Inhaltsverzeichnis

KAPITEL 4

Grundlegende Algebra

In diesem Kapitel widmen wir uns dem Ausbau mathematischer Strukturen. Die hier definierten Gruppen, Ringe und besonders die Körper bilden die Grundlage für die Theorien in Lineare Algebra und Analysis.

Schon in der Zeit der Antike haben in Griechenland berühmte Mathematiker gewirkt. Euklid (ca. 325–265 v.Chr.) (*euklidische* Geometrie, *euklidische* Räume) ist heute vor allem bekannt für sein Werk „Die Elemente“ (13 Bücher), das das erste bekannte mathematische Lehrwerk ist, in dem Axiome, Theoreme und Beweise in klarer Abfolge vorkommen und das auf rigorosen Umgang mit der Mathematik abzielt. Es enthält unter anderem Aussagen über ebene und räumliche Geometrie (etwa die Platonischen Körper), Zahlentheorie (z.B. den euklidischen Algorithmus), rationale und irrationale Zahlen. Etwa fünfhundert Jahre später schrieb Diophantus von Alexandria (ca. 200–284) (*diophantische* Gleichung, *diophantische* Approximation) neben anderen Büchern sein 13-bändiges Werk „Arithmetica“, von dessen Name unser heutiges „Arithmetik“ abgeleitet ist. In diesem machte er als erster einen Schritt in Richtung moderner Algebra. Er studierte lineare und quadratische Gleichungen sowie zahlentheoretische Probleme. Da aber zu seiner Zeit die Null noch nicht erfunden war und das Konzept negativer Zahlen noch in weiter Ferne lag, war die Behandlung dieser Gleichungen noch auf Fallunterscheidungen angewiesen. Darüber hinaus erschienen ihm einige dieser Gleichungen als sinnlos, etwa $4 = 4x + 20$, weil sie keine (d.h. negative) Lösungen hatten. Auch das „Buchstabenrechnen“ hatte er noch nicht eingeführt, und es gab noch kein praktisches Zahlensystem. Alle Theoreme und Rechnungen wurden in Worten präsentiert.

Weitere fünfhundert Jahre später verfasste der arabische Mathematiker Abu Abd Allah Mohammed Ibn Musa Al-Khwarizmi (ca. 780–850), Hofmathematiker in Bagdad, sein Hauptwerk „al-kitab almukhtamar fi hisab **al-jabr** wa’l-muqabala“, zu deutsch „Kurzgefasstes Buch über das Rechnen durch Vervollständigen und Ausgleichen“. Ein weiterer Meilenstein in der Mathematik (nicht primär im Inhalt aber bestimmt in der Wirkung), beschreibt dieses Buch die vollständige Behandlung der linearen und quadratischen Gleichungen, auch die negativen Fälle, beide Lösungen, aber noch immer ohne die Verwendung von Null und negativen Zahlen. Auch das Rechnen mit Buchstaben wurde zu dieser Zeit noch nicht erfunden. Allerdings wurden zum ersten Mal detaillierte Rechenschritte zur Lösung mathematischer Probleme angegeben. Außerdem wurde das hinduistische Zahlensystem (die heutigen arabischen Zahlen) mit den Ziffern 0 bis 9 und den Dezimalstellen zum ersten Mal ausführlich erklärt. Im zwölften Jahrhundert wurde es in Latein übersetzt und beginnt dort mit den Worten „Dixit Algoritmi“ (Al-Khwarizmi hat gesagt). Aus dieser Lateinisierung des Herkunftsnamens von Al-Khwarizmi (Khwarizm, das heutige Khiva südlich des Aralsees in Usbekistan und Turkmenistan) wird übrigens das Wort *Algorithmus* für das schrittweise Lösen mathematischer Probleme abgeleitet. Teile des arabischen Titels, besonders das **al-jabr**, wurden auch in späteren Büchern arabischer Mathematiker verwendet, und so wurde über viele Zwischenstufen aus dem arabischen al-jabr (Auffüllen, Vervollständigen) das moderne Wort *Algebra*.

Heute versteht man unter Algebra vor allem die mathematische Theorie von Strukturen, und was das genau ist, wollen wir uns in den nächsten Abschnitten genauer ansehen.

4.1. Motivation

Alle hier zu besprechenden Strukturen basieren auf dem Mengenkonzept. Es sind **Mengen zusammen mit Abbildungen**, die bestimmte Eigenschaften aufweisen. Wir beginnen mit einigen Beispielen.

Beispiel 4.1.1.

Hauptwörter: *Sei W die Menge aller Hauptwörter der deutschen Sprache. Wählt man zwei Wörter aus W, dann kann man (meist) durch (fast bloßes) Hintereinandersetzen ein weiteres Wort aus W erzeugen. Wir können etwa aus „Leiter“ und „Sprosse“ das Wort „Leitersprosse“ bilden. Auch „Dampf“ und „Schiff“ lassen sich zu „Dampfschiff“ verbinden, „Schiff“ und „Kapitän“ ergeben „Schiffskapitän“.*

Strichblöcke: *Sei S die Menge aller Strichblöcke. Ein Strichblock ist einfach eine Ansammlung hintereinander geschriebener gleich langer Striche:*

$$s = |||||||||||||||$$

Fügen wir zwei Strichblöcke aneinander, dann erhalten wir wieder einen (längeren) Strichblock.

Translationen: *Sei T die Menge aller Möglichkeiten, ein Objekt im dreidimensionalen Raum geradlinig zu verschieben, also die Menge der* Translationen. *Bei der Betrachtung solcher Verschiebungen können wir uns auf deren Richtung und Länge beschränken. Zusammen mit der Position des Objekts vor der Translation ist es uns dann leicht möglich, seine Endposition zu bestimmen. Verschieben wir ein Objekt zweimal, so hätten wir dieselbe Endposition auch mit einer einzigen Translation erreichen können. Das Hintereinander-Ausführen von Translationen ist also wieder eine Translation.*

Drehungen: *Betrachten wir wieder einen Gegenstand. Wir wählen eine beliebige Gerade g, die durch seinen Schwerpunkt geht. Dann geben wir uns einen Winkel φ vor und verdrehen das Objekt bezüglich der Drehachse g um den Winkel φ. Die Menge aller dieser Drehungen sei D. Wie bei den Translationen ergibt das Hintereinander-Ausführen zweier Drehungen wieder eine Drehung.*

Abbildungen: *Sei $M^M = \mathrm{Abb}(M)$ die Menge aller Abbildungen von M nach M. Die Hintereinander-Ausführung $\circ$ von Abbildungen (vgl. 3.3.51) ist eine Verknüpfung auf* $\mathrm{Abb}(M)$.

Zahlenmengen:

- $\mathbb{N}$**:** *Wenn wir zwei natürliche Zahlen addieren oder multiplizieren, erhalten wir wieder eine natürliche Zahl.*
- $\mathbb{Z}$**:** *Auch das Produkt und die Summe zweier ganzer Zahlen ist eine ganze Zahl.*
- $\mathbb{R}$**:** *Auch reelle Zahlen können wir addieren und multiplizieren, um eine neue reelle Zahl zu berechnen.*

Matrizen:

Addition: *Sei $M_2(\mathbb{R})$ die Menge aller 2×2–Matrizen reeller Zahlen. Eine 2×2–Matrix ist dabei ein kleines Zahlenquadrat der Form (vgl. 2.2.1)*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

aus Zahlen $a_{ij} \in \mathbb{R}$. Wir definieren die Summe zweier Matrizen komponentenweise, d.h.

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$

und erhalten wieder eine 2×2–Matrix.

Multiplikation: *Auf $M_2(\mathbb{R})$ kann man auch ein Produkt einführen, das zwei Matrizen eine weitere Matrix zuordnet. Die Definition ist nicht-trivial und lautet*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Visualisieren kann man sich die Verknüpfung an Hand der farbigen Pfeile in

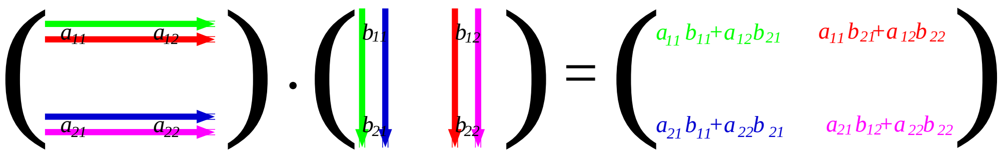

Abbildung 4.1. Multiplikation von Matrizen

Abbildung 4.1. Um etwa den grünen Eintrag in der Ergebnismatrix zu erhalten, wandert man die grünen Pfeile in den beiden Faktoren entlang. Dann berechnet man das Produkt der ersten Zahl links mit der ersten Zahl im Pfeil rechts, das der zweiten Zahl im linken Pfeil mit der zweiten Zahl im rechten Pfeil und summiert die Ergebnisse.

Gleitkommazahlen: *Sei FP_2 die Menge aller rationalen Zahlen, die sich schreiben lassen als $\pm 0.z_1z_2 \cdot 10^n$ mit Ziffern z_1 und z_2 und ganzzahligem Exponenten n. Diese Zahlen heißen auch dezimale Gleitkommazahlen mit zwei signifikanten Stellen. Addieren wir zwei solche Zahlen, erhalten wir wieder eine rationale Zahl. Diese Zahl lässt sich aber meist nicht in der obigen Form schreiben:*

$$0.23 + 4.5 = 4.73.$$

Wir zwingen das Ergebnis nun in die Gleitkommaform, indem wir runden. *Dann wird*

$$0.23 + 4.5 = 4.73 \approx 4.7, \quad 0.23 \oplus 4.5 = 4.7,$$

und mit dieser veränderten Addition $\oplus$ (Addition mit Runden), ergibt die Summe zweier Elemente von FP_2 wieder eine Gleitkommazahl mit zwei signifikanten Stellen.

Alle diese Beispiele haben eines gemeinsam. Wir starten mit einer Menge M und einer Methode, wie wir aus zwei Elementen von M ein weiteres Element von M erzeugen. In der nächsten Definition schälen wir diese Struktur heraus.

Definition 4.1.2 (Gruppoid)**.** *Sei G eine nichtleere Menge.*

(i) *Eine* Verknüpfung *auf G ist eine Abbildung*

$$\circ : G \times G \to G.$$

An Stelle von $\circ(g, h)$ für zwei Elemente $g, h \in M$ schreiben wir $g \circ h$, und wir nennen das Bild von (g, h) das Ergebnis *der Verknüpfung.*

(ii) *Wenn wir die Menge G zusammen mit der Verknüpfung $\circ$ untersuchen, so schreiben wir meist $(G, \circ)$ und nennen sie* Gruppoid *(oder* Magma*). In diesem Zusammenhang nennen wir G auch* Grundmenge*.*

Es sind also alle im Beispiele 4.1.1 betrachteten Mengen mit den entsprechenden Abbildungen Gruppoide.

Die Stärke, die in dieser und ähnlichen Definitionen von Strukturen liegt, ist dass man die Eigenschaften der Struktur und Konsequenzen aus diesen Eigenschaften unabhängig vom tatsächlichen Beispiel untersuchen kann. Die Ergebnisse dieser Untersuchung lassen sich dann auf alle zu dieser Struktur passenden Beispiele anwenden und erlauben es dadurch auf sehr elegantem Wege neue Erkenntnissen über die Beispiele zu gewinnen.

Verknüpfungen von Elementen werden meist mit Symbolen bezeichnet. Typische Symbole sind $\circ$, $+$, $\cdot$, $*$, $\oplus$, $\otimes$, $\boxdot$, $\circledast$, …

Betrachten wir Mengen mit mehr als einer Verknüpfung, so nehmen wir auch die anderen Verknüpfungssymbole in die Bezeichnung auf, z.B. $(B, \wedge, \vee)$.

Wird die Verknüpfung mit $\circ$ oder mit $\cdot$ bezeichnet, so lässt man das Verknüpfungssymbol meist weg, sofern keine Mehrdeutigkeiten bestehen. Man schreibt dann statt $g \circ h$ einfach gh. Kommen $\circ$ und $\cdot$ vor, so läßt man (meist) $\cdot$ weg. Z.B. schreibt man $(g \circ h)k$ statt $(g \circ h) \cdot k$. Falsch wäre $(gh) \cdot k$.

Alle Strukturen, die wir in diesem Abschnitt kennen lernen werden bauen aufeinander und insbesondere auf Definition 4.1.2 auf.

