern von P nur das Nullpolynom enthält. Wäre $0 \neq f \in \mathrm{Ker}(P)$, so wäre P_f die Nullfunktion, d.h. jedes Element von K wäre Nullstelle von f. Aus Satz 7.42 würde dann folgen, daß K höchstens $\deg(f)$ Elemente enthält, was im Widerspruch zur Voraussetzung steht, daß $|K| = \infty$.

Arbeitet man mit unendlichen Körper, wie z.B. $K = \mathbb{R}$ oder $K = \mathbb{C}$, dann ist es zulässig, den Polynomring mit seinem Bild unter P in K^K zu identifizieren, d.h. man kann es sich dann erlauben, nicht zwischen Polynomen und Polynomfunktionen zu unterscheiden. □

Wissen über die Existenz von Nullstellen kann hilfreich sein, um festzustellen, ob ein Polynome irreduzibel ist oder nicht.

Aufgabe 7.45 a. Ist K ein Körper und $f \in K[t]$ ein Polynom mit $\deg(f) \in \{2, 3\}$. Zeige, f ist genau dann irreduzibel, wenn f keine Nullstelle hat.

b. Ist $f = t^3 + 3t + 1 \in \mathbb{Z}[t]$ irreduzibel? Falls nicht, schreibe f als Produkt von irreduziblen Polynomen.

c. Ist $f_5 = t^3 + \overline{3} \cdot t + \overline{1} \in \mathbb{Z}_5[t]$ irreduzibel? Falls nicht, schreibe f_5 als Produkt von irreduziblen Polynomen.

Aufgabe 7.46
Beweise Satz 7.42.

Aufgabe 7.47
Zeige, $f = t^2 + t + 1 \in \mathbb{Z}_2[t]$ ist irreduzibel und $K = \mathbb{Z}_2[t]/\langle f \rangle$ ist ein Körper mit 4 Elementen. Stelle die Additions- und Multiplikationstabelle für K auf. Was ist die Charakteristik (siehe Aufgabe 7.21) von K? Ist K isomorph zum Ring $\mathbb{Z}_4$? Ist K isomorph zum Ring $\mathbb{Z}_2 \times \mathbb{Z}_2$ mit komponentenweisen Operationen? Betrachten wir den Polynomring $K[x]$ über K in der Unbestimmten x. Ist das Polynom $g = x^2 + x + \overline{1} \in K[x]$ irreduzibel? Hat g eine Nullstelle in K?

Anmerkung, in dieser Aufgabe wollen wir die Elemente $\overline{0}$ und $\overline{1}$ in $\mathbb{Z}_2$ der Einfachheit halber mit 0 und 1 bezeichnen, wobei $1+1 = 0$ gilt. Das ist deshalb sinnvoll, weil auch die Elemente von $\mathbb{Z}_2[t]/\langle f \rangle$ wieder Restklassen sind, und die doppelten Restklassen (z.B. $\overline{t + \overline{1}}$) für unnötige Verwirrung sorgen.

E) **Hauptidealringe**

In den vorigen Abschnitten haben wir gesehen, daß größte gemeinsame Teiler sowohl in faktoriellen, als auch in euklidischen Integritätsbereichen existieren. Da stellt sich die Frage, ob es einen Zusammenhang zwischen diesen beiden Begriffen gibt. Es gibt ihn, und er führt über die sogenannten Hauptidealringe

Definition 7.48
Ein Integritätsbereich R heißt *Hauptidealring,* wenn jedes Ideal ein Hauptideal ist, d.h. von einem Element erzeugt wird.

In einem Hauptidealring R gibt es also für jedes Ideal I ein Element $a \in I$ so, daß

$$I = \langle a \rangle_R = \{r \cdot a \mid r \in R\}.$$

Einfacher kann ein Ideal nicht mehr sein. Die Elemente in I sind alle Vielfache eines einzigen Elementes a.

Satz 7.49
Jeder euklidische Integritätsbereich ist ein Hauptidealring.

Beweis: Sei $I \trianglelefteq R$ ein beliebiges Ideal. Wir müssen zeigen, daß $I = \langle b \rangle_R$ für ein geeignetes Element $b \in I$. Da das Nullideal von 0 erzeugt wird, können wir $I \neq \{0\}$ annehmen. Wenn $\nu : R \setminus \{0\} \to \mathbb{N}$ eine euklidische Funktion von R bezeichnet, dann wählen wir $0 \neq b \in I$ so, daß $\nu(b)$ minimal wird. Sei nun $0 \neq a \in I$ beliebig, so gibt es $q, r \in R$ so, daß $a = q \cdot b + r$ mit $r = 0$ oder $\nu(r) < \nu(b)$. Aber dann gilt

$$r = a - q \cdot b \in I,$$

da $a \in I$ und $b \in I$. Wegen der Minimalitätsbedingung, der b genügt, muß dann aber $r = 0$ gelten. Also ist $a = q \cdot b \in \langle b \rangle_R$, und somit $I = \langle b \rangle_R$. □

Da wir wissen, daß $\mathbb{Z}$ und Polynomringe über Körpern euklidisch sind, erhalten wir folgende Korollare.

Korollar 7.50
$\mathbb{Z}$ ist ein Hauptidealring.

Korollar 7.51
Ist K ein Körper, so ist der Polynomring $\mathsf{K}[t]$ ein Hauptidealring.

Bemerkung 7.52
Für die ganzen Zahlen war uns diese Aussage bereits vorher bekannt, da wir in Korollar 6.30 die Ideale in $\mathbb{Z}$ als die Untergruppen der additiven Gruppe $\mathbb{Z}$ identifiziert haben, von denen wir bereits aus Proposition 1.38 wußten, daß sie von einem Element erzeugt werden. Schaut man sich den Beweis von Proposition 1.38 an, so stellt man fest, daß er mit dem Beweis von Satz 7.49 identisch ist.

Bemerkung 7.53
Der Ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{ a + b \cdot \frac{1+\sqrt{-19}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

ist ein Hauptidealring, der *nicht* euklidisch ist. Der Beweis dieser Aussage ist mit elementaren Mitteln möglich, ist aber sehr technisch und sprengt den Rahmen dieser Vorlesung. □

Obwohl nicht jeder Hauptidealring euklidisch ist, wollen wir nun zeigen, daß auch in jedem Hauptidealring R größte gemeinsame Teiler existieren. Sind zwei Elemente a und b in R gegeben, so muß das von a und b erzeugte Ideal

$$\langle a, b \rangle_R = \{ r \cdot a + s \cdot b \mid r, s \in R \}$$

nach Voraussetzung auch von einem einzigen Element erzeugt werden können. Ein solcher Erzeuger entpuppt sich als größter gemeinsamer Teiler von a und b.

Satz 7.54 (Bézout Identität)
Sei R ein Hauptidealring und $g, a, b \in R$. Die folgenden Aussagen sind gleichwertig:

a. $g \in \mathrm{ggT}(a, b)$.

b. $\langle g \rangle_R = \langle a, b \rangle_R$.

Insbesondere gibt es für $g \in \mathrm{ggT}(a, b)$ also $r, s \in R$ mit

$$g = r \cdot a + s \cdot b. \tag{41}$$

Man nennt (41) *auch eine* Bézout Identität *des größten gemeinsamen Teilers g von a und b.*

Beweis: Sei $g \in \mathrm{ggT}(a, b)$ und h ein Erzeuger des Ideals $\langle a, b \rangle_R$, so gilt nach Lemma 7.7

$$\langle h \rangle_R = \langle a, b \rangle_R \subseteq \langle g \rangle_R.$$

Aus dem gleichen Lemma folgt dann aber, daß h ein Teiler von a und b ist. Da g ein größter gemeinsamer Teiler ist, folgt notwendig $h \mid g$ und damit

$$\langle a, b\rangle_R = \langle h\rangle_R \supseteq \langle g\rangle_R.$$

Gilt umgekehrt die Gleichung

$$\langle a, b\rangle_R = \langle g\rangle_R,$$

so folgt aus Lemma 7.7 wieder, daß g ein Teiler von a und von b ist. Ist nun h irgend ein Teiler von a und von b, so gilt

$$\langle h\rangle_R \supseteq \langle a, b\rangle_R = \langle g\rangle_R,$$

so daß wiederum h ein Teiler von g ist. Damit ist $g \in \mathrm{ggT}(a, b)$. □

Bemerkung 7.55
Ist R nicht nur ein Hauptidealring, sondern sogar euklidisch, so lassen sich mit Hilfe des Euklidischen Algorithmus auch $r, s \in R$ mit $g = r \cdot a + s \cdot b$ für $g \in \mathrm{ggT}(a, b)$ berechnen. Dazu muß man sich aber die q_i und die r_i der Zwischenschritte merken und Rückeinsetzen. Wir führen dies nur am Beispiel vor.

Es seien $a = 8 \in \mathbb{Z}$ und $b = 3 \in \mathbb{Z}$. Der Euklidische Algorithmus liefert:

$$\begin{aligned} 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

so daß $1 \in \mathrm{ggT}(3, 8)$. Durch Rückeinsetzen erhalten wir dann:

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (8 - 2 \cdot 3) = 3 \cdot 3 + (-1) \cdot 8.$$

Mit Hilfe der Bézout Identität können wir die Einheitengruppe in $\mathbb{Z}_n$ bestimmen, auch wenn n keine Primzahl ist.

Proposition 7.56
Für $0 \neq n \in \mathbb{Z}$ ist

$$\mathbb{Z}_n^* = \{\overline{a} \mid 1 \in \mathrm{ggT}(a, n)\}$$

die Einheitengruppe von $\mathbb{Z}_n$, d.h. eine Nebenklasse $\overline{a} \in \mathbb{Z}_n$ ist invertierbar genau dann, wenn 1 ein größter gemeinsamer Teiler von a und n ist.

Beweis: Sei $\overline{a} \in \mathbb{Z}_n^*$. Dann gibt es ein $\overline{b} \in \mathbb{Z}_n$ mit $\overline{1} = \overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Mithin gilt

$$a \cdot b - 1 \in n\mathbb{Z}$$

ist ein Vielfaches von n. Also gibt es ein $r \in R$ mit

$$a \cdot b - 1 = r \cdot n,$$

und deshalb

$$1 = a \cdot b - r \cdot n \in \langle a, n\rangle_R \subseteq R = \langle 1\rangle_R.$$

Aber damit ist notwendig

$$\langle 1\rangle_R = \langle a, n\rangle_R,$$

und wegen Satz 7.54 ist $1 \in \mathrm{ggT}(a, n)$.

Sei umgekehrt $1 \in \mathrm{ggT}(a, n)$, so gibt es wegen Satz 7.54 $b, r \in R$ mit

$$1 = b \cdot a + r \cdot n,$$

und damit gilt

$$\overline{1} = \overline{b \cdot a + r \cdot n} = \overline{b} \cdot \overline{a} + \overline{r} \cdot \overline{n} = \overline{b} \cdot \overline{a} \in \mathbb{Z}_n,$$

da $\overline{n} = \overline{0}$. Also ist $\overline{a} \in \mathbb{Z}_n^*$ eine Einheit. □

Bemerkung 7.57

Der Beweis von Proposition 7.56 ist konstruktiv, d.h. er sagt uns, wie wir das Inverse von $\overline{a}$ in $\mathbb{Z}_n$ finden können, wenn a und n teilerfremd sind, nämlich mit Hilfe des Euklidischen Algorithmus. Ist $n = 8$ und $a = 3$, so haben wir in Bemerkung 7.55 mittels des Euklidischen Algorithmus folgende Darstellung der 1 bestimmt:

$$1 = 3 \cdot 3 + (-1) \cdot 8.$$

Mithin ist $\overline{3}^{-1} = \overline{3} \in \mathbb{Z}_8$. □

Als nächstes wollen wir zeigen, daß jeder Hauptidealring faktoriell ist, so daß insbesondere auch jeder euklidische Integritätsbereich faktoriell ist. Dazu benötigen wir aber einige Vorbereitungen.

Lemma 7.58

Sei R ein Hauptidealring, $a \in R$ irreduzibel und $b \in R \setminus \langle a \rangle_R$. Dann ist $1 \in \mathrm{ggT}(a, b)$.

Insbesondere gibt es also $r, s \in R$ so, daß $1 = r \cdot a + s \cdot b$.