Je mehr Eigenschaften eine Struktur aufweist, um so spezieller ist sie. Umgekehrt kann man aus einer spezielleren Struktur immer eine allgemeinere machen, indem man die Eigenschaften, die „zuviel“ sind, einfach *vergisst*. So ist etwa jede Gruppe (siehe Definition 4.2.16) auch eine Halbgruppe (siehe Definition 4.2.2). Die Abbildung 4.2 gibt ein grobes Diagramm der Strukturhierarchie wie wir sie in diesem Abschnitt kennen lernen werden. In dieser Ab-

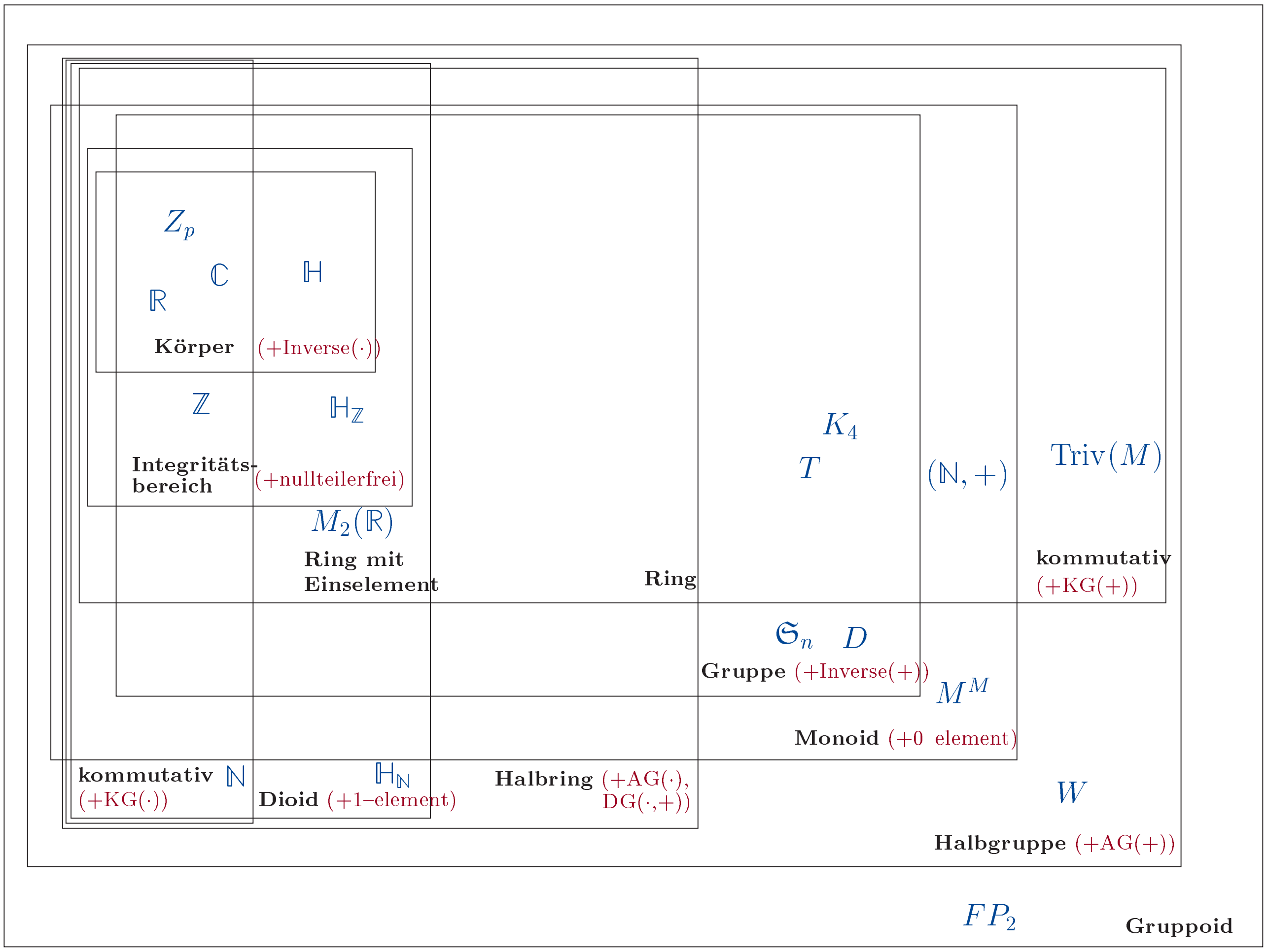

Abbildung 4.2. Hierarchie einiger algebraischer Strukturen

bildung sehen wir, dass zusätzlich geforderte Eigenschaften, jeweils angedeutet durch ein Rechteck, die Menge der passenden Strukturen einschränken. Es gilt aber immer, dass speziellere Strukturen eben speziellere Varianten von weniger speziellen (d.h. allgemeineren) Strukturen sind. So ist, wie in diesem Bild zu sehen ist, jeder Körper auch ein Ring und jeder Ring auch eine kommutative Gruppe und erst recht ein Gruppoid.

4.2. Gruppen

In diesem Abschnitt wollen wir uns zunächst auf Mengen zusammen mit einer Verknüpfung beschränken.

Beispiel 4.2.1 (Assoziativität).

$(W,\circ)$: *Sei $(W,\circ)$ die Menge aller Hauptwörter der deutschen Sprache mit dem Hintereinandersetzen als Verknüpfung. Man kann natürlich auch zusammengesetzte Hauptwörter mit weiteren Wörtern verknüpfen und dadurch längere (mehrfach) zusammengesetzte Hauptwörter konstruieren. „Dampf" und „Schiffskapitän" liefern etwa „Dampfschiffskapitän". Wenig überraschend setzen sich auch „Dampfschiff" und „Kapitän" zu „Dampfschiffskapitän" zusammen. Wir sehen also, dass das Ergebnis beim Hintereinandersetzen von „Dampf", „Schiff" und „Kapitän" das Wort „Dampfschiffskapitän" ergibt und das* unabhängig von der Reihenfolge des Zusammensetzens.

$(S,\circ)$: *Bezeichnen wir mit $(S,\circ)$ das Gruppoid der Strichblöcke mit der Zusammensetzung als Verknüpfung. Beim Zusammensetzen von drei Strichblöcken kommt es nicht darauf an, ob zuerst die ersten beiden zusammengefasst werden und danach der dritte hinzugefügt wird, oder ob zuerst die beiden hinteren verknüpft werden und danach der erste Strichblock daran gehängt wird.*

$(T,\circ)$, $(D,\circ)$: *Ebenso verhält sich die Verknüpfung zweier Translationen oder Drehungen.*

$(\mathrm{Abb}(M),\circ)$: *Allgemein ist das Hintereinander-Ausführen von Abbildungen assoziativ (das haben wir schon in Abschnitt 3.3.3 beobachtet).*

$(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{R},\cdot)$: *Auch bei der Addition natürlicher, ganzer und reeller Zahlen sowie bei der Multiplikation dieser macht es keinen Unterschied, welche einer Reihe von Verknüpfungen zuerst ausgeführt wird.*

$(M_2(\mathbb{R}),+)$: *Für 2×2–Matrizen überprüfen wir, ob $+$ diese Eigenschaft auch besitzt. Nehmen wir Elemente A, B und C aus $(M_2(\mathbb{R}),+)$. Dann finden wir*

$$\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22}\end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22}\end{pmatrix}\right) + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{pmatrix} =$$

$$\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22}\end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{pmatrix} = \begin{pmatrix} a_{11}+b_{11}+c_{11} & a_{12}+b_{12}+c_{12} \\ a_{21}+b_{21}+c_{21} & a_{22}+b_{22}+c_{22}\end{pmatrix} =$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22}\end{pmatrix} + \begin{pmatrix} b_{11}+c_{11} & b_{12}+c_{12} \\ b_{21}+c_{21} & b_{22}+c_{22}\end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22}\end{pmatrix} + \left(\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22}\end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{pmatrix}\right)$$

$(M_2(\mathbb{R}),\cdot)$: *Auch in $(M_2(\mathbb{R}),\cdot)$ verhält es sich ähnlich.*

$(\mathbb{FP}_2,\oplus)$: *Nun zum letzten Beispiel. Wir betrachten die Menge $(\mathbb{FP}_2,\oplus)$ der Gleitkommazahlen mit zwei signifikanten Stellen und der Addition mit Runden. In diesem Fall kommt es sehr wohl auf die Reihenfolge der Verknüpfungen an, denn*

$$(0.47\oplus 0.57)\oplus 0.88 = 1.0\oplus 0.88 = 1.9$$
$$0.47\oplus(0.57\oplus 0.88) = 0.47\oplus 1.5 = 2.0$$

liefert verschiedene Resultate.

Wir erkennen also: Die Eigenschaft, dass man auf die genaue Festlegung der Verknüpfungsreihenfolge verzichten kann, ist zwar (sehr) oft aber nicht immer erfüllt. Darum führen wir für solche speziellere Strukturen einen neuen Begriff ein.

Definition 4.2.2. *Ein Gruppoid $(G, \circ)$ heißt* Halbgruppe*, falls die Verknüpfung* assoziativ *ist, also das* Assoziativgesetz

$$\forall g, h, k \in G : (g \circ h) \circ k = g \circ (h \circ k)$$

gilt. In diesem Fall ist das Setzen von Klammern nicht notwendig, und wir dürfen an Stelle von $(g \circ h) \circ k$ einfach $g \circ h \circ k$ schreiben.

Beispiel 4.2.3 (Halbgruppen).

(i) *Wie schon erwartet bilden die Mengen W bis $M_2(\mathbb{R})$ mit den in Beispiel 4.1.1 definierten Verknüpfungen Halbgruppen.*
(ii) Keine *Halbgruppe ist etwa die Menge $(FP_2, \oplus)$ der Gleitkommazahlen mit zwei signifikanten Stellen mit der Addition mit Runden.*
(iii) *Immer nach der Einführung einer Struktur kann man untersuchen, welche Objekte diese Struktur beschreibt. Meist kann man schnell sehr einfach gebaute Objekte finden, die dazu passen. Abgesehen von der Halbgruppe, die nur ein Element besitzt, gibt es auch noch eine andere „triviale" Halbgruppe. Sei nämlich M eine beliebige Menge und $m \in M$ ein Element, dann definiert $m_1 \circ m_2 := m$ für alle $m_1, m_2 \in M$ eine assoziative Verknüpfung auf M, also eine Halbgruppe, die wir hier mit* $\mathrm{Triv}(M)$ *bezeichnen wollen.*

Wenn wir die mathematischen Beispiele $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{R}$ betrachten, dann wissen wir aus unserer Erfahrung, dass es die speziellen Elemente 0 und 1 gibt, die bei Addition bzw. Multiplikation ein besonders einfaches Verhalten zeigen; dieses motiviert die folgende Definition.

Definition 4.2.4. *Sei $(G, \circ)$ ein Gruppoid.*

(i) *Ein Element $e_L \in G$ heißt* Linkseinselement (linksneutrales Element)*, falls die Beziehung*

$$\forall g \in G : e_L \circ g = g$$

stimmt.
(ii) *Analog heißt ein Element $e_R \in G$* Rechtseinselement (rechtsneutrales Element)*, wenn sich bei Verknüpfung von rechts „nichts ändert":*

$$\forall g \in G : g \circ e_R = g.$$

(iii) *Ein Element $e \in G$ heißt* Einselement *oder* neutrales Element*, falls es Links- und Rechtseinselement ist, d.h. falls*

$$\forall g \in G : \ g \circ e = e \circ g = g$$

gilt. Wird die Verknüpfung mit $+$ bezeichnet (additiv geschrieben), so bezeichnet man e oft mit 0 oder $\mathbb{0}$ und nennt es Nullelement*. Einselemente bezüglich multiplikativ geschriebener Verknüpfungen erhalten auch oft die Bezeichung 1 oder $\mathbb{1}$.*

Beispiel 4.2.5 (Neutralitätseigenschaft).

$(\mathbb{N}, +), \ \ldots, (\mathbb{R}, \cdot)$: *Für die Addition von natürlichen, ganzen und reeelen Zahlen ist klarerweise 0 das Nullelement, und für die Multiplikation ist 1 das Einselement.*

$(T, \circ)$: *Die Menge T enthält die Translation der Länge 0, welche das Objekt nicht von der Stelle bewegt. (Die Richtung ist hierbei egal!) Sie ist das Einselement von T.*

$(D, \circ)$: *Die Drehung um 0 Grad (die Achse ist dabei unerheblich) ist das Einselement der Halbgruppe D.*

$(\mathrm{Abb}(M), \circ)$: *In der Menge der Abbildungen* $\mathrm{Abb}(M)$ *bildet die Identität $\mathbb{1}_M$ (vgl. Seite 56) auf M das Einselement.*

$(W, \circ)$, $(S\circ)$: *Führt man nicht künstlich leere Hauptwörter oder leere Strichblöcke ein, so enthalten W und S keine neutralen Elemente.*

$(M_2(\mathbb{R}), +)$: *Die Nullmatrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ist das Nullelement von $(M_2(\mathbb{R}), +)$.*

$(M_2(\mathbb{R}), \cdot)$: *Auch $(M_2(\mathbb{R}), \cdot)$ hat ein Einselement, nämlich die Einheitsmatrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.*

$(FP_2, \oplus)$: *Die Menge FP_2 hat ebenfalls ein Nullelement. Die Zahl 0 ist in FP_2 enthalten und besitzt alle Eigenschaften eines neutralen Elements.*

Nach Definition 4.2.4 können wir uns schon einmal fragen, welche Konsequenzen die Existenz eines Einselements hat. Die ersten beiden Ergebnisse finden wir in den folgenden Propositionen. Beim Beweis derselben, sowie bei den übrigen Beweisen in diesem Abschnitt müssen wir genauestens auf die Eigenschaften achten, die wir verwenden dürfen. Einer der beliebtesten Fehler in der Algebra ist, in Beweisen ohne zu zögern Eigenschaften der Verknüpfung zu verwenden, die gar nicht erfüllt sind — also Achtung!

Die Stärke der mathematischen Strukturtheorie gilt es auszunützen. Wir wollen zum Beispiel die interessante Frage beantworten, ob in all unseren Beispielen das angegebene Einselement das einzige Element der Grundmenge ist, das die Neutralitätseigenschaft aufweist. Um nicht jedes Beispiel einzeln untersuchen zu müssen, verwenden wir *nur* die Struktureigenschaften für den Beweis.

Proposition 4.2.6. *Ist $(G, \circ)$ ein Gruppoid mit Linkseinselement e_L und Rechtseinselement e_R, so gilt*

$$e_L = e_R =: e$$

und e ist Einselement in G

Speziell folgt daraus, dass das Einselement eines Gruppoides immer eindeutig bestimmt ist, *falls es existiert.*

Beweis. Es gilt $e_L = e_L e_R$, da e_R ein Rechtseinselement ist, und weil e_L linksneutral ist, haben wir $e_L e_R = e_R$. Aus diesen Gleichungen sieht man aber sofort $e_L = e_R$. Setzen wir $e = e_L = e_R$, so erhalten wir das gewünschte Einselement.

Gäbe es zwei Einselemente e_1 und e_2, so wäre jedes links- und rechtsneutral, und aus dem bereits gezeigten würde $e_1 = e_2$ folgen. Daher ist e eindeutig bestimmt. $\square$

Ein Element g in einem Gruppoid $(G, \circ)$ heißt *idempotent*, falls

$$g \circ g = g$$

gilt. Damit haben wir.

Proposition 4.2.7. *Ein (Links-, Rechts-) Einselement e eines Gruppoids $(G, \circ)$ ist immer idempotent.*

Beweis. Es gilt $e \circ e = e$, weil e (Links-, Rechts-) Einselement ist. $\square$

Nachdem Einselemente häufig anzutreffen sind, hat man Halbgruppen, die ein solches enthalten, einen eigenen Namen gegeben.

Definition 4.2.8. *Ist $(G, \circ)$ eine Halbgruppe und existiert ein Einselement $e \in G$, so nennt man G auch* Monoid *und schreibt oft $(G, \circ, e)$.*

Beispiel 4.2.9 (Monoide).

(i) *Sowohl* $(\mathbb{N},+)$ *als auch* $(\mathbb{N},\cdot)$ *sind Monoide. Auch* $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$ *sind Monoide, so wie* $(\mathrm{Abb}(M),\circ)$ *und* $(T,\circ)$ *bzw.* $(D,\circ)$.

(ii) *Die Menge* $(FP_2,\oplus)$ *ist kein Monoid. Sie besitzt zwar ein neutrales Element aber die Verknüpfung ist nicht assoziativ (*FP_2 *ist ja nicht einmal eine Halbgruppe!).*

(iii) $(W,\circ)$ *und* $(S,\circ)$ *sind ebenfalls keine Monoide, weil sie kein neutrales Element besitzen. Wir könnten aber durch Hinzufügen des* leeren Hauptwortes *bzw. des* leeren Strichblockes *Einselemente in* W *und* S *definieren.*

*Auf diese Weise kann man übrigens aus jeder Halbgruppe durch Hinzufügen (*Adjungieren*) eines neutralen Elements ein Monoid machen.*

Fahren wir fort, die verschiedenen Beispiele miteinander zu vergleichen. Vielleicht können wir noch weitere Eigenschaften der Verknüpfungen isolieren.

Da stoßen wir übrigens auf ein wichtiges mathematisches Prinzip. Wir spüren eine Eigenschaft auf, geben ihr einen Namen und machen sie so reif für eine Untersuchung. Kreative Namensgebung ist bereits der erste Schritt zur erfolgreichen Behandlung einer Theorie. Die Kreativität liegt dabei natürlich mehr darauf, *was* und nicht darauf *wie* etwas benannt wird — meist jedenfalls. Hätte nämlich der amerikanische Physiker George Zweig die kleinen Teilchen, aus denen die Elementarteilchen aufgebaut sind, nicht *Aces* genannt, so wäre heute sein Name berühmt und nicht der Name Murray Gell-Mann, der zur selben Zeit wie Zweig die Theorie der *Quarks* entdeckt aber den erfolgreicheren Namen gewählt hat.

Beispiel 4.2.10 (Kommutativität). *Wenn wir die Verknüpfungen untersuchen, die wir seit Beispiel 4.1.1 betrachten, dann fällt an manchen eine weitere Besonderheit auf.*

$(\mathbb{N},+),\dots,(\mathbb{R},\cdot)$**:** *Am ehesten offensichtlich ist es bei den Zahlenmengen. In allen Beispielen von* $(\mathbb{N},+)$ *bis* $(\mathbb{R},\cdot)$ *kann man erkennen, dass es beim Addieren und Multiplizieren auf die Reihenfolge der Operanden nicht ankommt. Jeder „weiß“, dass etwa* $4+5=5+4$ *und* $3\cdot 6=6\cdot 3$ *gelten.*

$(T,\circ)$**:** *Die Translationen* T *haben ebenfalls diese Eigenschaft. Egal welche von zwei Translationen zuerst durchgeführt wird, das verschobene Objekt wird am selben Platz landen.*

$(D,\circ)$**:** *Drehungen sind allerdings anders: Legen wir das Koordinatenkreuz so, dass Ursprung und Schwerpunkt des zu drehenden Objektes zusammen fallen. Drehen wir zuerst um* $90°$ *um die* x_1*–Achse und danach um* $90°$ *um die* x_3*–Achse, so ergibt das eine Gesamtdrehung um die Achse, die durch den Punkt* $(1,-1,1)$ *geht, um den Winkel* $120°$. *Vertauscht man die beiden Drehungen, dann ergibt sich eine Gesamtdrehung um die Achse durch den Punkt* $(1,1,1)$ *wieder um den Winkel* $120°$. *Die Reihenfolge, in der Drehungen ausgeführt werden, ist also wesentlich.*

$(\mathrm{Abb}(M),\circ)$**:** *Auch (allgemeine) Abbildungen darf man nicht einfach vertauschen. Sind etwa* $f:\mathbb{R}\to\mathbb{R}$, $f:x\mapsto x^2$ *und* $g:\mathbb{R}\to\mathbb{R}$, $g:x\mapsto -x$ *gegeben. Dann gilt* $f\circ g:x\mapsto x^2$, *aber* $g\circ f:x\mapsto -x^2$.

$(M_2(\mathbb{R}),+)$**:** *Bei der Addition von* 2×2*–Matrizen darf man die Terme vertauschen. Das folgt trivialerweise aus der Tatsache, dass die Addition komponentenweise definiert ist.*

$(M_2(\mathbb{R}), \cdot)$: *Die Multiplikation in $M_2(\mathbb{R})$ ist da schon problematischer. Es gilt etwa*

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}, \quad B := \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$$
$$AB = \begin{pmatrix} -1 & 5 \\ -3 & 6 \end{pmatrix}, \quad BA = \begin{pmatrix} 1 & 5 \\ -1 & 4 \end{pmatrix}$$

Das Ergebnis der Multiplikation reeller 2×2–Matrizen hängt also von der Reihenfolge der beiden Faktoren ab.

$(S, \circ)$: *Das Ergebnis der Verknüpfung von Strichblöcken S ist wieder unabhängig von der Reihenfolgen der Operanden.*

$(W, \circ)$: *Bei Worten macht es dagegen einen Unterschied. „Dampfschiff“ hat eine gänzlich andere Bedeutung als „Schiffsdampf“.*

Wir sehen also, dass manchmal die Operanden einer Verknüpfung vertauscht werden dürfen ohne das Ergebnis zu ändern, manchmal aber aber nicht. Jetzt fehlt nur noch der Name für diese Eigenschaft.

Definition 4.2.11. *Eine Verknüpfung in einem Gruppoid $(G, \circ)$ heißt* kommutativ*, falls das* Kommutativgesetz *erfüllt ist, d.h.*

$$\forall g, h \in G \Rightarrow g \circ h = h \circ g.$$

Beispiel 4.2.12 (Kommutativgesetz).

(i) *Aus unserer Beispielliste erfüllen die Zahlenmengen, die Translationen, $(M_2(\mathbb{R}, +)$ und die Strichblöcke mit den jeweiligen Verknüpfungen das Kommutativgesetz.*

(ii) *Nicht das Kommutativgesetz erfüllen hingegen die Drehungen, die Abbildungen (beide bzgl. der Hintereinanderausführung von Abbildungen), $(M_2(\mathbb{R}), \cdot)$ und die Menge der Hauptwörter (mit der Zusammensetzung).*

Und weiter führt uns unsere Entdeckungsreise durch die verschiedenen Verknüpfungseigenschaften. Die Frage ist, ob man einmal erfolgte Verknüpfungen wieder rückgängig machen kann. Bei den Translationen T kann man etwa nach jeder Verschiebung die Translation gleicher Länge aber entgegen gesetzter Richtung ausführen und damit das Objekt wieder an seinen ursprünglichen Platz zurückschieben. Translationen kann man also wieder ungeschehen machen. Wie das bei den anderen Verknüpfungen aussieht, wollen wir uns nach der folgenden Definitionen ansehen.

Definition 4.2.13. *Sei ein Gruppoid $(G, \circ, e)$ mit Einselement e gegeben.*

(i) *Ist $a \in G$, so nennen wir $a' \in G$ ein zu a* linksinverses Element*, falls*

$$a' \circ a = e.$$

(ii) *Ein Element $a' \in G$ heißt zu a* rechtsinvers*, wenn die umgekehrte Beziehung gilt, d.h.*

$$a \circ a' = e.$$

(iii) *Ist a' sowohl links- als auch rechtsinvers zu a, d.h. es gilt*

$$a' \circ a = a \circ a' = e,$$

so sagen wir a' ist ein inverses Element *von a (oder ein* Inverses zu a*) und schreiben meist a^{-1}. Ist das Verknüpfungszeichen ein $+$, schreiben wir die Operation also additiv, dann bezeichnen wir das Inverse von a üblicherweise mit $-a$.*

Beispiel 4.2.14 (Inverses).

$(\mathbb{N}, +), \dots, (\mathbb{R}, \cdot)$: *Bis zu diesem Zeitpunkt sind die Zahlenmengen brav neben einander marschiert und haben jeweils die gleichen Eigenschaften gehabt. Doch nun trennt sich die Verknüpfungsspreu vom Weizen.*

- *In* $(\mathbb{N}, +, 0)$ *gibt es außer für* 0 *zu keinem Element ein Inverses.*
- *In* $(\mathbb{Z}, +, 0)$ *und* $(\mathbb{R}, +, 0)$*, andererseits, hat jedes Element* $n \in \mathbb{Z}$ *bzw.* $n \in \mathbb{R}$ *ein inverses Element, nämlich* $-n$*.*
- *In* $(\mathbb{N}, \cdot, 1)$ *und* $(\mathbb{Z}, \cdot, 1)$ *besitzt außer* 1 *kein Element ein Inverses.*
- *In* $(\mathbb{R}, \cdot, 1)$ *hat jedes Element außer* 0 *ein Inverses.*

$(T, \circ)$: *Wir haben schon gesehen, dass die Translationen aus* T *Inverse besitzen, einfach die Verschiebung um dieselbe Länge in die Gegenrichtung.*

$(D, \circ)$: *Auch alle Drehungen in* D *haben Inverse, die Drehungen um dieselbe Achse um den negativen Winkel.*

$(\mathrm{Abb}(M), \circ)$: *In der Menge der Abbildungen* $\mathrm{Abb}(M)$ *haben nur die* bijektiven *Abbildungen Inverse (vgl. 3.3.52). Alle anderen können nicht rückgängig gemacht werden.*

$(M_2(\mathbb{R}), +)$: *In* $(M_2(\mathbb{R}), +)$ *hat jede Matrix* A *ein Inverses, nämlich diejenige Matrix* $-A$*, bei der man bei jedem Element von* A *das Vorzeichen gewechselt hat.*

$(M_2(\mathbb{R}), \cdot)$: *Für* $(M_2(\mathbb{R}), \cdot)$ *kann man beweisen (und das wird in der Linearen Algebra auch getan!) dass eine Matrix* A *genau dann ein Inverses hat, wenn* $a_{11}a_{22} - a_{12}a_{21} \neq 0$ *gilt.*

$(FP_2, \oplus)$: *Das Inverse eines Elements in* $(FP_2, \oplus)$ *ist nicht eindeutig bestimmt. Überdies zerstört das Runden i.A. die Möglichkeit die Addition rückgängig zu machen.*

Wieder stehen wir vor der Frage, ob das Inverse zu einem Element, falls es überhaupt existiert, eindeutig bestimmt ist oder ob mehr als ein (Links-, Rechts-) Inverses existieren kann. Wieder beantwortet uns die Untersuchung der Struktureigenschaften die Frage für alle Beispiele auf einmal.

Proposition 4.2.15. *Sei* $(G, \circ, e)$ *ein Monoid und* $g \in G$*. Ist* g_L^{-1} *ein Linksinverses von* g *und* g_R^{-1} *ein Rechtsinverses von* g*, d.h. gilt*

$$g_L^{-1} g = e = g g_R^{-1},$$

so ist $g_L^{-1} = g_R^{-1}. = g^{-1}$*. Speziell sind inverse Elemente in Monoiden eindeutig bestimmt, falls sie existieren.*

Beweis. Wir haben $g_L^{-1} = g_L^{-1} e = g_L^{-1}(g g_R^{-1}) = (g_L^{-1} g) g_R^{-1} = e g_R^{-1} = g_R^{-1}$. Daher sind sie gleich. Die Eindeutigkeit von Inversen folgt aus der Tatsache, dass jedes Inverse Links- und Rechtsinverses ist. $\square$

Jetzt haben wir alle Eigenschaften zusammen gesammelt und benannt und können endlich die Struktur definieren, auf die wir schon die ganze Zeit hinarbeiten.

Definition 4.2.16 (Gruppe).

(i) *Ein Monoid* $(G, \circ, e)$ *heißt* Gruppe*, falls zu jedem Element von* G *ein Inverses existiert, d.h. es gilt*

$$\forall g \in G : \exists g^{-1} \in G : g \circ g^{-1} = g^{-1} \circ g = e.$$

(ii) *Ist zusätzlich* $\circ$ *kommutativ, so spricht man von einer* kommutativen Gruppe *oder* abelschen Gruppe *(nach Nils Henrik Abel (1802–1829)).*

Gruppen werden in weiten Teilen der Mathematik benötigt. Sie beschreiben nicht nur Bewegungen sondern auch Symmetrien. Sie spielen ihre Rolle bei der Untersuchung von Differentialgleichungen genauso wie bei der Lösung von Optimierungsaufgaben oder der Lösung kombinatorischer Probleme. Zweifellos gehören Gruppen zu den zentralen Begriffen der Mathematik.

Auch im nächsten Abschnitt und in der linearen Algebra werden Gruppen gebraucht werden. Es ist also unerlässlich, diesen Begriff sorgfältig mit Fleisch (also mit Beispielen) zu füllen.

Beispiel 4.2.17 (Gruppen).

(i) *Aus unserer Beispielliste bilden die ganzen Zahlen* $(\mathbb{Z}, +, 0)$ *und die reellen Zahlen* $(\mathbb{R}, +)$ *eine abelsche Gruppe. Das selbe gilt für die Translationen und* $(M_2(\mathbb{R}), +)$

(ii) *Nicht kommutative Gruppen sind die Drehungen und* $(M_2(\mathbb{R}), \cdot)$.