Beweis: Sei $g \in \mathrm{ggT}(a, b)$. Es reicht zu zeigen, daß g eine Einheit ist. Es gilt $a \in \langle a, b \rangle_R = \langle g \rangle_R$. Folglich gilt $a = c \cdot g$ für ein geeignetes $c \in R$. Da a aber irreduzibel ist, muß entweder c eine Einheit sein oder g. Wäre c eine Einheit, so wäre $\langle a \rangle_R = \langle c \cdot g \rangle_R = \langle g \rangle_R = \langle a, b \rangle_R$ im Widerspruch zur Wahl von $b \notin \langle a \rangle_R$. Also muß g eine Einheit sein. □

Lemma 7.59

Ist R ein Hauptidealring, so ist jedes irreduzible Element prim.

Beweis: Sei dazu $a \in R$ irreduzibel und $a \mid b \cdot c$. Angenommen $a \nmid b$ und $a \nmid c$, d.h. $b \in R \setminus \langle a \rangle_R$ und $c \in R \setminus \langle a \rangle_R$. Dann gibt es nach Lemma 7.58 Elemente $r, s, r', s' \in R$ so, daß

$$1 = r \cdot a + s \cdot b \quad \text{und} \quad 1 = r' \cdot a + s' \cdot c.$$

Mithin gilt

$$a \mid a \cdot (a \cdot r \cdot r' + r \cdot s' \cdot c + r' \cdot s \cdot b) + s \cdot s' \cdot b \cdot c = 1,$$

und a ist eine Einheit im Widerspruch zur Irreduzibilität von a. □

Satz 7.60

Jeder Hauptidealring ist faktoriell.

Beweis: Da nach Lemma 7.59 jedes irreduzible Element prim ist, reicht es zu zeigen daß jedes $0 \neq a \in R \setminus R^*$ Produkt von endlich vielen irreduziblen Elementen ist.

Nehmen wir an es gibt ein Element $0 \neq a_0 \in R \backslash R^*$, welches sich nicht als Produkt von endlich vielen irreduziblen Elementen schreiben läßt. Dann ist a_0 insbesondere nicht selbst irreduzibel. Mithin gibt es Elemente $0 \neq a_1, b_1 \in R \backslash R^*$ so, daß $a_0 = a_1 \cdot b_1$. Da a_0 nicht Produkt von endlich vielen irreduziblen Elementen ist, muß dies ebenfalls für mindestens einen der Faktoren a_1 und b_1 gelten. Wir können ohne Einschränkung annehmen, daß es für a_1 gilt, und erhalten dann

$$\langle a_0 \rangle_R \subsetneqq \langle a_1 \rangle_R,$$

da b_1 keine Einheit ist. Wir können nun mit a_1 auf die gleiche Weise verfahren wie mit a_0, und auf diesem Wege konstruieren wir induktiv eine aufsteigende Kette von Idealen

$$\langle a_0 \rangle_R \subsetneqq \langle a_1 \rangle_R \subsetneqq \langle a_2 \rangle_R \subsetneqq \langle a_3 \rangle_R \subsetneqq \ldots. \tag{42}$$

Betrachten wir nun die Vereinigung

$$I = \bigcup_{i=0}^{\infty} \langle a_i \rangle_R$$

all dieser Ideale, so erhalten wir wieder ein Ideal. Denn sind $b, c \in I$, so gibt es $i, j \in \mathbb{N}$ so, daß $b \in \langle a_i \rangle_R$ und $c \in \langle a_j \rangle_R$. Ohne Einschränkung gilt $i \leq j$ und damit $\langle a_i \rangle_R \subseteq \langle a_j \rangle_R$. Aber dann sind b und c beide in $\langle a_j \rangle_R$ und da dieses ein Ideal ist gilt auch

$$b + c \in \langle a_j \rangle_R \subseteq I.$$

Mithin ist I abgeschlossen bezüglich der Addition. Außerdem gilt

$$r \cdot b \in \langle a_i \rangle_R \subseteq I$$

für $r \in R$. Dies zeigt, daß I in der Tat ein Ideal ist.

Da R ein Hauptidealring ist, ist I ein Hauptideal. Es gibt also ein $s \in R$ so, daß $I = \langle s \rangle_R$. Aber dann gibt es ein $i \in \mathbb{N}$, so daß $s \in \langle a_i \rangle_R$ und folglich

$$\langle a_{i+1} \rangle_R \subseteq I = \langle s \rangle_R \subseteq \langle a_i \rangle_R,$$

im Widerspruch zu (42). □

Bemerkung 7.61

Der Widerspruch im Beweis des obigen Satzes leitet sich aus dem Umstand her, daß es in einem Hauptidealring keine echt aufsteigende Kette von Idealen

$$\langle a_0 \rangle_R \subsetneqq \langle a_1 \rangle_R \subsetneqq \langle a_2 \rangle_R \subsetneqq \langle a_3 \rangle_R \subsetneqq \ldots$$

geben kann. Ringe, in denen jede aufsteigende Kette von Idealen nach endlich vielen Schritten abbrechen muß, nennt man *noethersch*. Hauptidealringe sind also Beispiele für noethersche Ringe. In der kommutativen Algebra werden noethersche Ringe genauer untersucht. □

Aus Satz 7.60 und Korollar 7.51 erhalten wir unmittelbar folgende Resultate.

Korollar 7.62
$\mathbb{Z}$ ist faktoriell.

Eine etwas ausführlichere Fassung dieser Aussage ist der *Fundamentalsatz der elementaren Zahlentheorie*, der unter Berücksichtigung von Bemerkung 7.19 und Bemerkung 7.20 folgt, da $\mathbb{Z}^* = \{1, -1\}$.

Korollar 7.63 (Fundamentalsatz der elementaren Zahlentheorie)
Für jedes $0 \neq z \in \mathbb{Z}$ gibt es eindeutig bestimmte, paarweise verschiedene Primzahlen $p_1, \ldots, p_k$ und eindeutig bestimmte positive ganze Zahlen $n_1, \ldots, n_k \in \mathbb{Z}_{>0}$, so daß

$$z = \operatorname{sgn}(z) \cdot p_1^{n_1} \cdots p_k^{n_k},$$

wobei

$$\operatorname{sgn}(z) := \begin{cases} 1, & z > 0, \\ -1, & z < 0. \end{cases}$$

Bezeichnen wir mit $\mathbb{P}$ die Menge der Primzahlen und führen wir für ein Primzahl $p \in \mathbb{P}$ die Notation

$$n_p(z) = \max\left\{n \in \mathbb{N} \;\middle|\; p^n \mid z\right\}$$

ein, so gilt

$$n_p(z) = \begin{cases} n_i, & p = p_i, \\ 0, & \text{sonst} \end{cases}$$

und

$$z = \operatorname{sgn}(z) \cdot \prod_{p \in \mathbb{P}} p^{n_p(z)}.$$

Man beachte bei der Formulierung im Fundamentalsatz, daß das Produkt $\prod_{p\in\mathbb{P}} p^{n_p(z)}$ zwar unendlich viele Faktoren hat, daß aber nur endlich viele davon ungleich Eins sind. Insofern ist das Produkt definiert, indem man nur die Faktoren ungleich Eins berücksichtigt.

Aus Bemerkung 7.20 erhalten wir folgendes Korollar zur Bestimmung von größten gemeinsamen Teilern und kleinsten gemeinsamen Vielfachen mittels Primfaktorzerlegung.

Korollar 7.64
Es seien $a, b \in \mathbb{Z} \setminus \{0\}$, so gilt

$$\operatorname{ggt}(a, b) = \prod_{p \in \mathbb{P}} p^{\min\{n_p(a), n_p(b)\}}$$

und

$$\operatorname{kgv}(a, b) = \prod_{p \in \mathbb{P}} p^{\max\{n_p(a), n_p(b)\}}.$$

Damit gilt insbesondere

$$|a \cdot b| = \operatorname{kgv}(a, b) \cdot \operatorname{ggt}(a, b).$$

Korollar 7.65
Ist K *ein Körper, so ist* $K[t]$ *faktoriell, d.h. jedes Polynom in* $K[t]$ *besitzt eine im wesentlichen eindeutige Primfaktorzerlegung.*

Beispiel 7.66
Das Polynom $f = t^4 + \overline{3} \cdot t^3 + \overline{2} \in \mathbb{Z}_5[t]$ hat die Primfaktorzerlegung

$$f = \left(t + \overline{1}\right)^2 \cdot \left(t^2 + t + \overline{2}\right).$$

Man beachte dabei, daß $t^2+t+\overline{2}$ nach Aufgabe 7.45 irreduzibel ist, da das Polynom keine Nullstelle in $\mathbb{Z}_5$ besitzt.

Wir haben in Korollar 7.51 gesehen, daß der Polynomring über einem Körper ein Hauptidealring ist. Die Aussage folgender Aufgabe, zeigt, daß die Bedingung an K nicht nur hinreichend, sondern auch notwendig ist.

Aufgabe 7.67
Für einen Integritätsbereich R sind die folgenden Aussagen gleichwertig:

a. R ist ein Körper.

b. $R[t]$ ist ein euklidischer Ring.

c. $R[t]$ ist ein Hauptidealring.

Aufgabe 7.68
Es sei K ein Körper und $I \lhd K[[t]]$ ein Ideal mit $I \neq \{0\}$ und $I \neq K[[t]]$. Zeige, es gibt ein $n \geq 1$ mit $I = \langle t^n \rangle_{K[[t]]}$. Ist $K[[t]]$ faktoriell?

F) **Der chinesische Restsatz**

Wir wollen in diesem Abschnitt folgende Frage beantworten. Gibt es Polynome $f, g \in \mathbb{Z}[t] \setminus \mathbb{Z}^*$, so daß

$$h := t^4 + 6t^3 + 17t^2 + 24t + 27 = f \cdot g,$$

d.h. ist h nicht irreduzibel in $\mathbb{Z}[t]$? Wir beachten zunächst, daß für die Leitkoeffizienten von f und g notwendig

$$\operatorname{lc}(f) \cdot \operatorname{lc}(g) = \operatorname{lc}(f \cdot g) = 1$$

gilt, so daß wir ohne Einschränkung $\operatorname{lc}(f) = 1 = \operatorname{lc}(g)$ annehmen können.

Wir gehen das Problem nun durch *Reduktion des Polynoms* h *modulo einer Primzahl* p an, d.h. wir betrachten das Bild von h unter der Abbildung

$$\phi_p : \mathbb{Z}[t] \longrightarrow \mathbb{Z}_p[t] : \sum_{k=0}^{n} a_k \cdot t^k \mapsto \sum_{k=0}^{n} \overline{a_k} \cdot t^k.$$

Nach Aufgabe 6.41 diese Abbildung ist ein Ringhomomorphismus, so daß die Gleichung $h = f \cdot g$ notwendig zu

$$\phi_p(h) = \phi_p(f) \cdot \phi_p(g)$$

führt.

In obigem Beispiel betrachten wir h modulo der Primzahlen 2 und 7, und erhalten

$$\begin{aligned}\phi_2(h) &= t^4 + \overline{6}\cdot t^3 + \overline{17}\cdot t^2 + \overline{24}\cdot t + \overline{27}\\ &= t^4 + t^2 + \overline{1} = \left(t^2 + t + \overline{1}\right)^2 \in \mathbb{Z}_2[t]\end{aligned}$$

und

$$\begin{aligned}\phi_7(h) &= t^4 + \overline{6}\cdot t^3 + \overline{17}\cdot t^2 + \overline{24}\cdot t + \overline{27}\\ &= t^4 + \overline{6}\cdot t^3 + \overline{3}\cdot t^2 + \overline{3}\cdot t + \overline{6}\\ &= \left(t^2 + \overline{5}\cdot t + \overline{2}\right)\cdot\left(t^2 + t + \overline{3}\right) \in \mathbb{Z}_7[t].\end{aligned}$$

Die Faktorisierung von $\phi_2(h)$ in $\mathbb{Z}_2[t]$ und von $\phi_7(h)$ in $\mathbb{Z}_7[t]$ erhält man, indem man die Produkte aller Paare zweier Polynome vom Grad höchstens drei durchprobiert, deren Grade sich zu vier addieren. Da es nur endlich viele sind, ist das kein wirkliches Problem, obwohl es durchaus etwas Zeit in Anspruch nimmt, wenn man das von Hand tun will. Die gefundenen Faktoren von $\phi_2(h)$ und von $\phi_7(h)$ sind irreduzibel nach Aufgabe 7.45, da sie jeweils Grad zwei haben, ohne eine Nullstelle zu besitzen. Letzteres ist wieder ein einfacher Test in $\mathbb{Z}_2$ bzw. in $\mathbb{Z}_7$.