(iii) *Die einelementige Menge* $M = \{e\}$ *ist eine abelsche Gruppe mit der einzig möglichen Verknüpfung* $e \circ e = e$*, sie heißt Permutationsgruppe von einem Element* $\mathfrak{S}^1$ *oder* triviale Gruppe.

Wir fassen die Eigenschaften einer Gruppe noch einmal zusammen, da sie so weit über den Abschnitt verstreut sind. Dabei wollen wir auch beweisen, dass man nur einen Teil der Eigenschaften fordern muß.

Proposition 4.2.18. *Sei* $(G, \circ)$ *ein Gruppoid. Sind folgende Eigenschaften erfüllt, dann ist* G *eine Gruppe.*

G1: *Assoziativgesetz:*

$$\forall g, h, k \in G : (g \circ h) \circ k = g \circ (h \circ k)$$

G2: *Linkseinselement:*

$$\exists e \in G : \forall g \in G : e \circ g = g$$

G3: *Linksinverse:*

$$\forall g \in G : \exists g^{-1} \in G : g^{-1} \circ g = e$$

Die Eigenschaften (G1) bis (G3) nennt man auch oft die Gruppenaxiome. *Gilt außerdem noch*

G4: *Kommutativgesetz:*

$$\forall g, h \in G : g \circ h = h \circ g,$$

dann ist G *eine abelsche Gruppe.*

Beweis. Wir haben nicht alles vorausgesetzt, was wir vorher von einer Gruppe verlangt hatten. Eigenschaft G1, das Assoziativgesetz macht $(G, \circ)$ zu einer Halbgruppe, doch wir haben nur *Links*einselement und *Links*inverse vorausgesetzt. Wir müssen also zeigen, dass das Linkseinselement auch Rechtseinselement ist und dass alle Linksinversen auch Rechtsinverse sind.

Schritt 1: Wir beginnen mit einer Teilbehauptung. Ist $g \in G$ idempotent, so gilt schon $g = e$. Wir haben nämlich

$$\begin{aligned} gg &= g \\ g^{-1}(gg) &= g^{-1}g && \text{das Linksinverse } g^{-1} \text{ existiert immer} \\ (g^{-1}g)g &= g^{-1}g && \text{Assoziativität} \\ eg &= e && \text{weil } g^{-1} \text{ Linksinverses ist} \\ g &= e && \text{weil } e \text{ Linkseinselement ist} \end{aligned}$$

Das beweist unsere Teilbehauptung.

Schritt 2: Jetzt beweisen wir, dass das Linksinverse g^{-1} auch $gg^{-1} = e$ erfüllt, also Rechtsinverses ist.

$$\begin{aligned} gg^{-1} &= g(eg^{-1}) && \text{weil } e \text{ Linkseinselement ist} \\ &= g((g^{-1}g)g^{-1}) && \text{weil } g^{-1} \text{ Linksinverses ist} \\ &= (gg^{-1})(gg^{-1}) && \text{Assoziativität.} \end{aligned}$$

Aus obiger Beziehung folgt, dass gg^{-1} idempotent ist. Wir haben aber in Schritt 1 bewiesen, dass dann schon $gg^{-1} = e$ gilt.

Schritt 3: Es bleibt noch zu zeigen, dass für alle $g \in G$ auch $ge = g$ gilt, e also Rechtseinselement ist.

$$\begin{aligned} ge &= g(g^{-1}g) && \text{weil } g^{-1} \text{ Linksinverses ist} \\ &= (gg^{-1})g && \text{Assoziativität} \\ &= eg && \text{das haben wir in Schritt 2 gezeigt} \\ &= g && e \text{ ist Linkseinselement} \end{aligned}$$

Wir haben also gezeigt, dass e Einselement ist. Darum ist $(G, \circ, e)$ ein Monoid, und jedes Element besitzt ein Inverses wegen Schritt 2. Daher ist G eine Gruppe.

Die Aussage über die Kommutativität ist trivial. □

Bemerkung 4.2.19.

(i) *Es existiert nur eine zweielementige Gruppe, nämlich* $\mathbb{Z}_2 := (\{0,1\}, +)$ *mit* $0+0 = 0$, $1 + 0 = 0 + 1 = 1$ *und* $1 + 1 = 0$.

(ii) *Ist die Menge* M *endlich, so kann man jede Verknüpfung direkt angeben, indem man den Wert jedes Elements von* $M \times M$ *in einer Tabelle, der* ***Verknüpfungstabelle*** *auch* ***Cayley–Tafel****, anschreibt.*

Für $\mathbb{Z}_2$ *würde das die Tabelle*

+	0	1
0	0	1
1	1	0

ergeben. Sie drückt aus, was wir über das Addieren gerader und ungerader Zahlen wissen (0 *ist die Äquivalenzklasse der geraden Zahlen und* 1 *diejenige der ungeraden Zahlen). Gerade plus gerade ist gerade, ungerade plus ungerade ist gerade, gerade plus ungerade ist ungerade.*

Beispiel 4.2.20. *Betrachten wir ein ebenes gleichseitiges Dreieck und alle Abbildungen, die das Dreieck auf sich selbst abbilden (solche Abbildungen nennt man* Deckabbildungen*). Es gibt sechs verschiedene solche Abbildungen:*

(1) *Die Identität* I,
(2) *Drehung um* $\frac{2}{3}\pi$ *(*$120°$*)* D_1,
(3) *Drehung um* $\frac{4}{3}\pi$ *(*$240°$*)* D_2,
(4) *Spiegelung* S_a *an der Höhe auf* a,
(5) *Spiegelung* S_b *an der Höhe auf* b,
(6) *Spiegelung* S_c *an der Höhe auf* c.

Die Menge dieser Abbildungen bildet eine Gruppe bezüglich Verknüpfung von Abbildungen. Man kann die Wirkung der Abbildung am einfachsten veranschaulichen, indem man beobachtet, wohin die Eckpunkte abgebildet werden. Die Abbildung D_1 *etwa bildet die Ecken* ABC *auf die Ecken* BCA *(in der Reihenfolge) ab. Die Spiegelung* S_a *bildet* ABC *auf* ACB *ab. Man sieht also, dass die Deckabbildungen des gleichseitigen Dreiecks genau die Permutationen der*

Eckpunkte sind. Die dabei entstehende Gruppe heißt $\mathfrak{S}^3$*, und ihre Verknüpfungstabelle ist*

$\circ$	I	S_a	S_b	S_c	D_1	D_2
I	I	S_a	S_b	S_c	D_1	D_2
S_a	S_a	I	D_2	D_1	S_c	S_b
S_b	S_b	D_1	I	D_2	S_a	S_c
S_c	S_c	D_2	D_1	I	S_b	S_a
D_1	D_1	S_b	S_c	S_a	D_2	I
D_2	D_2	S_c	S_a	S_b	I	D_1

Diese Gruppe ist die ***Permutationsgruppe*** *von drei Elementen oder auch Diedergruppe* D_3 *der Ordnung* 3*, eine* nicht abelsche *Gruppe. Sie ist sogar* die kleinste nicht abelsche Gruppe*.*

Beispiel 4.2.21. *Die Kleinsche Vierergruppe (*V_4*), auch Diedergruppe* D_2 *der Ordnung* 2 *genannt ist definiert durch die Verknüpfungstabelle*

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Sie ist übrigens die kleinste nicht-zyklische Gruppe (wobei eine Gruppe zyklisch heißt, wenn sich alle Elemente als Potenzen eines einzigen Elements schreiben lassen).

Nun wenden wir uns wieder dem Studium der abstrakten Struktur einer Gruppe zu. Zunächst zeigen wir, dass das Gesetz der doppelten Inversion auch in Gruppen gilt.

Proposition 4.2.22. *Ist* $(G, \circ)$ *eine Gruppe, so haben wir für jedes* $g \in G$

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

Beweis. Das Element $(g^{-1})^{-1}$ ist das Inverse von g^{-1}. Wir wissen aber, dass $gg^{-1} = e$ gilt. Daher ist auch g das Inverse von g^{-1}. Wegen der Eindeutigkeit der Inversen (Proposition 4.2.15) folgt $g = (g^{-1})^{-1}$. □

Achtgeben muss man, wenn man das Verhältnis von Gruppenoperation und Inversion untersucht.

Proposition 4.2.23. *Ist* $(G, \circ)$ *eine Gruppe, so gelten die Rechenregeln*

(1) $\forall g, h \in G : (g \circ h)^{-1} = h^{-1} \circ g^{-1}$ *(die Verknüpfung dreht sich um!),*

(2) $\forall g, h, k \in G : (k \circ g = k \circ h) \Rightarrow g = h$ *(es gilt die* Kürzungsregel*).*

Beweis.

(1) Es gilt $(g \circ h) \circ (h^{-1} \circ g^{-1}) = g \circ (h \circ h^{-1}) \circ g^{-1} = g \circ g^{-1} = e$. Die Aussage folgt nun aus der Eindeutigkeit der Inversen.
(2) Wir haben

$$\begin{aligned}
k \circ g &= k \circ h \\
k^{-1} \circ (k \circ g) &= k^{-1} \circ (k \circ h) \\
(k^{-1} \circ k) \circ g &= (k^{-1} \circ k) \circ h \\
e \circ g &= e \circ h \\
g &= h.
\end{aligned}$$

□

Im Folgenden werden wir Teilmengen von Gruppen studieren und dabei unser erstes Beispiel einer *Teilstruktur* kennen lernen. Wenn $H \subseteq G$ gilt und $(G, \circ, e)$ eine Gruppe ist, dann ist zunächst eine Abbildung

$$\circ : H \times H \to G$$

definiert; jedes $h \in H$ ist ja auch Element in G und daher ist für jedes Paar $(g, h) \in H \times H$ die Verknüpfung $g \circ h$ definiert. Man spricht von der von G *ererbten* oder auch *induzierten* Operationen auf H.

Besonders interessant sind nun solche Teilmengen von Gruppen, die mit der ererbten Operation dieselbe Struktur aufweisen wie ihre Obermenge, also selbst Gruppen sind.

Definition 4.2.24. *Sei $(G, \circ, e)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt* Untergruppe*, falls $(H, \circ, e)$ eine Gruppe ist.*

Beispiel 4.2.25.

- *Jede Gruppe G besitzt die beiden trivialen Untergruppen $\{e\}$ und G.*
- *Die Gruppe $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{R}, +)$.*
- *Die Gruppe $(\mathbb{Z}, +)$ besitzt etwa die Untergruppe $\mathbb{Z}_g$ aller geraden ganzen Zahlen.*

Man bezeichnet Teilstrukturen (die gleiche Struktur auf einer Teilmenge) meist mit Unter. . . oder mit Teil. . .

In der Algebra kommen etwa *Untergruppen*, *Unterringe* und *Unterkörper* vor. In der linearen Algebra spricht man von *Teilräumen*, *Teilalgebren*,. . .

Sei $H \subseteq G$ Teilmenge der Gruppe $(G, \circ, e)$. Damit $(H, \circ, e)$ eine Gruppe ist, ist es notwendig, dass

$$\forall g, h \in H : \; g \circ h \in H$$

gilt also alle Verknüpfungen von Elementen aus H wiederum in H liegen (und nicht bloß in G). Die Verknüpfung darf demnach nicht aus H herausführen. Diese Eigenschaft nennt man *Abgeschlossenheit*; genauer sagt man, dass die Verknüpfung $\circ$ auf der Teilmenge $H \subseteq G$ **abgeschlossen** ist.

Nun stellt sich die Frage, ob und welche weiteren Eigenschaften gelten müssen, damit $H \subseteq G$ zur Untergruppe wird. Die Antwort gibt die folgende Proposition.

Proposition 4.2.26. *Eine Teilmenge $H \subseteq G$ einer Gruppe $(G, \circ, e)$ ist genau dann eine Untergruppe, wenn eine der beiden äquivalenten Bedingungen gilt:*

(1) *Für alle $g, h \in H$ auch $g \circ h^{-1} \in H$*
(2) *Für alle $g, h \in H$ liegt Verknüpfung $g \circ h \in H$ und zusätzlich liegt zu jedem Element $h \in H$ auch das Inverse $h^{-1} \in H$.*

Ist G abelsch, dann auch H.

Beweis. Zuerst beweisen wir die Äquivalenz der Eigenschaften.
(1) ⇒ (2): Ist für je zwei Elemente $g, h \in H$ auch $g \circ h^{-1} \in H$, so sehen wir sofort, dass $e = g \circ g^{-1} \in H$ liegt. Damit ist aber auch zu jedem $g \in H$ das Element $e \circ g^{-1} = g^{-1} \in H$. Ferner muss dann aber für $g, h^{-1} \in H$ das Element $g \circ (h^{-1})^{-1} = g \circ h \in H$ liegen.
(2) ⇒ (1): Seien $g, h \in H$. Dann erhalten wir $h^{-1} \in H$, und daher ist auch $g \circ h^{-1} \in H$. Das beweist die behauptete Äquivalenz.

Nun zeigen wir, dass die Bedingung (2) impliziert, dass H eine Gruppe ist.

Der erste Schritt dabei ist zu zeigen, dass $(H, \circ)$ ein Gruppoid bildet, dass also $\circ$ eine Verknüpfung auf H ist. Das ist aber tatsächlich der Fall, weil wir schon wissen, dass für je zwei Elemente $g, h \in H$ auch $g \circ h \in H$ liegt. Damit ist aber H bereits eine Halbgruppe, denn das Assoziativgesetz gilt, weil es sogar für alle Elemente in G erfüllt ist.

Das Einselement e von G liegt ebenfalls in H, da für jedes Element $g \in H$ auch $g \circ g^{-1} = e \in H$ sein muss. Schließlich besitzt jedes Element $g \in H$ ein Inverses in G, nämlich g^{-1}, von dem wir bereits wissen, dass es in H liegt. Das beweist alle Gruppeneigenschaften für $(H, \circ, e)$, und daher ist H eine Untergruppe von G.

Die umgekehrte Richtung, d.h. dass für eine Untergruppe U die Eigenschaft (2) gilt, ist klar.

Nun fehlt nurmehr die Aussage über die Kommutativität, die aber ebenfalls leicht einzusehen ist. Wenn G abelsch ist, dann erfüllen alle Elemente in G das Kommutativgesetz, also erst recht alle in H. □

Ein wichtiger Begriff der Algebra fehlt noch. Wir haben jetzt aus zuvor unbedarften Mengen neue mathematische Strukturen geschaffen, indem wir auf ihnen eine Verknüpfung eingeführt haben. Dann haben wir die Eigenschaften dieser Verknüpfungen untersucht und sind so schließlich zur Definition der Gruppe gekommen. Wo sind aber die versprochenen Verbindungen zwischen unseren Gruppenobjekten? Bei den Mengen hatten wir die Abbildungen. Was sollen wir bei den Gruppen verwenden.

Die Lösung ist einfach. Gruppen sind Mengen, also können wir mit Abbildungen anfangen. Um allerdings die Gruppenstruktur nicht zu vergessen, müssen wir von den Abbildungen verlangen, dass sie die Gruppenstruktur nicht zerstören. Das führt zur folgenden Definition.

Definition 4.2.27. *Seien $(G, \circ)$ und $(H, \Box)$ Gruppoide.*

(i) *Ein* Gruppoidhomomorphismus *von G nach H ist eine Abbildung $f : G \to H$ mit*

$$\forall g_1, g_2 \in G : f(g_1 \circ g_2) = f(g_1) \Box f(g_2).$$

Das bedeutet also, dass es unerheblich ist, ob man zuerst in G verknüpft und dann nach H abbildet oder zuerst nach H abbildet und dann dort verknüpft.

(ii) *Sind G und H Halbgruppen, so heißt f auch* Halbgruppenhomomorphismus.

(iii) *Für zwei Gruppen G und H müssen wir sorgfältig darauf achten, dass wir die gesamte Gruppenstruktur beachten, und dazu gehören auch die Inversen. Eine Abbildung $f : G \to H$ heißt* Gruppenhomomorphismus *von G nach H, wenn*

$$\begin{aligned} &(1) \quad \forall g_1, g_2 \in G : \ f(g_1 \circ g_2) = f(g_1) \Box f(g_2) \\ &(2) \quad \forall g \in G : \ f(g^{-1}) = f(g)^{-1} \end{aligned}$$

Die letzte Eigenschaft bedeutet also, dass es egal ist, ob man vor der Abbildung (also in G) invertiert oder nach der Abbildung (also in H).

(iv) *Ist die Abbildung bijektiv, dann heißt sie* Gruppoid- *bzw.* Halbgruppen- *bzw.* Gruppenisomorphismus. *Man nennt in diesem Fall die beiden Gruppoide bzw. Halbgruppen bzw. Gruppen* isomorph.

Wie aus der obigen Definition bereits erahnt werden kann, werden in der Mathematik Abbildungen zwischen Mengen mit zusätzlicher Struktur, die diese Struktur erhalten **Homomorphismen** genannt und der Name der Struktur vorangestellt.

Bijektive Homomorphismen heißen **Isomorphismen**, wobei ebenfalls der Name der Struktur vorangestellt wird.

Ein Gruppenisomorphismus (wie jeder andere Isomorphismus in der Mathematik auch) ist im wesentlichen nichts anderes als eine *Umbenennung* der Gruppenelemente. Dass solche Umbenennungen mitunter sehr praktisch sein können, muss nicht extra erwähnt werden. Zwei isomorphe Strukturen sind vom Standpunkt der Strukturtheorie aus ununterscheidbar. Oftmals kann man sich bei der Untersuchung der Eigenschaften eines bestimmten Objektes damit wesentlich weiter helfen, einen Isomorphismus zu einem bereits bekannten Objekt zu konstruieren.

Beispiel 4.2.28.

- *Die Abbildung, die jedem $z \in \mathbb{Z}$ die reelle Zahl $z \in \mathbb{R}$ zuordnet, ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ in $(\mathbb{R}, +)$.*
- *Die Abbildung f von S nach $\mathbb{N}$, die jedem Strichblock die Anzahl der enthaltenen Striche zuordnet, ist ein Halbgruppenhomomorphismus von S nach $\mathbb{N}$. Haben wir zu S den leeren Strichblock hinzugefügt, dann ist $f : S \to \mathbb{N}$ bijektiv, also ein Halbgruppenisomorphismus. Die Menge der Strichblöcke ist also von den natürlichen Zahlen nicht unterscheidbar vom Standpunkt der Halbgruppentheorie aus. Die Menge S ist eine Möglichkeit, $\mathbb{N}$ zu konstruieren. Eine andere Variante, in der $\mathbb{N}$ aus den Mengenaxiomen hergeleitet wird, findet sich in Abschnitt 5.1.*

4.3. Ringe

Um uns den „Schmuckstücken" der Mathematik zu nähern, kehren wir zurück zu unseren Gruppoiden aus Beispiel 4.1.1. Einige dort betrachtete Mengen haben als doppeltes Beispiel gedient. So etwa $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{R}$ aber auch die 2×2–Matrizen $M_2(\mathbb{R})$. Für alle diese Mengen haben wir Summen und Produkte definiert. Alle diese Mengen sind also Gruppoide bezüglich zweier Verknüpfungen.

Beispiel 4.3.1 (Distributivität)**.** *Wichtig an den oben erwähnten Mengen mit Gruppoid–Strukturen bezüglich zweier Verknüpfungen ist die Eigenschaft, dass „Ausmultiplizieren" und „Herausheben" („Ausklammern") gültige Rechenregeln sind. Wir alle wissen ja, dass etwa* $(3 + 4) \cdot 5 = 3 \cdot 5 + 4 \cdot 5$ *gilt.*

Von nun an werden wir Mengen betrachten, auf denen *zwei* Verknüpfungen definiert sind. Wir schreiben die beiden Verknüpfungen $+$ und $\cdot$, vereinbaren, dass $\cdot$ stärker bindet als $+$ („Punktrechnung vor Strichrechung"), und lassen, wie schon angekündigt, den Punkt weg, wenn immer angebracht.

Definition 4.3.2 (Halbring)**.**

(i) *Eine Menge H, die eine Halbgruppe $(H, +)$ und eine Halbgruppe $(H, \cdot)$ bildet, heißt* Halbring*, falls die beiden Distributivgesetze von $+$ bezüglich $\cdot$*

 DG1: $a(b + c) = ab + ac$

 DG2: $(b + c)a = ba + ca$

erfüllt sind. Wir fassen dann beide Operationen zusammen und schreiben $(H, +, \cdot)$.

(ii) *Ist $(H, +)$ eine kommutative Halbgruppe, so sprechen wir von einem* additiv kommutativen *Halbring, ist $(H, \cdot)$ kommutativ, so nennen wir die Struktur einen* multiplikativ kommutativen *Halbring. Sind beide Verknüpfungen kommutativ, so liegt ein* kommutativer *Halbring vor.*

Beispiel 4.3.3 (Halbringe)**.**

(i) *Die natürlichen Zahlen $(\mathbb{N}, +, \cdot)$ bilden einen kommutativen Halbring. Manche nennen das sogar **Dioid**, da beide Halbgruppen $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ sogar Monoide sind.*

(ii) *Auch $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ besitzen eine Halbringstruktur. Dies folgt aus Beispiel 4.2.3 und der offensichtlichen Gültigkeit der Distributivgesetze.*

(iii) *Die interessante Frage ist: Ist $M_2(\mathbb{R})$ ebenfalls ein Halbring? Die Antwort ist ja, ein additiv kommutativer Halbring. Das Nachrechnen der Distributivgesetze ist allerdings ein bisschen mühsam, ergibt sich aber aus der Gültigkeit der Distributivgesetze für die reellen Zahlen.*

Das Nullelement der Operation $+$ in einem Halbring bezeichnen wir mit 0 und das Einselement von $\cdot$ mit 1, sofern sie existieren.

Beispiel 4.3.4. *Einige unserer Beispielmengen besitzen aber noch mehr Struktur. So ist zwar $(\mathbb{N}, +)$ keine Gruppe, sehr wohl sind aber $(\mathbb{Z}, +)$ und $(\mathbb{R}, +)$ kommutative Gruppen. Auch $(M_2(\mathbb{R}), +)$ ist eine abelsche Gruppe.*

Dies führt uns unmittelbar zum nächsten Begriff.

Definition 4.3.5 (Ring).

(i) *Ein Halbring* $(R, +, \cdot)$ *heißt* Ring, *falls zusätzlich gilt:*
  R1: $(R, +)$ *ist eine abelsche Gruppe.*

(ii) *Ist* $(R, \cdot)$ *ein Monoid und gilt* $0 \neq 1$*, so sagen wir* R *sei ein* Ring mit Einselement *und schreiben oft auch* $(R, +, \cdot, 0, 1)$*.*

(iii) *Ist die Operation* $\cdot$ *kommutativ, so liegt ein* kommutativer Ring *vor.*

(iv) *Hat man beides, Kommutativität und Einselement, dann nennt man die entstehende Struktur ganz einfach* kommutativer Ring mit Einselement*.*

Bemerkung 4.3.6. *Fassen wir nun analog zu Proposition 4.2.18 die ebenfalls etwas im Abschnitt verstreuten Ringaxiome zusammen, so ergibt sich durch einfaches Zusammensetzten der Definitionen: Eine Gruppoid* $(R, +, \cdot)$ *bezüglich zweier Verknüpfungen ist ein Ring, falls folgende Eigenschaften erfüllt sind:*

(R1): $(R, +)$ *ist abelsche Gruppe.*
(R2): $(R, \cdot)$ *erfüllt das Assoziativgesetz.*
(R3): $(R, +, \cdot)$ *erfüllt die Distributivgesetze (von* $+$ *bzgl.* $\cdot$*).*

Beispiel 4.3.7 (Ringe).

(i) *Die ganzen Zahlen* $(\mathbb{Z}, +, \cdot)$ *und die reellen Zahlen* $(\mathbb{R}, +, \cdot)$ *sind kommutative Ringe mit Einselement.*

(ii) *Die reellen* 2×2*–Matrizen bilden einen Ring mit Einselement, der aber nicht kommutativ ist.*

Einige Ringe haben wir jetzt identifiziert in unserer täglichen mathematischen Umgebung. Nun spielen wir wieder die Stärken der Algebra aus und suchen *nur an Hand der geforderten Eigenschaften* nach neuen Gesetzen, die in *allen* Ringen gelten.

Proposition 4.3.8. *Ist* $(R, +, \cdot)$ *ein Ring, so gelten die Rechenregeln*

(1) $\forall r \in R : r0 = 0r = 0,$
(2) $\forall r, s \in R : -(rs) = (-r)s = r(-s),$
(3) $\forall r, s \in R : rs = (-r)(-s).$
(4) *Besitzt* R *ein Einselement* $1 \neq 0$*, so gilt* $\forall r \in R : (-1)r = r(-1) = -r.$

Beweis.

(1) Es gilt $r0 = r(0 + 0) = r0 + r0$ und damit folgt aus der Kürzungsregel $r0 = 0$.
(2) Wir haben $(-r)s + rs = ((-r) + r)s = 0s = 0$ wegen (1). Aus der Eindeutigkeit des Inversen folgt $-(rs) = (-r)s$. Analog finden wir $r(-s) + rs = r((-s) + s) = r0 = 0$ und damit $-(rs) = r(-s)$.
(3) Aus Proposition 4.2.22 und (2) folgt $rs = -(-(rs)) = -((-r)s) = (-r)(-s)$.
(4) Es gilt $0 = 0r = (1 + (-1))r = 1r + (-1)r = r + (-1)r$ und damit $-r = (-1)r$ wegen der Eindeutigkeit der Inversen. Die zweite Gleichung zeigt man analog.

□

Genau wie für Gruppen können wir auch für Ringe Teilstrukturen definieren.

Definition 4.3.9. *Eine Teilmenge* $S \subseteq R$ *eines Ringes* $(R, +, \cdot)$ *heißt Teilring (Unterring) von* R*, falls* $(S, +, \cdot)$ *mit den induzierten Verknüpfungen ein Ring ist.*

Man muss zur Überprüfung der Tatsache, ob eine Teilmenge eines Rings ein Unterring ist, glücklicherweise nicht alle Ringeigenschaften nachprüfen. Im wesentlichen genügt es nämlich wiederum nur zu zeigen, dass die Verknüpfungen aus der Teilmenge nicht hinausführen.

Proposition 4.3.10. *Eine Teilmenge $S \subseteq R$ eines Ringes $(R, +, \cdot)$ ist ein Unterring genau dann, wenn für alle $r, s \in R$ die Elemente $r - s$ und rs in S liegen.*

Ist R kommutativ, dann auch S.

Beweis. Weil für $r, s \in S$ schon $r - s \in S$ folgt, wissen wir aus Proposition 4.2.26, dass $(S, +)$ eine Gruppe ist (eine Untergruppe von $(R, +)$). Die Verknüpfung $\cdot$ ist in H abgeschlossen, denn das haben wir vorausgesetzt. Weil aber das Assoziativgesetz und die Distributivgesetze für alle Elemente in R gelten, stimmen sie erst recht für alle Elemente von S. Daher ist S ein Ring.

Die Aussage über Kommutativität ist offensichtlich. □

Beispiel 4.3.11. *Für zwei ganze Zahlen p und q wissen wir folgende Eigenschaft: Sind $p \neq 0$ und $q \neq 0$, dann ist auch $pq \neq 0$. Auch die Menge der reellen Zahlen erfüllt das.*

In den 2×2–Matrizen können wir so schnell nicht schließen. Es gilt nämlich

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

In $M_2(\mathbb{R})$ ist also das Produkt von Null verschiedener Elemente nicht notwendigerweise auch von Null verschieden. Das ist eine bemerkenswerte Eigenschaft, die uns zur nächsten Definition führt.