Wenn es also Polynome f und g wie oben gibt, so müssen sie notwendig beide Grad zwei haben, d.h.

$$f = t^2 + b_1\cdot t + b_0 \quad \text{und} \quad g = t^2 + c_1\cdot t + c_0,$$

und ferner muß für die Reduktion modulo 2 bzw. 7 gelten

$$\phi_2(f) = \phi_2(g) = t^2 + t + \overline{1}$$

sowie ohne Einschränkung

$$\phi_7(f) = t^2 + \overline{5}\cdot t + \overline{2} \quad \text{und} \quad \phi_7(g) = t^2 + t + \overline{3}.$$

Wir suchen also Zahlen $b_0, b_1, c_0, c_1 \in \mathbb{Z}$ die folgende Kongruenzgleichungssysteme erfüllen:

$$\begin{aligned} b_0 &\equiv 1 \pmod 2\\ b_0 &\equiv 2 \pmod 7\end{aligned} \tag{43}$$

$$\begin{aligned} b_1 &\equiv 1 \pmod 2\\ b_1 &\equiv 5 \pmod 7\end{aligned} \tag{44}$$

$$\begin{aligned} c_0 &\equiv 1 \pmod 2\\ c_0 &\equiv 3 \pmod 7\end{aligned} \tag{45}$$

$$\begin{aligned} c_1 &\equiv 1 \pmod 2\\ c_1 &\equiv 3 \pmod 7\end{aligned} \tag{46}$$

Sind wir in der Lage, ein Kongruenzgleichungssystem wie (43) zu lösen? Die Antwort darauf gibt der chinesische Restsatz, ein algorithmisches Verfahren zur Lösung solcher Kongruenzgleichungssysteme, das in China bereits im 3. Jahrhundert bekannt war.

Die folgenden Lemmata sind wichtige Bausteine für den Beweis des chinesischen Restsatzes.

Lemma 7.69
Seien $n_1, \ldots, n_r \in \mathbb{Z} \setminus \{0\}$ *paarweise teilerfremd und sei* $N_i = \frac{n_1 \cdots n_r}{n_i}$.
Dann sind n_i *und* N_i *teilerfremd und* $\overline{N_i} \in \mathbb{Z}_{n_i}^*$ *für* $i \in \{1, \ldots, n\}$.

Beweis: Sei $i \in \{1, \ldots, r\}$ gegeben. Für $j \neq i$ sind n_i und n_j teilerfremd. Dies bedeutet $1 \in \mathrm{ggT}(n_i, n_j)$, und wegen der Bézout Identität existieren mithin $s_j, r_j \in R$ so, daß

$$1 = n_i \cdot r_j + n_j \cdot s_j.$$

Wenn wir j alle Indizes von 1 bis r außer i durchlaufen lassen, so können wir die Zahl 1 in folgender Weise als Produkt von $r-1$ Faktoren schreiben:

$$1 = \prod_{j \neq i} 1 = \prod_{j \neq i} (n_i \cdot r_j + n_j \cdot s_j). \tag{47}$$

Multiplizieren wir das Produkt auf der rechten Seite aus, so erhalten wir eine Summe, in der bis auf einen einzigen Term jeder Term n_i als Faktor enthält. Der eine Term, der n_i nicht als Faktor hat, ist

$$\prod_{j \neq i} (n_j \cdot s_j) = N_i \cdot \prod_{j \neq i} s_j.$$

Spalten wir n_i von den verbleibenden Termen ab, so erhalten wir eine Zahl $z \in \mathbb{Z}$, so daß (47) folgende Form annimmt:

$$1 = n_i \cdot z + N_i \cdot \prod_{j \neq i} s_j \in \langle n_i, N_i \rangle_{\mathbb{Z}}.$$

Aber damit gilt $\langle n_i, N_i \rangle_{\mathbb{Z}} = \langle 1 \rangle_{\mathbb{Z}}$ und wegen Satz 7.54 ist $1 \in \mathrm{ggT}(n_i, N_i)$, d.h. n_i und N_i sind teilerfremd. Aus Proposition 7.56 folgt schließlich, daß N_i eine Einheit in $\mathbb{Z}_{n_i}$ ist. □

Lemma 7.70
Sind $n_1, \ldots, n_r \in \mathbb{Z} \setminus \{0\}$ *paarweise teilerfremd und* $a \in \mathbb{Z} \setminus \{0\}$ *mit* $n_i \mid a$ *für* $i = 1, \ldots, r$*, so gilt:*

$$n_1 \cdots n_r \mid a.$$

Beweis: Wir führen den Beweis durch Induktion über r, wobei die Aussage für $r = 1$ trivialerweise erfüllt ist. Wir können also $r \geq 2$ annehmen.

Mit der Notation von Lemma 7.69 gilt dann nach Induktionsvoraussetzung

$$N_r = n_1 \cdots n_{r-1} \mid a.$$

Mithin gibt es ganze Zahlen $b, c \in \mathbb{Z}$ mit $a = n_r \cdot b$ und $a = N_r \cdot c$. Da nach Lemma 7.69 zudem n_r und N_r teilerfremd sind, liefert die Bézout Identität ganze Zahlen $x, y \in \mathbb{Z}$ mit

$$x \cdot n_r + y \cdot N_r = 1.$$

Kombinieren wir die drei Gleichungen, so erhalten wir:

$$\begin{aligned} a = a \cdot (x \cdot n_r + y \cdot N_r) &= a \cdot x \cdot n_r + a \cdot y \cdot N_r \\ &= N_r \cdot c \cdot x \cdot n_r + n_r \cdot b \cdot y \cdot N_r = n_r \cdot N_r \cdot (c \cdot x + b \cdot y). \end{aligned}$$

Mithin wird a von $N_r \cdot n_r = n_1 \cdots n_r$ geteilt. □

Satz 7.71 (Chinesischer Restsatz)
Seien $n_1, \ldots, n_r \in \mathbb{Z} \setminus \{0\}$ *paarweise teilerfremd,* $N = n_1 \cdots n_r$ *und* $N_i = \frac{N}{n_i}$.

a. *Zu beliebig vorgegebenen ganzen Zahlen* $a_1, \ldots, a_r \in \mathbb{Z}$ *existiert eine Lösung* $x \in \mathbb{Z}$ *des* Kongruenzgleichungssystems

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_r \pmod{n_r}. \end{aligned} \tag{48}$$

b. *Ist* $\overline{x_i} = \overline{N_i}^{-1} \in \mathbb{Z}_{n_i}$ *für* $i = 1, \ldots, r$, *so ist*

$$x' = \sum_{i=1}^{r} N_i \cdot x_i \cdot a_i \in \mathbb{Z} \tag{49}$$

eine Lösung von (48).

c. *Genau dann ist* $x'' \in \mathbb{Z}$ *eine Lösung von* (48), *wenn* x'' *sich von* x' *nur um ein Vielfaches von* N *unterscheidet. Insbesondere ist die Lösung von* (48) *modulo* N *eindeutig bestimmt.*

Beweis: Wir zeigen zunächst, daß x' eine Lösung von (48) ist und beweisen damit a. und b.. Nach Lemma 7.69 existiert für $i = 1, \ldots, r$ ein $x_i \in \mathbb{Z}$ mit $\overline{x_i} = \overline{N_i}^{-1} \in \mathbb{Z}_{n_i}$. Wir können deshalb

$$x' := \sum_{j=1}^{r} N_j \cdot x_j \cdot a_j$$

betrachten. Wegen $n_i \mid N_j$ für $j \neq i$ gilt aber in $\mathbb{Z}_{n_i}$ die Gleichung

$$\overline{x'} = \sum_{j=1}^{r} \overline{N_j} \cdot \overline{x_j} \cdot \overline{a_j} = \overline{N_i} \cdot \overline{x_i} \cdot \overline{a_i} = \overline{a_i} \in \mathbb{Z}_{n_i},$$

d.h.

$$x' \equiv a_i \pmod{n_i}.$$

Es bleibt also zu zeigen, daß $x' + N\mathbb{Z}$ die Menge der Lösungen von (48) ist. Sei $x'' \in \mathbb{Z}$ eine beliebige Lösung von (48). Dann gilt für $i = 1, \ldots, r$

$$x' - a_i, x'' - a_i \in n_i\mathbb{Z}.$$

Damit gilt aber $x' - x'' \in n_i\mathbb{Z}$, d. h. $n_i \mid (x' - x'')$, für alle $i = 1, \ldots, r$. Aus Lemma 7.70 folgt dann $N \mid (x' - x'')$, d. h. $x' - x'' \in N\mathbb{Z}$, und damit

$$x' \equiv x'' \pmod{N}.$$

Ist umgekehrt $x'' = x' + N \cdot z$ für ein $z \in \mathbb{Z}$, so gilt $N \mid x' - x''$ und damit $n_i \mid x' - x''$ für alle $i = 1, \ldots, r$. Da wir bereits wissen, daß $x' \equiv a_i \pmod{n_i}$ gilt, d.h. $n_i \mid x' - a_i$, so folgt

$$n_i \mid \big((x' - a_i) - (x' - x'')\big) = (x'' - a_i),$$

d.h. $x'' \equiv a_i \pmod{n_i}$ für alle $i = 1, \ldots, r$. Also ist x'' dann auch eine Lösung von (48). □

Bemerkung 7.72
Da wir das Inverse von $\overline{N_i}$ in $\mathbb{Z}_{n_i}$ mit Hilfe des Euklidischen Algorithmus berechnen können (siehe Bemerkung 7.57), sind wir auch in der Lage ein Kongruenzgleichungssystem der Form (48) mit Hilfe der Formel (49) zu lösen.

In Anwendungen werden die n_i meist paarweise verschiedene Primzahlen sein, wie in dem Eingangsbeispiel des Abschnitts.

Man kann die Aussage des chinesischen Restsatzes auch etwas algebraischer formulieren, wenn man das karthesische Produkt

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r}$$

mit komponentenweiser Addition und Multiplikation als kommutativen Ring mit Eins betrachtet. Diese algebraische Formulierung wird in der Vorlesung Elementare Zahlentheorie eine wichtige Rolle spielen.

In folgendem Korollar werden wir die Restklasse von x in $\mathbb{Z}_m$ ausnahmsweise mit $\overline{x}_m$ statt mit $\overline{x}$ bezeichnen, um deutlich zu machen, in welchem Ring sie lebt.

Korollar 7.73 (Chinesischer Restsatz)
Es seien $n_1, \ldots, n_r \in \mathbb{Z}_{>0}$ paarweise teilerfremde positive Zahlen, dann ist die Abbildung

$$\overline{\alpha} : \mathbb{Z}_{n_1 \cdots n_r} \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r} : \overline{x}_{n_1 \cdots n_r} \mapsto \big(\overline{x}_{n_1}, \ldots, \overline{x}_{n_r}\big)$$

ein Isomorphismus kommutativer Ringe mit Eins.

Ferner ist die induzierte Abbildung

$$\mathbb{Z}^*_{n_1 \cdots n_r} \longrightarrow \mathbb{Z}^*_{n_1} \times \ldots \times \mathbb{Z}^*_{n_r} : \overline{x}_{n_1 \cdots n_r} \mapsto \big(\overline{x}_{n_1}, \ldots, \overline{x}_{n_r}\big)$$

ein Isomorphismus der Einheitengruppen der Ringe.

Beweis: Die Abbildung

$$\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r} : x \mapsto \big(\overline{x}_{n_1}, \ldots, \overline{x}_{n_r}\big)$$

ist offensichtlich ein Ringhomomorphismus. Der Chinesische Restsatz 7.71 besagt nun, daß α surjektiv ist mit

$$\mathrm{Ker}(\alpha) = \langle n_1 \cdots n_r \rangle_{\mathbb{Z}}.$$

Die erste Behauptung folgt dann mit dem Homomorphiesatz 4.51.