Definition 4.3.12. *Ein kommutativer Ring mit Einselement $(R, +, \cdot, 0, 1)$ heißt* Integritätsbereich, *wenn für je zwei Elemente $r, s \in R$ aus $rs = 0$ schon $r = 0$ oder $s = 0$ folgt.*

Anders ausgedrückt, besitzt ein Integritätsbereich keine so genannten **Nullteiler**, wobei Nullteiler Elemente $r, s \neq 0$ mit $rs = 0$ sind.

Beispiel 4.3.13 (Integritätsbereiche)**.**

(i) *Die ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ sind ein Integritätsbereich, ebenso die reellen Zahlen $(\mathbb{R}, +, \cdot, 0, 1)$.*
(ii) *Die Matrizen $M_2(\mathbb{R})$ sind kein Integritätsbereich, denn die Multiplikation ist nicht kommutativ, und $M_2(\mathbb{R})$ ist nicht nullteilerfrei.*

Wie zu den Gruppen gehören auch zu den Ringen bestimmte Abbildungen, die sich mit der Struktur vertragen. Es ist immer das gleiche Prinzip. Ein Ring ist eine Gruppe mit etwas Zusatzstruktur, also ist ein Ringhomomorphismus ein Gruppenhomomorphismus, der „noch ein bisschen mehr kann“.

Definition 4.3.14. *Seien $(R, +, \cdot)$ und $(S, \oplus, \otimes)$ zwei Ringe.*

(i) *Ein* Ringhomomorphismus *ist ein Gruppenhomomorphismus $f : (R, +) \to (S, \oplus)$, für den zusätzlich noch*

$$\forall r, r' \in R : f(rr') = f(r) \otimes f(r')$$

gilt (der also außerdem noch ein Halbgruppenhomorphismus $(R, \cdot) \to (S, \otimes)$ ist).

(i) *Ist f bijektiv, dann heißt f* Ringisomorphismus *und man sagt, R und S sind* isomorph.

Beispiel 4.3.15. *Die Abbildung $\iota : \mathbb{R} \to M_2(\mathbb{R})$, die jeder reellen Zahl r die Matrix $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ zuordnet, ist ein Ringhomomorphismus von $(\mathbb{R}, +, \cdot)$ nach $(M_2(\mathbb{R}), +, \cdot)$. Es gilt nämlich*

$$\iota(r_1) + \iota(r_2) = \begin{pmatrix} r_1 & 0 \\ 0 & r_1 \end{pmatrix} + \begin{pmatrix} r_2 & 0 \\ 0 & r_2 \end{pmatrix} = \begin{pmatrix} r_1 + r_2 & 0 \\ 0 & r_1 + r_2 \end{pmatrix} = \iota(r_1 + r_2),$$

sowie

$$\iota(-r) = \begin{pmatrix} -r & 0 \\ 0 & -r \end{pmatrix} = -\iota(r).$$

Für die Multiplikation gilt

$$\iota(r_1)\,\iota(r_2) = \begin{pmatrix} r_1 & 0 \\ 0 & r_1 \end{pmatrix} \begin{pmatrix} r_2 & 0 \\ 0 & r_2 \end{pmatrix} = \begin{pmatrix} r_1 r_2 & 0 \\ 0 & r_1 r_2 \end{pmatrix} = \iota(r_1 r_2)$$

und

$$\iota(r_1^{-1}) = \begin{pmatrix} r_1^{-1} & 0 \\ 0 & r_1^{-1} \end{pmatrix} = \iota(r)^{-1}.$$

Dieser Ringhomomorphismus ist sogar injektiv. Man sagt er ***bettet*** $\mathbb{R}$ *in die Menge der* 2×2*–Matrizen* ***ein****. Er ist nicht surjektiv, da z.B.* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *nicht im Bild von* $\mathbb{R}$ *liegt.*

Dass ι *nicht bijektiv sein kann, wissen wir schon aufgrund folgender Tatsache: Wäre* ι *ein Ringisomoprhismus, so wären* $\mathbb{R}$ *und* $M_2(\mathbb{R})$ *aus Sicht der Ringtheorie ununterscheidbar. Das kann aber nicht sein, da* $\mathbb{R}$ *ein Integritätsbereich ist und* $M_2(\mathbb{R})$ *nicht.*

4.4. Körper

Jetzt sind wir beinahe am Ende unseres Weges angelangt. Die folgende speziellste Struktur der Algebra für Mengen mit zwei Verknüpfungen spielt in der Mathematik eine herausragende Rolle. Sie wird sowohl in der Analysis, als auch in der Linearen Algebra ein wesentlicher Begleiter sein, und daher ist es wichtig, sich die Eigenschaften möglichst gut einzuprägen.

Definition 4.4.1. *Ein Ring mit Einselement* $(K, +, \cdot)$ *heißt* Körper, *wenn zusätzlich*

K: $(K \setminus \{0\}, \cdot)$ *ist eine abelsche Gruppe*

erfüllt ist.

Beispiel 4.4.2. *Die rationalen Zahlen* $(\mathbb{Q}, +, \cdot, 0, 1)$ *bilden ebenso einen Körper wie die reellen oder komplexen Zahlen.*

Um weitere Beispiele zu finden, müssen wir ein wenig arbeiten — was wir in Beispiel 4.4.4 auch tun werden. Zunächst fassen wir aber wie schon früher für Gruppen und Ringe die definierenden Eigenschaften für Körper zusammen.

Bemerkung 4.4.3. *Eine Menge* K *mit den beiden Verknüpfungen* $+$ *und* $\cdot$ *bildet einen Körper, wenn die folgenden* ***Körperaxiome*** *gelten.*

K1: $\forall a, b, c \in K : (a + b) + c = a + (b + c)$ *(Assoziativität von +),*
K2: $\forall a, b \in K : a + b = b + a$ *(Kommutativität von +),*
K3: $\exists 0 \in K : \forall a \in K : a + 0 = a$ *(Nullelement),*
K4: $\forall a \in K : \exists (-a) \in K : a + (-a) = 0$ *(Inverse bzgl. +),*
K5: $\forall a, b, c \in K : (ab)c = a(bc)$ *(Assoziativität von ·),*
K6: $\forall a, b \in K : ab = ba$ *(Kommutativität von ·),*
K7: $\exists 1 \in K : 1 \neq 0 \wedge \forall a \in K \setminus \{0\} : a1 = a$ *(Einselement),*
K8: $\forall a \in K \setminus \{0\} : \exists a^{-1} \in K : aa^{-1} = 1$ *(Inverse bzgl. ·),*
K9: $\forall a, b, c \in K : a(b + c) = ab + ac$ *(Distributivität).*

Die Bedingungen (K1) bis (K4) machen $(R, +, 0)$ *zur abelschen Gruppe und die Bedingungen (K5)–(K8) implizieren, dass* $(R\setminus\{0\}, \cdot)$ *ebenfalls eine abelsche Gruppe ist. Schließlich sorgt das Distributivgesetz (K8) (wegen der Kommutativität gilt das zweite Distributivgesetz (DG2) dann automatisch) für die „Verträglichkeit" der beiden Operationen.*

Beispiel 4.4.4. *Die schon aus Beispiel 3.3.34 bekannten Restklassen $\mathbb{Z}_p$ bilden einen kommutativen Ring mit Einselement mit den Verknüpfungen*

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Ist p eine Primzahl, so ist $\mathbb{Z}_p$ sogar ein Körper.

Zuerst seien die Eigenschaften für Ringe überprüft: Die Operation $+$ ist wohldefiniert, *weil für je zwei verschiedene* Repräsentanten *$a, a' \in \overline{a}$ bzw. $b, b' \in \overline{b}$ gilt: $a = a' + kp$ und $b = b' + \ell p$ für geeignete $k, \ell \in \mathbb{Z}$. Dann ist aber $a + b = a' + b' + (k + \ell)p$, und damit ist $\overline{a+b} = \overline{a'+b'}$.*

*Der Ausdruck **wohldefiniert** bedeutet nicht, dass etwas „schön“ definiert ist. Diesen Ausdruck verwendet man, wenn man eine Beziehung, eine Operation, eine Abbildung für eine Klasse von Objekten dadurch definiert, dass man einen **Repräsentanten** aus der Klasse wählt und für diesen die Beziehung, Operation, Abbildung erklärt. Dann muss man nämlich überprüfen, ob diese Definition **unabhängig** von der Wahl des Repräsentanten ist oder ob die Definition etwa auf verschiedenen Elementen der Äquivalenzklasse verschiedenes bedeutet, denn das wäre schlecht.*

Ein Beispiel einer nicht wohldefinierte Operation auf $\mathbb{Z}_3$ ist $\sqrt{\overline{a}} := \overline{\sqrt{a}}$, wenn a eine Quadratzahl ist. Wollen wir $\sqrt{\overline{1}}$ berechnen, so finden wir $\sqrt{\overline{1}} = \overline{\sqrt{1}} = \overline{1}$. Gleichzeitig gilt aber $\overline{1} = \overline{4}$, und wir hätten $\sqrt{\overline{1}} = \sqrt{\overline{4}} = \overline{\sqrt{4}} = \overline{2}$, was zu einem Widerspruch führt. Die Operation $\sqrt{\ }$ wie oben eingeführt ist also nicht *wohldefiniert. Ebenso gilt für $\cdot$: $ab = (a'+kp)(b'+\ell p) = (a'b' + (a'\ell + kb' + k\ell p)p)$, und daher ist $\overline{ab} = \overline{a'b'}$. Auch $\cdot$ ist also wohldefiniert.*

Weil für ganze Zahlen (und das sind die Repräsentanten der Nebenklassen ja auch!) Assoziativgesetz, Kommutativgesetz und Distributivgesetz gelten, gelten diese Gesetze auch für $+$ und $\cdot$ auf $\mathbb{Z}_p$. Das Nullelement ist $\overline{0}$, und das Einselement $\overline{1}$ erfüllt für $p > 1$ auch $\overline{0} \neq \overline{1}$. Das additiv Inverse einer Klasse $\overline{a}$ ist leicht gefunden. Es ist $\overline{-a}$.

Um zu überprüfen, dass $\mathbb{Z}_p$ ein Körper ist, wenn p eine Primzahl ist, müssen wir nur noch beweisen, dass jedes Element $\overline{a} \neq \overline{0}$ ein Inverses besitzt. Dazu müssen wir eine Restklasse $\overline{b}$ finden mit $\overline{a} \cdot \overline{b} = \overline{1}$. Ein Satz aus der elementaren Zahlentheorie besagt folgendes:

Sind $a, b \in \mathbb{N}$ mit $\mathrm{ggT}(a, b) = 1$, so gibt es ganze Zahlen m, n mit

$$1 = ma + nb.$$

Für jede Restklasse $\overline{a}$ mit $\overline{a} \neq \overline{0}$ ist $\mathrm{ggT}(a, p) = 1$, da p Primzahl ist. Somit folgt die Existenz zweier Zahlen b, n mit $ba + np = 1$. Daher ist $\overline{b}$ das Inverse zu $\overline{a}$, und $\mathbb{Z}_p$ ist tatsächlich ein (endlicher) Körper.

In der Zahlentheorie sind die Operationen in den $\mathbb{Z}_m$ sehr wichtig. Dort hat sich eine eigene Schreibweise etabliert. Für $a + b = c$ in $\mathbb{Z}_m$ schreibt man

$$a + b \equiv c \mod m$$

*und spricht: „a plus b **kongruent** c **modulo** m“. Ebenso für das Produkt*

$$a \cdot b \equiv c \mod m.$$

Im folgenden wenden wir uns wieder dem Studium der abstrakten Struktur zu.

Proposition 4.4.5. *Ist $(K, +, \cdot)$ ein Körper, so gelten die Rechenregeln*

1. $\forall a, b \in K : (ab)^{-1} = a^{-1}b^{-1}$.
2. $\forall a \in K : (-a)^{-1} = -a^{-1}$,

Beweis.

(1) Wir haben $(ab)(a^{-1}b^{-1}) = aa^{-1}bb^{-1} = 1 \cdot 1 = 1$. Der Rest folgt wieder aus der Eindeutigkeit der Inversen.
(2) Es gilt $-a = (-1)a$ wegen Proposition 4.3.8.(4) und somit ist $(-1)^{-1} = -1$. Aus Proposition 4.3.8.(3) folgt $1 = 1 \cdot 1 = (-1)(-1)$. Schließlich erhalten wir unter Verwendung von (1) $(-a)^{-1} = ((-1)a)^{-1} = (-1)^{-1}a^{-1} = (-1)a^{-1} = -a^{-1}$.