Da ein Isomorphismus von Ringen Einheiten auf Einheiten abbildet, gilt

$$\overline{\alpha}\big(\mathbb{Z}^*_{n_1\cdots n_r}\big) = (\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r})^* = \mathbb{Z}^*_{n_1} \times \ldots \times \mathbb{Z}^*_{n_r},$$

wobei die letzte Gleichheit aus Beispiel 6.4 folgt. Da die Abbildung $\overline{\alpha}$ die Multiplikation respektiert, induziert sie somit einen Gruppenisomorphismus der multiplikativen Gruppen. □

Beispiel 7.74
Wir wollen nun die Kongruenzgleichungssysteme (43), (44), (45) und (46) lösen. Ersteres hat die Form:

$$\begin{aligned} b_0 &\equiv 1 \pmod{2} \\ b_0 &\equiv 2 \pmod{7} \end{aligned}$$

Dabei ist in der Notation des chinesischen Restsatzes $n_1 = N_2 = 2$, $n_2 = N_1 = 7$, $a_1 = 1$ und $a_2 = 2$. Auch ohne den Euklidischen Algorithmus anzuwenden sehen wir

$$1 = 4 \cdot 2 + (-1) \cdot 7.$$

Mithin gilt $\overline{x_1} = \overline{1} = \overline{-1} = \overline{N_1}^{-1} \in \mathbb{Z}_2$ und $\overline{x_2} = \overline{4} = \overline{N_2}^{-1} \in \mathbb{Z}_7$. Die gesuchte Lösung b_0 läßt sich bis auf ein Vielfaches von $N = 2 \cdot 7 = 14$ mithin beschreiben als

$$b_0 \equiv x_1 \cdot N_1 \cdot a_1 + x_2 \cdot N_2 \cdot a_2 = 1 \cdot 7 \cdot 1 + 4 \cdot 2 \cdot 2 = 23 \equiv 9 \pmod{14}.$$

Für die verbleibenden drei Kongruenzgleichungssysteme bleiben die $\overline{n_i}$, $\overline{N_i}$ und $\overline{x_i}$ unverändert, und nur die a_i werden ausgetauscht, so daß wie die Lösungen modulo $N = 14$ unmittelbar angeben können:

$$b_1 \equiv x_1 \cdot N_1 \cdot 1 + x_2 \cdot N_2 \cdot 5 = 1 \cdot 7 \cdot 1 + 4 \cdot 2 \cdot 5 = 47 \equiv 5 \pmod{14},$$

$$c_0 \equiv x_1 \cdot N_1 \cdot 1 + x_2 \cdot N_2 \cdot 3 = 1 \cdot 7 \cdot 1 + 4 \cdot 2 \cdot 3 = 31 \equiv 3 \pmod{14}$$

und

$$c_1 \equiv x_1 \cdot N_1 \cdot 1 + x_2 \cdot N_2 \cdot 5 = 1 \cdot 7 \cdot 1 + 4 \cdot 2 \cdot 3 = 31 \equiv 3 \pmod{14}.$$

Wüßten wir aus irgendwelchen Zusatzüberlegungen bereits, daß die Koeffizienten zwischen 0 und 13 zu liegen, so könnten wir die Polynome f und g mit Gewissheit angeben, nämlich

$$f = t^2 + b_1 \cdot t + b_0 = t^2 + 5t + 9$$

und

$$g = t^2 + c_1 \cdot t + c_0 = t^2 + 3t + 3.$$

Da dies nicht der Fall ist, bleibt uns nur, unser Ergebnis zu testen, und in der Tat gilt

$$f \cdot g = (t^2 + 5t + 9) \cdot (t^2 + 3t + 3) = t^4 + 6t^3 + 17t^2 + 24t + 27 = h.$$

□

Bemerkung 7.75
Das in der Einleitung zu diesem Abschnitt angegebene und in Beispiel 7.74 fortgeführte Beispiel, wie man die Zerlegung eines Polynoms in $\mathbb{Z}[t]$ in irreduzible Faktoren erreichen kann, funktioniert nicht nur zufällig. Es gibt Sätze, die es erlauben, aus den Koeffizienten des Polynoms h die Größe der Koeffizienten potenzieller Teiler von h abzuschätzen. Wählt man nun hinreichend viele paarweise verschiedene Primzahlen, so daß deren Produkt größer als diese Schranke ist, so kann man im wesentlichen in der angegebenen Weise die Zerlegung von f in irreduzible Polynome in $\mathbb{Z}[t]$ bestimmen. Wenn man dann noch ein weiteres Resultat verwendet, welches sagt, daß ein in $\mathbb{Z}[t]$ irreduzibles Polynom auch in $\mathbb{Q}[t]$ irreduzibel ist, so kann man auf diesem Weg Polynome in $\mathbb{Q}[t]$ in Primfaktoren zerlegen, indem man zunächst den Hauptnenner der Koeffizienten ausklammert.

Man beachte, daß es für die Polynomringe $\mathbb{R}[t]$ und $\mathbb{C}[t]$ kein derartiges Verfahren gibt, was einer der wesentlichen Gründe für die Notwendigkeit numerischer Verfahren ist. □

Wir wollen das Kapitel mit einem etwas längeren Beispiel zum chinesischen Restsatz abschließen.

Beispiel 7.76
Gegeben sei das folgende Kongruenzgleichungssystem:

$$\begin{aligned} x &\equiv a_1 = 1 \pmod{2}, \\ x &\equiv a_2 = 2 \pmod{3}, \\ x &\equiv a_3 = 4 \pmod{7}. \end{aligned}$$

Es sind $n_1 = 2, n_2 = 3, n_3 = 7$ paarweise teilerfremd, und $N = 2 \cdot 3 \cdot 7 = 42$, $N_1 = 21$, $N_2 = 14$ und $N_3 = 6$.

Die Berechnung der Inversen von $\overline{N_i}$ in $\mathbb{Z}_{n_i}$ geschieht mit Hilfe des Euklidischen Algorithmus. Da n_i und N_i teilerfremd sind, gilt wegen der Bézout Identität

$$x_i N_i + y_i n_i = 1$$

für geeignete $x_i \in \mathbb{Z}$ (und $y_i \in \mathbb{Z}$, die hier nicht interessieren):

$$\overline{x_1} = \overline{21}^{-1} = \overline{1}^{-1} = \overline{1} \in \mathbb{Z}_2,$$

$$\overline{x_2} = \overline{14}^{-1} = \overline{2}^{-1} = \overline{2} \in \mathbb{Z}_3,$$

und

$$\overline{x_3} = \overline{6}^{-1} = \overline{6} \in \mathbb{Z}_7.$$

Es folgt:

$$\begin{aligned} x &\equiv N_1 \cdot x_1 \cdot a_1 + N_2 \cdot x_2 \cdot a_2 + N_3 \cdot x_3 \cdot a_3 \\ &= 21 \cdot 1 \cdot 1 + 14 \cdot 2 \cdot 2 + 6 \cdot 4 \cdot 6 = 221 \equiv 11 \pmod{42}. \end{aligned}$$

Also ist $x = 11$ die modulo 42 eindeutig bestimmte Lösung, und die Menge aller Lösungen ist

$$\{11 + z \cdot 42 \mid z \in \mathbb{Z}\}.$$

$\square$

Bemerkung 7.77
Die Voraussetzung des chinesischen Restsatzes, daß die n_i paarweise teilerfremd sein sollen, ist nicht nur für unseren Beweis notwendig. Ohne diese Voraussetzung ist die Aussage im allgemeinen falsch, wie folgendes Beispiel zeigt: $n_1 = 2$, $n_2 = 4$, $a_1 = 0$, $a_2 = 1$, dann impliziert $x \equiv a_1 \pmod 2$, daß x eine gerade Zahl ist, während $x \equiv a_2 \pmod 4$ nur für eine ungerade Zahl möglich ist. Es kann also keine ganze Zahl x geben, die beide Kongruenzgleichungen zugleich erfüllt, was daran liegt, daß $n_1 = 2$ und $n_2 = 4$ nicht teilerfremd sind.

Wir wollen das Vorlesungsskript mit der alten Erkenntnis abschließen, daß Primzahlen keine Seltenheit sind.

Satz 7.78 (Euklid)
Es gibt unendlich viele Primzahlen in $\mathbb{Z}$.

Beweis: Da 2 eine Primzahl ist, gibt es eine Primzahl. Nehmen wir nun an, daß es nur endlich viele Primzahlen $p_1, \ldots, p_r \in \mathbb{Z}$ gibt, und betrachten wir die Zahl

$$z = p_1 \cdots p_r + 1 > 1.$$

Aufgrund des Fundamentalsatzes der elementaren Zahlentheorie besitzt z eine Primfaktorzerlegung und es muß mithin mindestens eine Primzahl geben, die z teilt. D.h. es gibt ein i so, daß $p_i \mid z$. Aber dann gilt auch

$$p_i \mid z - p_1 \cdots p_r = 1,$$

was nur möglich ist, wenn p_i eine Einheit ist. Letzteres steht im Widerspruch zur Voraussetzung, daß p_i eine Primzahl ist.

Dies zeigt, daß es unendlich viele Primzahlen geben muß. $\square$

Anhang A Grundlegende Begriffe aus der Logik

Die Mathematik verwendet die *axiomatische Methode*, d. h. gewisse Aussagen nennt man *Axiome*. Mit den Regeln der *Logik* werden daraus neue, wahre Aussagen gewonnen. Viele Bemühungen der Mathematik sind darauf gerichtet, in den unterschiedlichen Erscheinungsformen gemeinsame einfache *Strukturen* und Prinzipien zu finden und diese axiomatisch zu fassen. Die Mathematik läßt sich aber nicht auf Logik reduzieren. Mathematik ist wesentlich mehr, als nur aus wahren Aussagen andere wahre Aussagen korrekt zu folgern. Die Mathematik ist eine äußerst kreative Wissenschaft, die ständig neue Strukturen schafft, deren große Bedeutung sich manchmal erst viel später erschließt. Die Mathematik hat ihre gesellschaftliche Relevanz über Jahrtausende bewiesen, und zwar nicht durch korrektes logisches Schließen, sondern durch die Schaffung von *wichtigen* Strukturen. Was wichtig ist, wird nicht durch Logik entschieden, sondern über einen historisch längeren Zeitraum und in einem komplexeren Rückkoppelungsprozeß mit der Realität.

Natürlich ist korrektes logisches Schließen die Grundlage jeder mathematischen Argumentation. Jeder weiß, wie oft in der Umgangssprache etwa die doppelte Verneinung falsch verwendet wird. Das darf in mathematischen Beweisen auf gar keinen Fall passieren. Das korrekte Verneinen sollte deshalb besonders geübt werden.

Einige Begriffe und Notationen, die zum täglichen mathematischen Handwerkszeug gehören, werden jetzt eingeführt.

Definition A.1
Es seien A und B Aussagen, so lassen sich daraus durch folgende Operationen neue Aussagen gewinnen:

Name	**Symbol**	**Bedeutung**
Konjunktion	$\mathsf{A} \wedge \mathsf{B}$	"A und B"; sowohl A als auch B
Disjunktion	$\mathsf{A} \vee \mathsf{B}$	"A oder B" (oder beides); nicht-ausschließendes Oder
Negation	$\neg\mathsf{A}$	"nicht A"
Implikation	$\mathsf{A} \Rightarrow \mathsf{B}$	"aus A folgt B"; "A impliziert B"; in der Bedeutung $(\neg\mathsf{A}) \vee \mathsf{B}$
Äquivalenz	$\mathsf{A} \Leftrightarrow \mathsf{B}$	"A ist äquivalent zu B"; " A ist gleichbedeutend zu B"; in der Bedeutung $(\mathsf{A} \Rightarrow \mathsf{B}) \wedge (\mathsf{B} \Rightarrow \mathsf{A})$

Bemerkung A.2
Man beachte, daß der *Schluß* "aus A folgt B" für jede Aussage B richtig ist, wenn A falsch ist. Das folgt aus der Definition von "$\Rightarrow$". Mit der Wahrheit von B hat die Richtigkeit der *Schlußweise* nichts zu tun!

Beispiel A.3
Hier nun einige mathematische Aussagen.

A. Jede gerade Zahl ist Summe zweier ungerader Zahlen.

B. Es gibt unendlich viele Primzahlen.

C. Jede gerade Zahl größer zwei ist Summe zweier Primzahlen.

D. Zu jedem Kreis läßt sich, nur mit Zirkel und Lineal, ein Quadrat konstruieren, das den gleichen Flächeninhalt hat.

E. Die Gleichung $x^n + y^n = z^n$ besitzt für $n > 2$ keine Lösung mit positiven ganzen Zahlen x, y, z.

F. Gegeben sei eine Familie nicht-leerer Mengen. Dann läßt sich aus jeder der Mengen ein Element auswählen.

Die Aussage A ist offensichtlich wahr, und auch die Aussage B ist richtig, allerdings ist dies keine triviale Aussage. Sie muß bewiesen werden. Die Aussage C ist die bekannte *Goldbachsche Vermutung* aus dem Jahre 1742. Sie ist bis heute weder bewiesen noch widerlegt.

Die Aussage D ist unter dem Begriff *Quadratur des Kreises* bekannt. Sie ist falsch, was sich daraus ableiten läßt, daß die Kreiszahl π transzendent ist (Lindemann 1882). Umgangssprachlich sollte man also die Quadratur des Kreises nicht als Synonym für etwas extrem Schwieriges verwenden, sondern für etwas Unmögliches.