□

Analog zu Ringen kann man auch wieder Unterkörper definieren:

Definition 4.4.6. *Eine Teilmenge $Q \subseteq K$ eines Körpers $(K, +, \cdot)$ heißt* Unterkörper, *wenn $(Q, +, \cdot)$ selbst ein Körper ist.*

Beispiel 4.4.7. *Die rationalen Zahlen $\mathbb{Q}$ sind ein Unterkörper der reellen Zahlen $\mathbb{R}$. Diese sind wiederum ein Unterkörper der komplexen Zahlen $\mathbb{C}$.*

Proposition 4.4.8. *Eine Teilmenge Q eines Körpers $(K, +, \cdot)$ ist genau dann ein Unterkörper, wenn eine der folgenden äquivalenten Bedingungen gilt.*

(1) *Für je zwei Elemente $a, b \in Q$ ist sowohl $a - b \in Q$ als auch, sofern $b \neq 0$, $ab^{-1} \in Q$.*
(2) *Für je drei Elemente $a, b, c \in Q$ mit $c \neq 0$ ist auch $(a - b)c^{-1} \in Q$.*

Beweis. Dies folgt aus Proposition 4.2.26 für $(K, +)$ und $(K, \cdot)$. Ferner beachte man, dass $(a - 0)c^{-1} = ac^{-1}$ und $(a - b)1^{-1} = a - b$ gelten. □

Beispiel 4.4.9. *Seien auf*

$$K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

die folgenden Operationen definiert:

$$(a_1 + b_1\sqrt{2}) \oplus (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$
$$(a_1 + b_1\sqrt{2}) \otimes (a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_2b_1 + a_1b_2)\sqrt{2}.$$

Bei genauerer Betrachtung sehen wir, dass $\oplus$ und $\otimes$ genau die von $\mathbb{R}$ ererbten Operationen $+$ und $\cdot$ sind. Wir untersuchen also:

$$(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in K,$$

und für $(a_2, b_2) \neq (0, 0)$

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})^{-1} = \frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} = \frac{(a_1 + b_1\sqrt{2})(a_2 - b_2\sqrt{2})}{a_2^2 - 2b_2^2} =$$
$$= \frac{a_1a_2 - 2b_1b_2}{a_2^2 - 2b_2^2} + \frac{a_2b_1 - a_1b_2}{a_2^2 - 2b_2^2}\sqrt{2}.$$

Dieses Ergebnis liegt in K, sofern $a_2^2 - 2b_2^2 \neq 0$ gilt. Dies ist aber wahr, da nicht beide a_2 und b_2 gleich Null sein dürfen. Darüber hinaus gilt noch, dass $a_2^2 \neq 2b_2^2$ sein muss, weil a_2 und b_2 rational sind, $\sqrt{2}$ aber irrational ist. Daher sind die Voraussetzungen von Proposition 4.4.8 erfüllt, und K ist in der Tat ein Unterkörper von $\mathbb{R}$. Wir schreiben auch $K = \mathbb{Q}[\sqrt{2}]$.

Nach den Definitionen der Struktur und den Beispielen müssen wir uns ein weiteres Mal um die Abbildungen kümmern. Das Prinzip ist wieder dasselbe wie schon zuvor. Jeder Körper ist ein Ring mit zusätzlichen Eigenschaften, also ist ein Körperhomomorphismus — bitte raten! — genau, ein Ringhomomorphismus, der auch diese zusätzlichen Eigenschaften respektiert.

Definition 4.4.10. *Seien $(K, +, \cdot)$ und $(K', \oplus, \otimes)$ zwei Körper.*

(i) *Ein* Körperhomomorphismus *ist ein Gruppenhomomorphismus* $f : (K, +) \to (K', \oplus)$, *der auch noch ein Gruppenhomomorphismus* $f : (K \setminus \{0\}, \cdot) \to (K' \setminus \{0\}, \otimes)$ *ist.*
(ii) *Ist* f *bijektiv, so nennt man die Abbildung* Körperisomorphismus *und sagt, die beiden Körper* K *und* K' *sind* isomorph.

Beispiel 4.4.11. *Definieren wir auf* $\mathbb{Q} \times \mathbb{Q}$ *die Verknüpfungen*

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) := (a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1)$$

dann ist $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ *ein Körper.*

Wir überprüfen das, indem wir die Körperaxiome nachrechnen:

K1: *Seien* $a, b, c \in \mathbb{Q} \times \mathbb{Q}$. *Wir finden*

$$\begin{aligned}(a + b) + c &= \big((a_1, a_2) + (b_1, b_2)\big) + (c_1, c_2) = (a_1 + b_1, a_2 + b_2) + (c_1, c_2) = \\ &= (a_1 + b_1 + c_1, a_2 + b_2 + c_2) = (a_1, a_2) + (b_1 + c_1, b_2 + c_2) = \\ &= (a_1, a_2) + \big((b_1, b_2) + (c_1, c_2)\big) = a + (b + c).\end{aligned}$$

K2: *Nehmen wir beliebige* $a, b \in \mathbb{Q} \times \mathbb{Q}$. *Es gilt*

$$\begin{aligned}a + b &= (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) = \\ &= (b_1 + a_1, b_2 + a_2) = (b_1, b_2) + (a_1, a_2) = b + a.\end{aligned}$$

K3: *Für* $0 := (0, 0) \in \mathbb{Q} \times \mathbb{Q}$ *gilt*

$$a + 0 = (a_1, a_2) + (0, 0) = (a_1 + 0, a_2 + 0) = (a_1, a_2) = a.$$

K4: *Sei* $a \in \mathbb{Q} \times \mathbb{Q}$ *gegeben. Wir definieren* $-a := (-a_1, -a_2) \in \mathbb{Q} \times \mathbb{Q}$ *und berechnen*

$$a + (-a) = (a_1, a_2) + (-a_1, -a_2) = (a_1 + (-a_1), a_2 + (-a_2)) = (0, 0) = 0.$$

K5: *Für alle* $a, b, c \in \mathbb{Q} \times \mathbb{Q}$ *folgt*

$$\begin{aligned}(ab)c &= \big((a_1, a_2)(b_1, b_2)\big)(c_1, c_2) = (a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1)(c_1, c_2) = \\ &= \big((a_1b_1 + 2a_2b_2)c_1 + 2(a_1b_2 + a_2b_1)c_2, (a_1b_1 + 2a_2b_2)c_2 + (a_1b_2 + a_2b_1)c_1\big) = \\ &= \big(a_1b_1c_1 + 2a_2b_2c_1 + 2a_1b_2c_2 + 2a_2b_1c_2, a_1b_1c_2 + a_1b_2c_1 + a_2b_1c_1 + 2a_2b_2c_2\big) = \\ &= \big(a_1(b_1c_1 + 2b_2c_2) + 2a_2(b_1c_2 + b_2c_1), a_1(b_1c_2 + b_2c_1) + a_2(b_1c_1 + 2b_2c_2)\big) = \\ &= (a_1, a_2)(b_1c_1 + 2b_2c_2, b_1c_2 + b_2c_1) = \\ &= (a_1, a_2)\big((b_1, b_2)(c_1, c_2)\big) = a(bc).\end{aligned}$$

K6: *Es seien wieder* $a, b \in \mathbb{Q} \times \mathbb{Q}$. *Wir rechnen nach:*

$$\begin{aligned}ab &= (a_1, a_2)(b_1, b_2) = (a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1) = \\ &= (b_1a_1 + 2b_2a_2, b_1a_2 + b_2a_1) = (b_1, b_2)(a_1, a_2) = ba.\end{aligned}$$

K7: *Wir definieren* $1 := (1, 0) \in \mathbb{Q} \times \mathbb{Q}$. *Klarerweise gilt* $0 \neq 1$, *und außerdem für* $a \in \mathbb{Q} \times \mathbb{Q}$

$$a1 = (a_1, a_2)(1, 0) = (a_1 1 + 0, 0 + a_2 1) = (a_1, a_2) = a.$$

K8: *Sei* $0 \neq a \in \mathbb{Q} \times \mathbb{Q}$ *gegeben. Wir definieren* $a^{-1} := \left(\frac{a_1}{a_1^2 - 2a_2^2}, \frac{-a_2}{a_1^2 - 2a_2^2}\right)$. *Es gilt* a^{-1} *ist für alle* $a \neq 0$ *definiert. Zu diesem Zweck muss* $a_1^2 - 2a_2^2 \neq 0$ *gelten. Das folgende Argument beweist das: Sei* $a_1^2 = 2a_2^2$. *Dann gilt auch, falls* $a_2 \neq 0$ *stimmt, dass* $(a_1/a_2)^2 = 2$. *Die linke Seite dieser Gleichung ist das Quadrat einer rationale Zahl. Das Quadrat einer rationalen Zahl kann aber niemals gleich 2 sein, da andernfalls*

$\sqrt{2}$ rational wäre. Folglich ist $a_2 = 0$. Dann haben wir aber auch $a_1 = 0$ und damit $a = 0$, was wir ausgeschlossen haben.

Es ist a^{-1} also für alle $a \neq 0$ definiert. Nun können wir rechnen

$$\begin{aligned} aa^{-1} &= (a_1, a_2)(a_1/(a_1^2 - 2a_2^2), -a_2/(a_1^2 - 2a_2^2)) = \\ &= \big((a_1^2 - 2a_2^2)/(a_1^2 - 2a_2^2), 0\big) = (1, 0) = 1. \end{aligned}$$

K9: *Seien wieder $a, b, c \in \mathbb{Q} \times \mathbb{Q}$. Auch das letzte Axiom ist eine längliche Rechnung:*

$$\begin{aligned} ab + ac &= (a_1, a_2)(b_1, b_2) + (a_1, a_2)(c_1, c_2) = \\ &= (a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1) + (a_1c_1 + 2a_2c_2, a_1c_2 + a_2c_1) = \\ &= (a_1b_1 + a_1c_1 + 2a_2b_2 + 2a_2c_2, a_1b_2 + a_1c_2 + a_2b_1 + a_2c_1) = \\ &= \big(a_1(b_1 + c_1) + 2a_2(b_2 + c_2), a_1(b_2 + c_2) + a_2(b_1 + c_1)\big) = \\ &= (a_1, a_2)(b_1 + c_1, b_2 + c_2) = (a_1, a_2)\big((b_1, b_2) + (c_1, c_2)\big) = a(b + c). \end{aligned}$$

Wir haben also alle Eigenschaften nachgeprüft, und daher ist $(\mathbb{Q}\times\mathbb{Q}, +, \cdot)$ wirklich ein Körper.

Als nächstes definieren wir eine Abbildung $f : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}[\sqrt{2}]$ durch $(a_1, a_2) \mapsto a_1 + a_2\sqrt{2}$. Die Abbildung ist offensichtlich bijektiv, und es gilt

$$\begin{aligned} f(a + b) &= f((a_1, a_2) + (b_1, b_2)) = f((a_1 + b_1, a_2 + b_2)) = (a_1 + b_1) + (a_2 + b_2)\sqrt{2} = \\ &= (a_1 + a_2\sqrt{2}) \oplus (b_1 + b_2\sqrt{2}) = f(a) \oplus f(b), \\ f(-a) &= f((-a_1, -a_2)) = -a_1 + (-a_2)\sqrt{2} = \ominus(a_1 + a_2\sqrt{2}) = \ominus f(a), \\ f(ab) &= f((a_1, a_2)(b_1, b_2)) = f((a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1)) = \\ &= (a_1b_1 + 2a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2} = (a_1 + a_2\sqrt{2}) \otimes (b_2 + b_2\sqrt{2}) = f(a) \otimes f(b), \\ f(a^{-1}) &= f(a_1/(a_1^2 - 2a_2^2), -a_2/(a_1^2 - 2a_2^2)) = \frac{a_1}{a_1^2 - 2a_2^2} + \frac{-a_2}{a_1^2 - 2a_2^2}\sqrt{2} = \\ &= (a_1 + a_2\sqrt{2})^{-1} = f(a)^{-1}. \end{aligned}$$

Daher ist f ein Körperisomorphismus, deshalb ist $(\mathbb{Q}\times\mathbb{Q}, +, \cdot)$ isomorph zu $\mathbb{Q}[\sqrt{2}]$. Die beiden Strukturen sind also identisch bis auf Umbenennen der Elemente.

Abschließend beweisen wir noch, dass der Körper wirklich die speziellste aller hier vorgestellten Strukturen ist.

Proposition 4.4.12. *Jeder Körper ist ein Integritätsbereich.*

Beweis. Seien a und b Elemente des Körpers mit $ab = 0$. Ist $a \neq 0$, dann existiert a^{-1}, und es folgt

$$\begin{aligned} ab &= 0 \\ a^{-1}(ab) &= a^{-1}0 \\ (a^{-1}a)b &= 0 \\ 1b &= 0 \\ b &= 0. \end{aligned}$$

Umgekehrt folgt aus $b \neq 0$ sofort $a = 0$. Der Körper ist also nullteilerfrei. □

Diese letzte Proposition schließt unsere algebraischen Untersuchungen ab. Aufbauend auf den Körperaxiomen werden in der Linearen Algebra darüber hinaus gehend neue Strukturen erschaffen werden wie die eines **Vektorraumes**. Für die Analysis werden wir genauere Untersuchungen der rationalen, reellen und komplexen Zahlen benötigen. Alle diese Mengen sind mit den bereits bekannten Rechengesetzen ausgestattet und bilden Körper.

In der (höheren) Algebra wird mit der genaueren Untersuchung der Strukturen selbst fortgefahren werden. Man wird Fragen stellen wie: Welche Arten von Gruppen (Ringen, Körpern) gibt es? Kann man alle endlichen Gruppen (Ringe, Körper) finden? Alle diese Fragen und viele andere werden zum Ausbau der mathematischen Theorie beitragen und teilweise tief gehende Resultate hervorbringen.

KAPITEL 5

Zahlenmengen

Der letzte Abschnitt wird uns zurück zu den konkreten Dingen führen. Wir werden uns wieder mit Zahlen beschäftigen. Nach der langen Wanderung durch die Grundbegriffe der Mathematik wie Logik, Mengenlehre und elementare Algebra, kehren wir zurück zu den Anfängen der Mathematik.

Wir haben im Verlauf der vergangenen Kapitel häufig die verschiedenen Zahlenmengen als Beispiel verwendet. Wir sind durch den täglichen Umgang mit den Zahlen überzeugt, sie zu beherrschen, ihre Eigenschaften zu kennen. Es scheint uns, dass wir mit ihnen völlig vertraut sind.

Doch trügt der Schein nicht? Was ist $\sqrt{2}$ eigentlich? Haben wir diese Zahl wirklich verstanden? Das Hinterfragen dessen, was wir zu wissen glauben, die kritische Analyse, ist eines der Grundprinzipen der modernen Naturwissenschaft.

Im Gegensatz zu zuvor wollen wir aber jetzt den bereits mathematisch geschulten Blick auf das richten, was wir bereits zu kennen glaubten. Wir werden unser Wissen über Mengenlehre und mathematische Strukturen anzuwenden versuchen und die Zahlen selbst in einem etwas veränderten Licht betrachten.

Das Kapitel ist in zwei Teile geteilt, die munter durcheinander gemischt erscheinen. Nur Farben trennen den vergleichsweise beschreibenden Zugang zu den Zahlenmengen vom axiomatischen Zugang, bei dem die Zahlenmengen direkt aus dem Zermelo–Fraenkelschen Axiomensystem ZFC konstruiert werden.