Die Aussage E hat jahrhundertelang als *Fermatsche Vermutung* die Mathematiker beschäftigt. Sie wurde erst 1995 von dem englischen Mathematiker Wiles als wahr nachgewiesen. Für den Beweis wurden modernste und tiefste mathematische Methoden verwendet.

Die Aussage F, möchte man meinen, ist offensichtlich wahr, eher noch als Aussage A. In gewissem Sinne ist diese Aussage jedoch weder beweisbar noch widerlegbar. Sie ist im Axiomensystem der Mengenlehre von Zermelo und Fraenkel unabhängig von den anderen Axiomen. In der Tat kann man die Aussage F, die als *Auswahlaxiom* bezeichnet wird, als Axiom der Mengenlehre zulassen (was wir, wie die überwiegende Zahl der Mathematiker, tun wollen) oder auch nicht. Da das Auswahlaxiom, wenn überhaupt, so nur für überabzählbare Mengen strittig ist, sind Zustimmung oder Ablehnung kaum von praktischer Relevanz.

Soweit zu einigen interessanten mathematischen Aussagen. Mit den Mitteln der Logik erhalten wir, daß die nächste Aussage wahr und die übernächste Aussage falsch ist.

Beispiel A.4 G. Die Aussage A oder die Aussage D ist wahr. ($A \vee D$)

H. Die Aussagen A und D sind wahr. ($A \wedge D$)

Beispiel A.5
Ein typischer Gebrauch des mathematischen “oder” findet sich bei der Multiplikation

von ganzen Zahlen a, b:

$$a \cdot b = 0 \;\Rightarrow\; a = 0 \vee b = 0.$$

Natürlich können beide Zahlen null sein.

Neben Aussagen, die wahr oder falsch sein können, sind *Aussagefunktionen* oder *Prädikate* wichtig, die erst dann wahr oder falsch werden, wenn spezielle Werte eingesetzt werden.

Beispiel A.6
So ist etwa für ganze Zahlen a und b die Aussage $a > b$ erst dann wahr oder falsch, wenn konkrete Zahlen eingesetzt werden, z. B. $42 > 37$.

Aussagefunktionen werden in der Praxis häufig mit *Quantoren* gebraucht.

Definition A.7
$\forall$ oder $\bigvee$: "für alle".
$\exists$ oder $\bigwedge$: "es gibt".
Ist P eine Aussagefunktion, so bedeutet:
$\forall\, x : P(x)$: "für alle x gilt $P(x)$",
$\exists\, x : P(x)$: "es gibt ein x, so daß $P(x)$ gilt".

Beispiel A.8

$$\forall\, x, \forall\, y, \forall\, z, \forall\, n \;:\; n > 2 \Rightarrow x^n + y^n \neq z^n.$$

Dies ist für positive natürliche Zahlen x, y, z und n die Fermatsche Vermutung.

Bemerkung A.9
Wichtig ist das richtige Verneinen einer Aussage.

$$\neg\big(\forall\, x \;:\; P(x)\big) \;\Leftrightarrow\; \exists\, x \;:\; \big(\neg P(x)\big).$$

Die Verneinung der Aussage "für alle x gilt die Aussage $P(x)$" ist gleichbedeutend mit "es gibt ein x, für das die Aussage $P(x)$ nicht gilt".

$$\neg\big(\exists\, x \;:\; P(x)\big) \;\Leftrightarrow\; \forall\, x \;:\; \big(\neg P(x)\big).$$

Die Verneinung der Aussage "es gibt ein x, für das die Aussage $P(x)$ gilt" ist gleichbedeutend mit "für alle x gilt die Aussage $P(x)$ nicht" bzw. mit "für kein x gilt die Aussage $P(x)$".

$$(A \Rightarrow B) \;\Leftrightarrow\; (\neg B \Rightarrow \neg A).$$

Die Aussage "aus A folgt B" ist gleichbedeutend mit "aus nicht B folgt nicht A". Letzteres bezeichnet man auch als *Kontraposition* von ersterem.

Notation A.10
Als Notation haben sich "," sowie "und" anstelle von "$\bigwedge$" eingebürgert, und "oder" statt "$\bigvee$" sowie "nicht" statt "$\neg$".

Anhang B Abbildungen und Mengen

Der folgende "naive" Mengenbegriff des deutschen Mathematikers Cantor (1845-1918) ist praktisch für alle Zwecke der Mathematik ausreichend. Danach ist eine *Menge* eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens. Die Objekte heißen *Elemente* der Menge.

Wir führen nun einige wichtige Symbole und Konstruktionen im Zusammenhang mit Mengen ein.

Definition B.1
Es seien M, N, I, M_i ($i \in$ I) Mengen, P eine Aussagefunktion.

$\{x_1, \ldots, x_n\}$	: Menge aus den (verschiedenen) Elementen $x_1, \ldots, x_n$
	: z. B. $\{1,1\} = \{1\}$, $\{1,2,3\} = \{3,1,2\}$;
$x \in M$	: x ist *Element* der Menge M;
$x \notin M$	: x ist *nicht Element* der Menge M;
$\{x \in M \mid P(x)\}$	: Menge aller Elemente $x \in M$, für die die Aussage $P(x)$ gilt;
$\emptyset$ oder $\{\,\}$	: *leere Menge*, die Menge, die keine Elemente enthält;
$M \subset N$ oder $M \subseteq N$	: M ist *Teilmenge* von N, d. h. jedes Element von M ist auch Element von N, d. h. $x \in M \;\Rightarrow\; x \in N$;
$M = N$	: $M \subseteq N$ und $N \subseteq M$;
$M \neq N$	: $\neg(M = N)$;
$M \subsetneqq N$	: $M \subseteq N$ und $M \neq N$;
$M \cap N$	: *Durchschnitt* der Mengen M und N, d. h. $M \cap N = \{x \mid x \in M \;\wedge\; x \in N\}$;
$\bigcap\limits_{i \in I} M_i$	: Durchschnitt aller Mengen M_i mit $i \in I$, wobei I als *Indexmenge* bezeichnet wird, d. h. $\bigcap_{i \in I} M_i = \{x \mid \forall\, i \in I \,:\, x \in M_i\} = \{x \mid x \in M_i \;\forall\, i \in I\}$;
$M \cup N$	: *Vereinigung* der Mengen M und N, d. h. $M \cup N = \{x \mid x \in M \vee x \in N\}$;
$\bigcup\limits_{i \in I} M_i$	: Vereinigung aller Mengen M_i mit $i \in I$, d. h. $\bigcup_{i \in I} M_i = \{x \mid \exists\, i \in I \,:\, x \in M_i\}$;
$M \setminus N$	: *Differenz* von M und N, d. h. $M \setminus N = \{x \in M \mid x \notin N\}$;
$M \times N$	: *kartesisches Produkt* von M und N, Menge aller (geordneten) Paare, d. h. $M \times N = \{(m,n) \mid m \in M \wedge n \in N\}$;
$\prod\limits_{i \in I} M_i$	: kartesisches Produkt aller Mengen M_i mit $i \in I$, d. h. $\prod_{i \in I} M_i = \left\{(x_i)_{i \in I} \mid x_i \in M_i \;\forall\, i \in I\right\}$;
$\mathcal{P}(M)$	: *Potenzmenge* von M, Menge aller Teilmengen von M, d. h. $\mathcal{P}(M) = \{N \mid N \subseteq M\}$.

Führen wir nun noch einige spezielle Mengen ein:

$\mathbb{N} := \{0, 1, 2, 3, \ldots\}$	:	die Menge der *natürlichen Zahlen*;
$\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots\}$	:	die Menge der *ganzen Zahlen*;
$\mathbb{Q} := \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$	:	die Menge der *rationalen Zahlen*;
$\mathbb{R}$	:	die Menge der *reellen Zahlen* - diese lassen sich durch endliche oder unendliche Dezimalbrüche darstellen;
$\mathbb{R}_{>0}$ bzw. $\mathbb{R}_{<0}$	:	die Menge der positiven bzw. negativen reellen Zahlen.

Hier und im Folgenden verwenden wir die folgenden Symbole:

$:=$	:	"per definitionem gleich", d. h. die linke Seite wird durch die rechte Seite definiert;
$:\Leftrightarrow$	:	"per definitionem äquivalent", d. h. die linke Seite gilt definitionsgemäß genau dann, wenn die rechte Seite gilt.

Bemerkung B.2
In Definitionen werden wir häufig statt "$:\Leftrightarrow$" etwas unexakt "falls" verwenden, siehe etwa Definition B.8.

Beispiel B.3 a. $\mathbb{N} \subsetneqq \mathbb{Z} \subsetneqq \mathbb{Q} \subsetneqq \mathbb{R}$.

Die Inklusionen sind klar. Daß die Mengen nicht gleich sind, zeigt man dadurch, daß man ein Element der größeren Menge angibt, das nicht in der kleineren enthalten ist.

$$-1 \in \mathbb{Z},\ -1 \notin \mathbb{N};\ \ \frac{1}{2} \in \mathbb{Q},\ \frac{1}{2} \notin \mathbb{Z};\ \ \sqrt{2} \in \mathbb{R},\ \sqrt{2} \notin \mathbb{Q}.$$

b. Sei für $i \in \mathbb{N}$ die Menge $M_i := [-i, i] := \{x \in \mathbb{R} \mid -i \leq x \leq i\}$. Dann gilt:

$$\bigcap_{i \in \mathbb{N}} M_i = \{0\};\ \ \bigcup_{i \in \mathbb{N}} M_i = \mathbb{R}.$$

c. $\mathbb{R} \times \overset{n}{\cdots} \times \mathbb{R} := \prod_{i=1}^{n} \mathbb{R} := \prod_{i \in \{1,\ldots,n\}} \mathbb{R} = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{R}\}.$

Aufgabe B.4
Ist M eine Menge und sind $A, B \subseteq M$ Teilmengen, so zeige man

$$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Definition B.5
Seien M und N Mengen.

a. Eine *Relation* zwischen M und N ist eine Teilmenge $\Gamma \subseteq M \times N$.

b. Sei $\Gamma \subseteq M \times N$ eine Relation. Das Tripel $f = (M, N, \Gamma)$ heißt *Abbildung* von M in N, falls gilt:
   (i) f ist *linksvollständig*, d. h. $\forall\, x \in M\ \exists\, y \in N\ :\ (x, y) \in \Gamma$, und

(ii) f ist *rechtseindeutig*, d. h. $\forall\ (x, y) \in \Gamma\ \forall\ (x', y') \in \Gamma$ gilt: $x = x' \Rightarrow y = y'$.

Statt $f = (M, N, \Gamma)$ schreibt man gemeinhin auch $f : M \to N$, und statt $(x, y) \in \Gamma$ schreibt man $y = f(x)$ oder $x \mapsto y$.

Die Menge $\Gamma_f := \Gamma = \{(x, y) \in M \times N \mid y = f(x)\}$ heißt der *Graph* der Abbildung f.

Wir bezeichnen mit

$$N^M := \{f : M \to N \mid f \text{ ist Abbildung}\}$$

die Menge der Abbildungen von M nach N.

Bemerkung B.6

Eine Abbildung $f : M \to N$ besteht also aus drei Daten, dem *Definitionsbereich* M, dem *Wertebereich* N und der *Abbildungsvorschrift*, die *jedem* $x \in M$ *genau ein* $y = f(x) \in N$ zuordnet. Man beachte, daß nicht gefordert wird, daß $f(x)$ in irgendeiner Form aus x (mittels einer universellen Formel) berechenbar sein muß. Mit den Mitteln der Logik läßt sich beweisen, daß es nicht berechenbare Abbildungen gibt.

Für Abbildungen, die auf dem Computer dargestellt werden sollen, kommen natürlich nur berechenbare Abbildungen in Frage. Mehr noch, man braucht einen Algorithmus, der aus gegebenem x den Wert $f(x)$ in endlich vielen Schritten berechnet.

Statt des Begriffs rechtseindeutig verwendet man häufig auch den Begriff *wohldefiniert*.

Man beachte ferner, daß für zwei Abbildungen $f, g : M \to N$ genau dann gilt $f = g$, wenn für alle $x \in M$ gilt $f(x) = g(x)$.

Definition B.7 a. Es sei M eine Menge. Die Abbildung $\mathrm{id}_M : M \to M : x \mapsto x$ heißt die *Identität* oder *identische Abbildung* auf M.

Wir schreiben häufig kurz id statt id_M, wenn keine Unklarheiten zu befürchten sind.

b. Ist $N \subseteq M$ eine Teilmenge, so nennen wir $i_{N,M} : N \to M : x \mapsto x$ die (kanonische) *Inklusion* von N in M.

Wir schreiben manchmal auch i_N oder i statt $i_{N,M}$, sofern keine Mißverständnisse auftreten können.

Definition B.8

Es sei $f : M \to N$ eine Abbildung, $A \subseteq M$, $B \subseteq N$.

a. $f(A) := \{f(x) \mid x \in A\}$ heißt das *Bild* von A unter der Abbildung f.

b. $f^{-1}(B) := \{x \in M \mid f(x) \in B\}$ heißt *Urbild* von B unter f.

Ist $B = \{y\}$ für ein $y \in N$, so schreiben wir auch $f^{-1}(y)$ statt $f^{-1}(B)$.

c. Die Abbildung $f_{|A} : A \to N : x \mapsto f(x)$ heißt *Einschränkung* von f auf A.
Es gilt offenbar $\Gamma_{f_{|A}} = \Gamma_f \cap (A \times N)$.

d. f heißt *injektiv*, falls gilt:

$$\forall\, x, x' \in M \;:\; f(x) = f(x') \;\Rightarrow\; x = x',$$

d. h. zwei verschiedene Elemente von M können durch f nicht auf dasselbe Element in N abgebildet werden.

e. f heißt *surjektiv*, falls gilt:

$$\forall\, y \in N\; \exists\, x \in M \;:\; y = f(x),$$

d. h. $f(M) = N$, d. h. jedes Element von N kommt als Bild unter f vor.

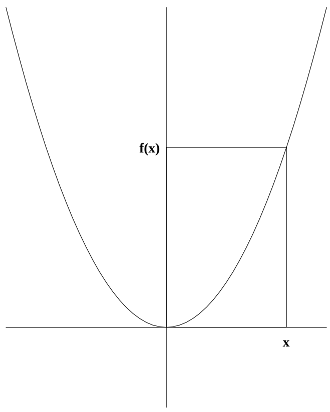
f. f heißt *bijektiv*, falls f injektiv und surjektiv ist.

Bemerkung B.9
Ist $f : M \to N$ eine Abbildung, $A \subseteq M$ und $B \subseteq N$ mit $f(A) \subseteq B$, dann bezeichnen wir hin und wieder auch die Abbildung

$$A \to B : x \mapsto f(x)$$

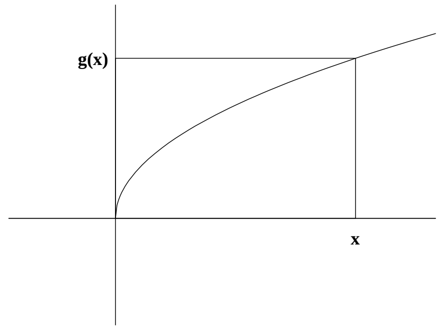
mit $f_{|A}$ und als Einschränkung von f auf A. Das ist zwar etwas unsauber, wird aber in den konkreten Fällen nicht zu Zweideutigkeiten führen.

Beispiel B.10 a. Sei $f : \mathbb{R} \to \mathbb{R}$ die Abbildung, die durch die Vorschrift $f(x) = x^2$ gegeben ist. Der Graph $\Gamma_f = \left\{(x, y) \in \mathbb{R}^2 \;\middle|\; y = x^2\right\}$ ist die Normalparabel.



f ist weder surjektiv (da etwa $-1 \notin f(\mathbb{R})$) noch injektiv (da z. B. $f(-1) = 1 = f(1)$).

b. $g : \mathbb{R}_{\geq 0} \to \mathbb{R} : x \mapsto \sqrt{x}$ ist eine Abbildung, die injektiv ist (da für $x, x' \in \mathbb{R}_{\geq 0}$ aus $\sqrt{x} = \sqrt{x'}$ folgt, daß $x = x'$), aber nicht surjektiv (da $f\big(\mathbb{R}_{\geq 0}\big) = \mathbb{R}_{\geq 0} \neq \mathbb{R}$).



c. $h : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto \sqrt{x}$ unterscheidet sich von g nur durch den Wertebereich. Aber dies reicht, daß h bijektiv ist.

Definition B.11
Es seien I und M Mengen

a. Eine *Familie* von Elementen in M mit *Indexmenge* I ist eine Abbildung $F : I \to M$.

   Für $i \in I$ setze $x_i := F(i) \in M$. Dann schreibt man statt $F : I \to M$ auch $(x_i)_{i\in I}$ (oder kurz (x_i), falls über I kein Zweifel besteht) und nennt dann $(x_i)_{i\in I}$ eine Familie von Elementen in M mit Indexmenge I.

b. Ist $F : I \to M$ eine Abbildung und $J \subseteq I$, so heißt die Einschränkung $F_{|J}$ von F auf J auch eine *Teilfamilie* und wird gemeinhin auch mit $(x_i)_{i\in J}$ bezeichnet.

Bemerkung B.12
Beachte, daß in der Familie $F = (x_i)_{i\in I}$ für $i, j \in I$ mit $i \neq j$ sehr wohl $x_i = x_j$ gelten kann, während dies in der Menge $\{F\} := F(I) = \{x_i \mid i \in I\}$ nicht der Fall ist.

Wir schreiben meist kurz $x \in F$, wenn wir $x \in F(I)$ meinen.

Beispiel B.13 a. Für $J = \emptyset$ spricht man von der *leeren Familie*.

b. Die Familien in M mit Indexmenge $I = \{1, \ldots, n\}$ werden mittels der Schreibweise in Definition B.11 a. mit den Elementen des n-fachen kartesischen Produktes $M \times \overset{n}{\cdots} \times M$ identifiziert, d. h. eine Familie $(x_i)_{i\in I} = (x_1, \ldots, x_n)$ ist das Gleiche wie ein n-Tupel.

c. Eine Familie mit $I = \mathbb{N}$ nennt man eine *Folge*. Somit ist

$$M^{\mathbb{N}} = \{F : \mathbb{N} \to M \mid F \text{ ist Abbildung}\} = \{(x_i)_{i\in\mathbb{N}} \mid x_i \in M\}$$

   die Menge aller Folgen in M.

d. Jede Teilmenge $N \subseteq M$ ist eine Familie mittels der kanonischen Inklusion i_N.

e. Ist $M = \{M_i \mid i \in I\}$ und $F : I \to M : i \mapsto M_i$, so heißt $F = (M_i)_{i\in I}$ auch eine *Familie von Mengen.*

   In Definition B.1 haben wir - ohne dies zu erwähnen - bereits Familien von Mengen benutzt und den Schnitt, die Vereinigung sowie das kartesische Produkt von beliebigen Familien von Mengen definiert!

Definition B.14
Sind $f_1 : M_1 \to M_2$ und $f_2 : M_2 \to M_3$ Abbildungen, so heißt die Abbildung $f_2 \circ f_1 : M_1 \to M_3 : x \mapsto f_2\big(f_1(x)\big)$ die *Komposition* von f_1 und f_2.

Lemma B.15
Die Komposition ist assoziativ, d. h. sind $f_1 : M_1 \to M_2$, $f_2 : M_2 \to M_3$ *und* $f_3 : M_3 \to M_4$ *Abbildungen, so gilt:*

$$(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1).$$

Wir schreiben für die beiden Ausdrücke deshalb auch vereinfacht $f_3 \circ f_2 \circ f_1$.

Beweis: Nach Definition der Komposition gilt für alle $x \in M_1$:

$$\begin{aligned}\big((f_3 \circ f_2) \circ f_1\big)(x) &= (f_3 \circ f_2)\big(f_1(x)\big) = f_3\Big(f_2\big(f_1(x)\big)\Big) \\ &= f_3\big((f_2 \circ f_1)(x)\big) = \big(f_3 \circ (f_2 \circ f_1)\big)(x).\end{aligned}$$

□

Bemerkung B.16
Man darf die Reihenfolge der Komposition nicht vertauschen! Betrachte etwa:

$$f : \mathbb{R} \to \mathbb{R} : x \mapsto x + 1, \quad g : \mathbb{R} \to \mathbb{R} : x \mapsto x^2.$$

Dann gilt:

$$(f \circ g)(x) = f\big(x^2\big) = x^2 + 1, \quad (g \circ f)(x) = g(x + 1) = (x + 1)^2.$$

Damit ist $f \circ g \neq g \circ f$, da etwa $(f \circ g)(1) = 2 \neq 4 = (g \circ f)(1)$.

Wir führen nun die folgenden Notationen ein.

Definition B.17
Zwei Mengen M und N heißen *gleichmächtig*, falls es eine bijektive Abbildung $f : M \to N$ gibt. Mit

$$\#M := |M| := \begin{cases} \text{Anzahl der Elemente in } M, \text{ falls } M \text{ endlich ist,} \\ \infty, \text{ falls } M \text{ unendlich viele Elemente enthält,} \end{cases}$$

bezeichnen wir die *Mächtigkeit* der Menge M.[31]

Lemma B.18
Es seien M *und* N *zwei endliche Mengen.*

a. *Genau dann gilt* $|M| \leq |N|$, *wenn es eine injektive Abbildung* $f : M \to N$ *gibt.*
b. *Genau dann gilt* $|M| \geq |N|$, *wenn es eine surjektive Abbildung* $f : M \to N$ *gibt.*
c. *Genau dann gilt* $|M| = |N|$, *wenn es eine bijektive Abbildung* $f : M \to N$ *gibt.*

[31] Auch für unendliche Mengen gibt es unterschiedliche Mächtigkeiten, sog. *Kardinalzahlen*, auf die wir hier aber nicht eingehen wollen.

Beweis: Es seien $M = \{x_1, \ldots, x_m\}$ und $N = \{y_1, \ldots, y_n\}$ mit paarweise verschiedenen Elementen $x_i \neq x_j$ für $i \neq j$ und $y_i \neq y_j$ für $i \neq j$. Es gilt $|M| = m$ und $|N| = n$.

a. Ist $m \leq n$, so definiere $f : M \to N$ durch $f(x_i) = y_i$ für $i = 1, \ldots, m$. Dann gilt für $i, j \in \{1, \ldots, m\}$ mit $i \neq j$

$$f(x_i) = y_i \neq y_j = f(x_j).$$

Mithin ist f injektiv.

Ist umgekehrt $f : M \to N$ eine injektive Abbildung, so gilt $f(M) = \{f(x_1), \ldots, f(x_m)\} \subseteq N$ eine Teilmenge von paarweise verschiedenen Elementen. Mithin enthält N mindestens m Elemente, und folglich gilt $m \leq n$.

b. Ist $m \geq n$, so definiere $f : M \to N$ durch $f(x_i) = y_i$ für $i = 1, \ldots, n$ und $f(x_i) = y_1$ für $i = n + 1, \ldots, m$. Dann gilt offenbar $f(M) = \{y_1, \ldots, y_n\} = N$ und f ist surjektiv.

Ist umgekehrt $f : M \to N$ eine surjektive Abbildung, so gilt $\{y_1, \ldots, y_n\} = N = f(M) = \{f(x_1), \ldots, f(x_m)\}$. Mithin enthält die Menge $\{f(x_1), \ldots, f(x_m)\}$ n verschiedene Elemente, und folglich ist $m \geq n$.

c. Die Aussage folgt unmittelbar aus den ersten beiden Teilen.

□

Bemerkung B.19
Sind M und N endliche Mengen, so folgt aus $M \subsetneqq N$ mittels Lemma B.18 unmittelbar $|M| < |N|$ und M und N sind nicht gleichmächtig.

Dies gilt für unendliche Mengen nicht mehr, wie das Beispiel $\mathbb{N} \subsetneqq \mathbb{Z}$ zeigt. Denn die Abbildung

$$f : \mathbb{Z} \to \mathbb{N} : k \mapsto \begin{cases} 2k, & \text{für } k \geq 0, \\ -2k - 1 & \text{für } k < 0, \end{cases}$$

ist bijektiv, wie man sich leicht überzeugt. Also sind $\mathbb{N}$ und $\mathbb{Z}$ gleichmächtig.

Lemma B.20
Seien M *und* N *zwei nicht-leere Mengen,* $f : M \to N$ *eine Abbildung.*

a. f *ist genau dann injektiv, wenn es eine Abbildung* $g : N \to M$ *gibt mit* $g \circ f = \mathrm{id}_M$.

b. f *ist genau dann surjektiv, wenn es eine Abbildung* $g : N \to M$ *gibt mit* $f \circ g = \mathrm{id}_N$.

c. f *ist genau dann bijektiv, wenn es eine Abbildung* $g : N \to M$ *gibt mit* $g \circ f = \mathrm{id}_M$ *und* $f \circ g = \mathrm{id}_N$.

d. *Ist* f *bijektiv, so ist die nach c. existierende Abbildung* g *eindeutig bestimmt und ebenfalls bijektiv. Sie heißt die* Inverse *oder* Umkehrabbildung *von* f *und wird mit* f^{-1} *bezeichnet.*

Beweis: a. <u>“$\Rightarrow$”:</u> Es sei f injektiv. Dann gilt für $y \in f(M)$, daß $\left|f^{-1}(y)\right| = 1$, also $f^{-1}(y) = \{x_y\}$ für ein geeignetes $x_y \in M$ und $f(x_y) = y$. Hingegen ist $f^{-1}(y) = \emptyset$ für $y \notin f(M)$. Wähle ein $x_0 \in M \neq \emptyset$ fest und definiere eine Abbildung

$$g : N \to M : y \mapsto \begin{cases} x_y, & \text{falls } y \in f(M), \\ x_0, & \text{falls } y \in N \setminus f(M). \end{cases}$$

Dann gilt für $x \in M$:

$$(g \circ f)(x) = g\big(f(x)\big) = x_{f(x)} = x = \mathrm{id}_M(x).$$

Da $x \in M$ beliebig gewählt war, folgt also $g \circ f = \mathrm{id}_M$.

<u>“$\Leftarrow$”:</u> Es sei nun $g : N \to M$ mit $g \circ f = \mathrm{id}_M$ gegeben. Seien ferner $x, x' \in M$ mit $f(x) = f(x')$, dann gilt:

$$x = \mathrm{id}_M(x) = (g \circ f)(x) = g\big(f(x)\big) = g\Big(f\big(x'\big)\Big) = (g \circ f)\big(x'\big) = \mathrm{id}_M\left(x'\right) = x'.$$

Also ist f injektiv.

b. <u>“$\Rightarrow$”:</u> Es sei f surjektiv. Dann können wir zu jedem $y \in N = f(M)$ ein $x_y \in M$ wählen mit $f(x_y) = y$. Definiere eine Abbildung

$$g : N \to M : y \mapsto x_y.$$

Dann gilt für $y \in N$:

$$(f \circ g)(y) = f\big(g(y)\big) = f(x_y) = y = \mathrm{id}_N(y).$$

Da $y \in N$ beliebig gewählt war, folgt also $f \circ g = \mathrm{id}_N$.

<u>“$\Leftarrow$”:</u> Es sei nun $g : N \to M$ mit $f \circ g = \mathrm{id}_N$ gegeben. Für $y \in N$ definiere $x := g(y) \in M$. Dann gilt:

$$y = \mathrm{id}_N(y) = (f \circ g)(y) = f\big(g(y)\big) = f(x) \in f(M).$$

Also ist f surjektiv.

c. <u>“$\Rightarrow$”:</u> Ist f bijektiv, so gilt für jedes $y \in N$, daß $\left|f^{-1}(y)\right| = 1$ und die Definitionen der Abbildungen g in den beiden obigen Teilen stimmen überein, so daß wir eine einzige Abbildung $g : N \to M$ erhalten mit:

$$g \circ f = \mathrm{id}_M \quad \text{und} \quad f \circ g = \mathrm{id}_N\,.$$

<u>“$\Leftarrow$”:</u> Dies folgt unmittelbar aus den obigen beiden Teilen.

d. Die Bijektivität von g folgt aus dem in c. bewiesenen Kriterium für Bijektivität. Mithin bleibt die Eindeutigkeit von g zu zeigen, unter der Voraussetzung. Angenommen, $h : N \to M$ sei eine weitere Abbildung mit

$$h \circ f = \mathrm{id}_M \quad \text{und} \quad f \circ h = \mathrm{id}_N\,.$$

Für $y \in N$ beliebig gilt dann:

$$f\big(g(y)\big) = (f \circ g)(y) = \mathrm{id}_N(y) = (f \circ h)(y) = f\big(h(y)\big).$$

Da aber f injektiv ist, folgt damit $g(y) = h(y)$ und schließlich und $g = h$.

$\square$

Bemerkung B.21
Man beachte, daß die Umkehrabbildung $f^{-1} : N \to M$ nur für eine bijektive Abbildung $f : M \to N$ erklärt ist, daß aber für eine beliebige Abbildung $h : M \to N$ und eine beliebige Teilmenge $B \subseteq N$ das Urbild $h^{-1}(B)$ definiert ist.

Für ein bijektives f stimmen beide Notationen überein, das heißt das Urbild $f^{-1}(B)$ von $B \subseteq N$ unter f ist gleich dem Bild $f^{-1}(B)$ von $B \subseteq N$ unter f^{-1}.

Ist f nicht bijektiv, so ist zwar weiterhin für jedes $y \in N$ das Urbild $f^{-1}(y)$ erklärt, aber die Relation $\big\{(y,x) \in N \times M \mid x \in f^{-1}(y)\big\}$ ist keine Abbildung, da sowohl $f^{-1}(y) = \emptyset$ (falls f nicht surjektiv ist) als auch $\big|f^{-1}(y)\big| > 1$ (falls f nicht injektiv ist) möglich ist. In ersterem Fall ist die Linksvollständigkeit verletzt, in letzterem Fall die Rechtseindeutigkeit.

Beispiel B.22 a. Ist M eine Menge, so ist id_M bijektiv, da offenbar $\mathrm{id}_M = \mathrm{id}_M \circ \mathrm{id}_M$.

b. Die Abbildung $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto 2x$ ist injektiv, da für $x, y \in \mathbb{Z}$ aus $2x = 2y$ unmittelbar $x = y$ folgt. f ist aber nicht surjektiv, da etwa die Zahl 1 kein Urbild besitzt.

c. Im Gegensatz zu b. ist die Abbildung $g : \mathbb{Q} \to \mathbb{Q} : x \mapsto 2x$ sowohl injektiv, als auch surjektiv. Für letzteres beachte man, daß für eine rationale Zahl $y \in \mathbb{Q}$ die rationale Zahl $\frac{y}{2} \in \mathbb{Q}$ ein Urbild von y unter g ist.

Wir kommen noch einmal auf Relationen zurück. Wir hatten schon Abbildungen als Relationen mit besonderen Eigenschaften definiert. Andere wichtige Relationen haben auch einen speziellen Namen.

Definition B.23
Es sei M ein Menge. Eine *Ordnungsrelation* auf M, auch *Halbordnung* oder *partielle Ordnung* genannt, ist eine Relation $R \subseteq M \times M$, so daß für alle $x, y, z \in M$ gilt:

a. $(x, x) \in R$, (“Reflexivität”)

b. $(x, y), (y, x) \in R \;\Rightarrow\; x = y$, (“Antisymmetrie”)

c. $(x, y), (y, z) \in R \;\Rightarrow\; (x, z) \in R$. (“Transitivität”)

Notation B.24
Es sei M eine Menge und R ein Ordnungsrelation auf M. Wir definieren für $x, y \in M$

$$x \leq y \;:\Leftrightarrow\; (x, y) \in R,$$

und sprechen hin und wieder auch von der Ordnungsrelation “$\leq$” statt R, sofern keine Mißverständnisse zu befürchten sind. Ferner sprechen wir von der *partiell* oder *(teil-)geordneten Menge* $(M, \leq)$.

Mit dieser Schreibweise lassen sich die drei Axiome in Definition B.23 wie folgt formulieren. Für $x, y, z \in M$ soll gelten:

a. $x \leq x$, ("Reflexivität")

b. $x \leq y, y \leq x \;\Rightarrow\; x = y$, ("Antisymmetrie")

c. $x \leq y, y \leq z \;\Rightarrow\; x \leq z$. ("Transitivität")

Gilt für $x, y \in M$, daß $x \leq y$ und $x \neq y$, so schreiben wir auch $x < y$.

Definition B.25
Es sei M ein Menge.

a. Eine Ordnungsrelation "$\leq$" heißt *Totalordnung* oder *lineare Ordnung*, falls je zwei Elemente aus M vergleichbar sind, d. h. für je zwei Elemente $x, y \in M$ gilt $x \leq y$ oder $y \leq x$.

b. Ist "$\leq$" eine Ordnungsrelation auf M, $A \subseteq M$ und $x \in A$, so heißt x *minimal* (bzw. *maximal*) in A, falls für alle $y \in A$ mit $y \leq x$ (bzw. $x \leq y$) gilt $x = y$.

c. Eine Totalordnung heißt *Wohlordnung*, falls jede nicht-leere Teilmenge von M ein minimales Element besitzt.

Beispiel B.26
Die reellen Zahlen $(\mathbb{R}, \leq)$ mit der üblichen Kleiner-Gleich-Relation $\leq$ sind total geordnet, aber nicht wohlgeordnet.

Gleiches trifft auf $(\mathbb{Z}, \leq)$ mit der üblichen Kleiner-Gleich-Relation

$$\ldots - 2 < -1 < 0 < 1 < 2 < \ldots$$

zu. Allerdings definiert die "unübliche" Anordnung

$$0 < -1 < 1 < -2 < 2 < -3 < 3 < \ldots$$

in der Tat ein Wohlordnung auf $\mathbb{Z}$.

Die natürlichen Zahlen $(\mathbb{N}, \leq)$ sind bereits mit der üblichen Kleiner-Gleich-Relation wohlgeordnet.

Beispiel B.27
Ist M eine Menge, so ist die Potenzmenge $\mathcal{P}(M)$ von M durch

$$A \leq B \;:\Leftrightarrow\; A \subseteq B, \text{ für } A, B \in \mathcal{P}(M),$$

partiell geordnet, aber im allgemeinen nicht total geordnet. Z. B. sind im Fall $M = \mathbb{N}$ die Elemente $\{2\}$ und $\{3\}$ in $\mathcal{P}(\mathbb{N})$ nicht vergleichbar.

Allgemeiner gilt, ist N eine Menge, deren Elemente wieder Mengen sind, so wird N mit der analogen Definition von "$\leq$" eine partiell geordnete Menge.

Anhang C Komplexe Zahlen

Die komplexen Zahlen sind eine Erweiterung des Körpers $\mathbb{R}$ der reellen Zahlen, in ganz ähnlicher Weise wie die reellen Zahlen eine Erweiterung des Körpers $\mathbb{Q}$ der rationlen Zahlen sind. Da man in der Praxis doch ohnehin nur mit endlichen Dezimalbrüchen rechnet, ist die Frage berechtigt, wozu man eigentlich die rellen und dann gar die komplexen Zahlen braucht.

Die Antwort auf die erste Frage ist schnell gegeben. Wir wissen, daß ganz natürlich auftretende Größen wie die Länge der Diagonalen eines Quadrates mit Seitenlänge eins, sprich die Zahl $\sqrt{2}$, oder das Verhältnis von Umfang zum Durchmesser eines Kreises, sprich die Kreiszahl π, keine rationalen Zahlen sind. Sie sind aber reelle Zahlen und die reellen Zahlen sind in gewissen Sinne, eine *Vervollständigung* der rationalen Zahlen. Wir brauchen also die reellen Zahlen, da die rationalen Zahlen Lücken aufweisen. Die komplexen Zahlen werden nun deshalb eingeführt, um einen Mangel, den die reellen Zahlen immer noch haben, zu beheben. Hierbei geht es um das Lösen von Gleichungen, aber nicht mehr linearen, sondern quadratischen. Es ist bekannt, daß das Quadrat einer reellen Zahl stets nicht-negativ ist. Also kann es keine reelle Zahl x geben, die die Gleichung $x^2 = -1$ löst.

Als Lösung genau dieser Gleichung wird nun eine neue Größe eingeführt, die *imaginäre Einheit* i. Definitionsgemäß ist sie diejenige Zahl, für die $i^2 = -1$ gilt. Wenn man nun eine solche Größe i einführt, dann ist damit alleine gar nichts gewonnen. Man will ja mit i auch rechnen können, und zwar will man möglichst alle Rechenregeln von $\mathbb{R}$ übertragen. Man will nicht nur $i^2 = i \cdot i$, sondern auch $i+i$ oder Ausdrücke wie $37+42i$ bilden können. Dabei sollen die so zu konstruierenden *komplexen Zahlen* die reellen Zahlen als Teilmenge enthalten.

Daß es wirklich ein solches Zahlsystem komplexer Zahlen, in unserer Sprache den Körper der komplexen Zahlen, gibt, ist überhaupt nicht klar und wurde historisch erst spät realisiert und auch akzeptiert.[32] Gauß hat die Zahlen geometrisch, als Punkte in der Ebene, eingeführt, weshalb die komplexen Zahlen heute noch *gaußsche Zahlenebene* heißen. Wir führen die komplexen Zahlen ebenfalls als reelle Zahlenpaare ein, definieren die Addition und die Multiplikation aber algebraisch und werden die Definitionen erst im Anschluß daran geometrisch interpretieren.

Definition C.1
Die Menge $\mathbb{C} := \{(x, y) \mid x, y \in \mathbb{R}\}$ zusammen mit der durch

$$(x, y) + (u, v) := (x + u, y + v), \quad \text{für } (x, y), (u, v) \in \mathbb{C},$$

und

$$(x, y) \cdot (u, v) := (xu - yv, xv + yu), \quad \text{für } (x, y), (u, v) \in \mathbb{C},$$

[32]Erstmals taucht $\sqrt{-1}$ wohl um 1540 bei Cardano auf. Wirklich als Zahlsystem wurden die komplexen Zahlen aber erst durch Gauß, 1777-1855, etabliert. Hierzu und zu vielen weiteren interessanten Tatsachen um die komplexen Zahlen vgl. [Ebb92] § 3.

definierten Addition und Multiplikation heißt der *Körper der komplexen Zahlen.* Für $z = (x, y) \in \mathbb{C}$ heißt $\mathrm{Re}(z) := x$ der Realteil von z und $\mathrm{Im}(z) := y$ der Imaginärteil.

Satz C.2
$(\mathbb{C}, +, \cdot)$ *ist ein Körper.*

Beweis: Man sieht sofort, daß $(\mathbb{C}, +)$ eine abelsche Gruppe ist mit $(0, 0)$ als neutralem Element und $(-x, -y)$ als Inversem zu $(x, y) \in \mathbb{C}$.

Etwas mehr ist zu zeigen, um zu sehen, daß $(\mathbb{C} \setminus \{(0, 0)\}, \cdot)$ eine abelsche Gruppe ist mit $(1, 0)$ als neutralem Element und $\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)$ als Inversem zu $(x, y) \in \mathbb{C} \setminus \{(0, 0)\}$. Wir überlassen den Nachweis dem Leser als Übungsaufgabe. $\square$

Bemerkung C.3
Wir wollen nun sehen, daß $\mathbb{C}$ ein Erweiterungskörper von $\mathbb{R}$ ist. Dazu betrachten wir die Abbildung

$$\varphi : \mathbb{R} \to \mathbb{C} : x \mapsto (x, 0).$$

Man prüft leicht nach, daß φ ein Körpermonomorphismus ist.

Wir identifizieren $\mathbb{R}$ mit dem Bild $\varphi(\mathbb{R}) = \mathbb{R} \times \{0\} \subset \mathbb{R} \times \mathbb{R} = \mathbb{C}$. Damit ist $\mathbb{R}$ ein *Unterkörper* von $\mathbb{C}$.

Notation C.4
Praktischer als das Rechnen mit Paaren von Zahlen ist die folgende Notation für komplexe Zahlen. Wir setzen $x := (x, 0)$ für $x \in \mathbb{R}$ und $i := (0, 1)$. Dann gilt für $z = (x, y) \in \mathbb{C}$

$$z = (x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1) \cdot (y, 0) = x + iy.$$

Bemerkung C.5
Mit dieser Schreibweise gilt zunächst:

$$i^2 = (0, 1) \cdot (0, 1) = -1.$$

Ferner ergibt sich die etwas willkürlich anmutende Definition der Multiplikation ganz "natürlich" aus

$$(x + iy)(u + iv) = \big(xu + i^2 yv\big) + i(xv + yu) = (xu - yv) + i(xv + yu).$$

Bemerkung C.6
Auf $\mathbb{R}$ und $\mathbb{C}$ hat man noch andere wichtige Strukturen, die man auf beliebigen Körpern nicht hat.

Auf $\mathbb{R}$ hat man die *Ordnungsrelation* $\leq$, die eine totale Ordnung auf $\mathbb{R}$ ist, und die mit den Operationen auf $\mathbb{R}$ verträglich ist, d. h. für $x, y, z \in \mathbb{R}$ gilt:

a. $x \leq y \;\Rightarrow\; x + z \leq y + z$, und
b. $0 < x, 0 < y \;\Rightarrow\; 0 < xy$.

Außerdem hat man auf $\mathbb{R}$ die *Betragsfunktion*

$$|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto \begin{cases} x, & x \geq 0 \\ -x, & x < 0. \end{cases}$$

Die Ordnungsrelation $\leq$ auf $\mathbb{R}$ läßt sich nicht so auf $\mathbb{C}$ fortsetzen, daß die obigen Gesetze a. und b. erhalten bleiben.[33] Im Gegensatz dazu besitzt $\mathbb{C}$ aber eine Betragsfunktion,

$$|\cdot| : \mathbb{C} \to \mathbb{R}_{\geq 0} : x + iy \mapsto \sqrt{x^2 + y^2},$$

die die Betragsfunktion auf $\mathbb{R}$ fortsetzt.

Außerdem gibt es auf $\mathbb{C}$ eine weitere wichtige Abbildung, die *komplexe Konjugation*

$$\bar{\cdot} : \mathbb{C} \to \mathbb{C} : z = x + iy \mapsto \overline{z} := x - iy.$$

Für $z \in \mathbb{C}$ heißt $\overline{z}$ die zu z *konjugiert komplexe Zahl*.

Die folgenden Eigenschaften der komplexen Zahlen sind einfach nachzuweisen, und ihr Nachweis sei dem Leser überlassen.

Lemma C.7
Für $z, w \in \mathbb{C}$ gelten:

a. $\overline{z} + \overline{w} = \overline{z + w}$,

b. $\overline{z} \cdot \overline{w} = \overline{z \cdot w}$,

c. $\overline{\overline{z}} = z$,

d. $\overline{z} = z \iff z \in \mathbb{R}$,

e. $z \cdot \overline{z} = |z|^2$,

f. $|z| \cdot |w| = |zw|$,

g. $|z + w| \leq |z| + |w|$, *und*

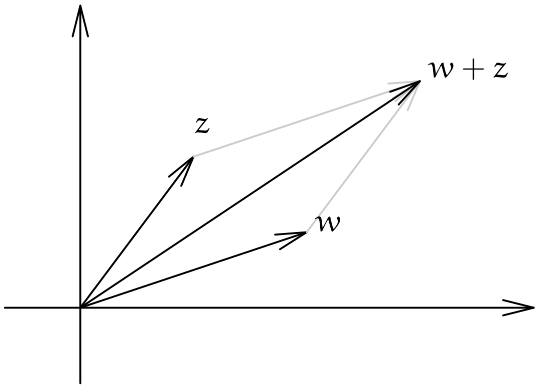
h. $z = 0 \iff |z| = 0$.

Teil g. nennt man die *Dreiecksungleichung*. Sie wird vor allem in der Analysis von großer Bedeutung sein. Elementargeometrisch wird ihre Bedeutung im Folgenden augenscheinlich.

Geometrische Deutung der komplexen Zahlen
Wir betrachten $z = (x, y)$ als Richtungsvektor in der Zahlenebene $\mathbb{R}^2$.

Die Addition ist einfach die komponentenweise Addition, also die Addition der Vektoren.

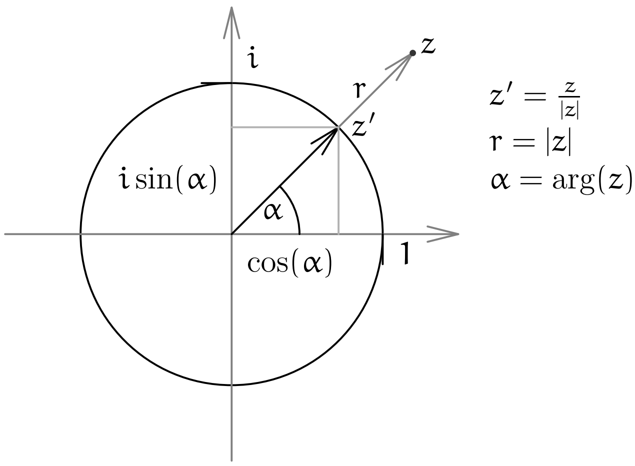
[33] Sonst würde entweder $0 < i$ oder $0 < -i$ gelten, und somit $0 < i^2 = -1$ oder $0 < (-i)^2 = -1$, was im Widerspruch zur Definition von $\leq$ auf $\mathbb{R}$ steht.



Zur geometrischen Interpretation der Multiplikation brauchen wir die Betragsfunktion. Der Betrag $r := |z|$ einer komplexen Zahl z ist die Länge des Vektors z (Pythagoras). Für $z \neq 0$ hat $z' := \frac{z}{|z|}$ die Länge eins, und es gilt

$$z = |z| \cdot z' = r \cdot z'.$$

D. h. z ist das Produkt eines Vektors von Länge eins mit einer nicht-negativen reellen Zahl. Dabei ist z' vollständig durch den Winkel α bestimmt, den z' mit der x-Achse einschließt, nämlich $z' = \big(\cos(\alpha), \sin(\alpha)\big)$. Also ist jede komplexe Zahl $z \neq 0$ eindeutig durch ihren Betrag und den Winkel $\alpha =: \arg(z)$, das *Argument* von z, bestimmt. Das Paar $(r, \alpha) = \big(|z|, \arg(z)\big)$ nennt man die *Polarkoordinaten* von z.



Die komplexen Zahlen vom Betrag eins sind genau die Punkte auf dem Einheitskreis. Für $z' \in \mathbb{C}$ mit $\left|z'\right| = 1$ gibt es also genau ein $0 \leq \alpha < 2\pi$ mit

$$z' = \cos(\alpha) + i\sin(\alpha) = e^{i\alpha}.$$

Damit gilt für ein beliebiges $c \in \mathbb{C}$

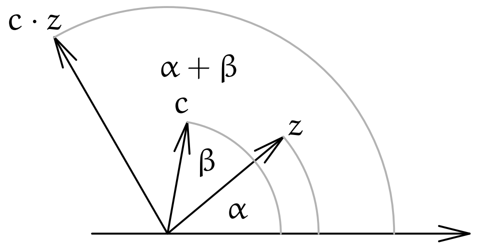
$$c = |c| \cdot \big(\cos(\beta) + i\sin(\beta)\big) = |c| \cdot e^{i\beta},$$

für $\beta = \arg(c)$.

Daraus ergibt sich für die Multiplikationsabbildung mit einer festen komplexen Zahl $z = |z| \cdot e^{i\alpha}$,

$$m_z : \mathbb{C} \to \mathbb{C} : c \mapsto |z| \cdot |c| \cdot e^{i(\alpha+\beta)}.$$

Die Multiplikation mit z ist also eine *Drehstreckung*, daß heißt der Vektor c wird um den Winkel $\alpha = \arg(z)$ gedreht und um den Faktor $|z|$ gestreckt.



Index

Literatur

[Beu94] Albrecht Beutelspacher, *Kryptologie*, 4 ed., Vieweg, 1994.

[DH76] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. on Info. Theory **IT-22** (1976), 644–654.

[Ebb92] Heinz-Dieter Ebbinghaus (ed.), *Zahlen*, 3 ed., Springer, 1992.

[GK00] Gert-Martin Greuel and Thomas Keilen, *Lineare Algebra I & II*, Vorlesungsskript, FB Mathematik, Universität Kaiserslautern, 2000.

[Hum96] John F. Humphreys, *A course in group theory*, OUP, Oxford, 1996.

[Kei01] Thomas Keilen, *Endliche Gruppen*, Fachbereich Mathematik, Universität Kaiserslautern, Jan. 2001, Proseminarskript, 3. Auflage, http://www.mathematik.uni-kl.de/~wwwagag/download/scripts/Endliche.Gruppen.ps.gz.

[Kei02] Thomas Keilen, *Algebra I*, Mathematics Institute, University of Warwick, Oct. 2002, http://www.mathematik.uni-kl.de/~keilen/download/Lehre/ALGWS02/algebra.ps.gz.

[Lan97] Serge Lang, *Algebraische Strukturen*, Springer, 1997.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.

[Sch91] Ralph-Hardo Schulz, *Codierungstheorie, Eine Einführung*, Vieweg, 1991.

[Sie81] Helmut Siemon, *Anwendungen der elementaren Gruppentheorie: in Zahlentheorie und Kombinatorik*, Klett Studienbücher, Klett, 1981.

[Ver75] J. Verhoeff, *Error detecting decimal codes*, Mathematical Centre Tracts, no. 29, Mathematisch Centrum Amsterdam, 1975.