5.1. Die natürlichen Zahlen $\mathbb{N}$

> „Die natürlichen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.“
> Leopold Kronecker (1823–1891)

> „Die natürlichen Zahlen sind freie Schöpfungen des menschlichen Geistes.“
> Richard Dedekind (1831–1916)

Die natürlichen Zahlen sind schon seit langer Zeit bekannt. Sie entstanden historsich gesehen aus dem natürlichen Zählbegriff. Die Null als Zeichen und als eigenständige Zahl wurde aber erst Ende des Mittelalters akzeptiert. Wahrscheinlich stammt das Zeichen aus Indien. Die Null ist Element der natürlichen Zahlen. Wir definieren das so, und auch die DIN Norm 5473 stimmt damit überein.

Demnach ist

$$\mathbb{N} := \{0, 1, 2, 3, 4, \dots\}.$$

Definiert sind für $\mathbb{N}$ die Addition $+$, die Multiplikation $\cdot$, mit denen $\mathbb{N}$ einen kommutativen Halbring mit 0 und 1 (ein Dioid) ohne Nullteiler bildet (siehe Beispiel 4.3.3). Ferner ist eine Totalordnung (Definition 3.3.35) $\leq$ erklärt, die verträglich mit den Verknüpfungen ist:

O1: Ist $a \leq b$, so ist für alle $c \in \mathbb{N}$ auch $a + c \leq b + c$,
O2: Sind $x > 0$ und $y > 0$, so ist $xy > 0$.

Die Menge $\mathbb{N}$ ist also ein geordnetes Dioid bezüglich Addition und Multiplikation. Sie ist die kleinstmächtige unendliche Menge, und es gilt $|\mathbb{N}| = \aleph_0$ (siehe Ende Kapitel 3).

Die einfachste axiomatische Beschreibung von $\mathbb{N}$, die die Punkte in obiger Beschreibung exakt macht, stammt aus dem 19. Jahrhundert und wurde von Giuseppe Peano gegeben.

Bemerkung 5.1.1. *Die natürlichen Zahlen sind eine Menge $\mathbb{N}$ zusammen mit einer Vorschrift S die die* ***Peano Axiome*** *erfüllt:*

PA1: 0 *ist einen natürliche Zahl, d.h.* $0 \in \mathbb{N}$,

PA2: *Jeder natürlichen Zahl wird genau eine natürliche Zahl $S(n)$ zugeordnet, die ihr* Nachfolger *genannt wird, d.h.*

$$\forall n \in \mathbb{N} : (S(n) \in \mathbb{N}),$$

PA3: 0 *ist kein Nachfolger, i.e.,*

$$\forall n \in \mathbb{N} : \neg(S(n) = 0),$$

PA4: *Sind zwei natürliche Zahlen verschieden, so sind das auch ihre Nachfolger, d.h.*

$$\forall n \in \mathbb{N} : \forall m \in \mathbb{N} : ((S(n) = S(m)) \Rightarrow n = m),$$

PA5: *Enthält eine Menge M natürlicher Zahlen die Zahl 0 und mit jeder Zahl ihren Nachfolger, so ist $M = \mathbb{N}$, genauer*

$$\forall M \in \mathbb{P}\mathbb{N} : (\psi(M) \Rightarrow M = \mathbb{N}),$$

wobei wir hier die Nachfolgereigenschaft

$$\psi(Y) := \forall x : (0 \in Y \wedge (x \in Y \Rightarrow S(x) \in Y)).$$

verwendet haben.

Das letzte Axiom postuliert übrigens das Induktionsprinzip.

5.1.1. Mengentheoretische Konstruktion von $\mathbb{N}$. Die Konstruktion der natürlichen Zahlen aus ZFC (den Axiomen der Mengenlehre von Zermelo und Fraenkel) funktioniert folgendermaßen.

Wir definieren

$$\begin{aligned}
&0 := \emptyset\\
&1 := S(0) = 0 \cup \{0\} = \{\emptyset\}\\
&2 := S(1) = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\}\\
&3 := S(2) = 2 \cup \{2\} = \Big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\Big\}
\end{aligned}$$

$$n := \begin{cases} \emptyset & n = 0 \\ S(n) = n \cup \{n\} & n \neq 0 \end{cases}$$

Somit erhalten wir in Kurzform $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$ und allgemein $n = \{0, 1, \dots, n-1\}$. Jede Zahl ist also identifiziert als die Menge, die alle kleineren Zahlen enthält.

So stellen wir uns das jedenfalls vor. Die Konstruktoren, die wir verwendet haben, sind alle bereits definiert, und ZF7 garantiert uns, dass eine Menge existiert, die alle diese Zahlen n enthält. Leider wissen wir zwei Dinge noch nicht, nämlich ob es eine Menge gibt die **genau alle** diese Zahlen enthält, denn nur dann ist sie eindeutig bestimmt (und das, was wir uns naiv unter $\mathbb{N}$ vorstellen).

Theorem 5.1.2. *Sei die Nachfolgereigenschaft* ψ

$$\psi(Y) := \forall X : (\emptyset \in Y \wedge (X \in Y \Rightarrow S(X) \in Y)).$$

gegeben. Dann gilt

$$\exists! \mathbb{N} : \forall M : (\psi(\mathbb{N}) \wedge (\psi(M) \Rightarrow \mathbb{N} \subseteq M)).$$

Mit anderen Worten, es gibt genau eine Menge der natürlichen Zahlen. Sie ist die kleinste Menge, die die Nachfolgereigenschaft besitzt.

Beweis. Wegen ZF7 gibt es eine Menge Z, die die Eigenschaft $\psi(Z)$ besitzt. Wir definieren $\mathcal{N} := \{M \in \mathbb{P}Z \mid \psi(M)\}$. Sei nun $\mathbb{N} := \bigcap \mathcal{N}$. (Für eine Mengenfamilie $\mathcal{F}$ ist $\bigcap \mathcal{F}$ definiert durch $\bigcap \mathcal{F} := \{x \in \bigcup \mathcal{F} \mid \forall F \in \mathcal{F} : (x \in F)\}$.)

Dann gilt $\forall M \in \mathcal{N} : \psi(M)$, und daher $\forall M \in \mathcal{N} : (\emptyset \in M)$, also auch $\emptyset \in \mathbb{N}$. Ferner wissen wir $X \in \mathbb{N} \Rightarrow (\forall M \in \mathcal{N} : (X \in M))$, deshalb $\forall M \in \mathcal{N} : (S(X) \in M)$, was wiederum $S(X) \in \mathbb{N}$ zur Folge hat. Daher gilt $\psi(\mathbb{N})$.

Um Eindeutigkeit zu zeigen, nehmen wir an, dass $\exists M : \psi(M)$ (etwa ein M, das nicht Teilmenge von Z ist). Mit denselben Argumenten wie oben können wir zeigen, dass $\psi(Z \cap M)$ gilt, sowie $(Z \cap M) \subseteq M$ und $\mathbb{N} \subseteq Z \cap M$, was $\mathbb{N} \subseteq M$ impliziert. □

Korollar 5.1.3. *Es gilt das Induktionsprinzip*

$$\forall M \in \mathbb{P}\mathbb{N} : (\psi(M) \Rightarrow M = \mathbb{N}).$$

Beweis. Sei $M \in \mathbb{P}\mathbb{N}$ beliebig. Gilt $\psi(M)$, so ist $M \subseteq \mathbb{N}$, und nach Voraussetzung gilt $\mathbb{N} \subseteq M$, und daher ist $M = \mathbb{N}$. □

Diese (etwas unintuitive) Version der Konstruktion der natürlichen Zahlen ist viel mächtiger als die Definitionen, die im neunzehnten Jahrhundert gegeben wurden. Das sieht man allein daran, dass man das Induktionsprinzip *beweisen* kann und nicht als Axiom fordern muss. Alle fünf von Peano für die natürlichen Zahlen angegebenen Axiome kann man leicht überprüfen.

Proposition 5.1.4. *Die Menge der natürlichen Zahlen* $\mathbb{N}$ *erfüllt die Peano Axiome.*

Beweis. Die Axiome PA1 und PA2 gelten wegen der Definition von $\mathbb{N}$ und PF5 haben wir in Korollar 5.1.3 gezeigt. Es bleiben also nur noch PA3 und PA4.

PA3 beweisen wir indirekt. Sei also $n \in \mathbb{N}$ gegeben mit $S(n) = 0$. Dann ist $S(n) = n \cup \{n\} = \emptyset$, doch es gilt $n \in S(n)$, und daher $S(n) \neq \emptyset$. Dieser Widerspruch beweist PA3.

Zum Beweis von PA4 nehmen wir an, dass $m, n \in \mathbb{N}$ sind mit $S(n) = S(m)$. Sei $k \in n$. Dann ist auch $k \in n \cup \{n\} = S(n) = S(m) = m \cup \{m\}$, also $k \in m$ oder $k \in \{m\}$ wegen der Eigenschaften von $\cup$. Weil aber die Menge $\{m\}$ nur ein Element, nämlich m enthält, folgt daraus die Tatsache $k \in m \vee k = m$. Ist $k = m$, so gilt $n \in k \vee n = k$, weil $n \in S(n) = S(m) = S(k)$, und daher widerspricht entweder $\{n, k\}$ oder $\{k\}$ dem Fundierungsaxiom ZF9. Daher gilt $k \in m$ und auch $n \subseteq m$. Analog zeigt man durch Vertauschen von m und n die Relation $m \subseteq n$, und es folgt $n = m$. Dies beweist auch PA4, und wir sind fertig. □

Die arithmetischen Operationen $+$ und $\cdot$ definiert man ebenfalls über S. Die Totalordnung $\leq$ ist einfach

$$m \leq n :\Leftrightarrow (m \in n \vee m = n).$$

Proposition 5.1.5. *Die Relation* $\leq$ *ist eine Totalordnung.*

Beweis. Reflexivität und Transitivität sind offensichtlich, und wäre die Antisymmetrie nicht erfüllt, dann existierten zwei natürliche Zahlen $m \neq n \in \mathbb{N}$ mit $n \leq m$ und $m \leq n$, also mit $m \in n$ und $n \in m$. Gäbe es diese Zahlen, dann könnten wir die Menge $\{m, n\}$ bilden, welche ZF9 widerspräche. Daher ist die Antisymmetrie erfüllt, und $\leq$ ist eine Halbordnung.

Um zu beweisen, dass $\leq$ eine Totalordnung ist, müssen wir zeigen, dass für je zwei Zahlen $m, n \in \mathbb{N}$ entweder $m < n$ oder $m = n$ oder $m > n$ gilt.

Beweisen wir zwei Hilfsresultate zuerst:

HB1. $\forall m, n \in \mathbb{N} : (m \in n \Rightarrow S(m) \subseteq n)$.
Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : (m \in n \Rightarrow S(m) \subseteq n)\}$. Die 0 erfüllt die Bedingung trivialerweise, daher ist $0 \in M$. Sei nun $n \in M$. Gilt $m \in S(n) = n \cup \{n\}$, so ist entweder $m = n$ oder $m \in n$. Ist $m = n$, so ist $S(m) = S(n)$ und daher gilt $S(m) \subseteq S(n)$. Ist hingegen $m \in n$, so gilt wegen $n \in M$ auch $S(m) \subseteq n \subseteq S(n)$, und somit gilt immer $S(m) \subseteq S(n)$. Daher ist auch $S(n) \in M$ und wegen Korollar 5.1.3 folgt $M = \mathbb{N}$. Dies beweist HB1.

HB2. $\forall m, n \in \mathbb{N} : ((m \subseteq n \wedge m \neq n) \Rightarrow m \in n)$.
Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : ((m \subseteq n \wedge m \neq n) \Rightarrow m \in n)\}$. Ist $m \subseteq 0$, so ist $m = 0$ und daher $0 \in M$. Sei nun $n \in M$. Wir betrachten $S(n)$, und daher sei $m \in \mathbb{N}$ mit $m \subseteq S(n) \wedge m \neq S(n)$. Ist $k \in m$, so gilt wegen $S(n) = n \cup \{n\}$, dass entweder $k \in n$ oder $k = n$. Ist $k = n$, so ist $n \in m$ und wegen HB1 folgt dann $S(n) \subseteq m$. Dies ist aber ein Widerspruch zu $m \subseteq S(n) \wedge m \neq S(n)$. Daher gilt $\forall k \in m : k \in n$, also $m \subseteq n$. Ist $m = n$, dann haben wir $m \in n \cup \{n\} = S(n)$. Sonst gilt $m \subseteq n \wedge m \neq n$, und weil $n \in M$ vorausgesetzt ist auch $m \in n$. Dies impliziert aber $m \in S(n)$, und $S(n) \in M$. Aus Korollar 5.1.3 folgt $M = \mathbb{N}$, was HB2 beweist.

Sei $M = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : (m < n \vee m = n \vee n < m)\}$. Betrachten wir zuerst 0. Ist $0 \neq n$, so gilt $0 = \emptyset \subseteq n$, also $0 \in n$ wegen HB2, und daher $0 \in M$. Sei nun $n \in M$. Betrachten wir $S(n)$. Sei $m \in \mathbb{N}$ gegeben. Gelten $m \in n$ oder $m = n$, so haben wir $m \in n \cup \{n\} = S(n)$. Gilt andererseits $n \in m$, so folgt aus HB1, dass $S(n) \subseteq m$. Ist $S(n) \neq m$, so ist $S(n) \in m$ wegen HB2. Es gilt also $m \in S(n) \vee m = S(n) \vee S(n) \in m$, und daher $S(n) \in M$. Verwenden wir ein weiteres Mal Korollar 5.1.3, so sehen wir $M = \mathbb{N}$ und wir sind fertig. □

Die arithmetische Operation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ sei unser nächstes Opfer. Wir definieren

$$n + 0 = n$$
$$n + S(m) = S(n + m)$$

und finden das folgende Resultat

Proposition 5.1.6. *Es gibt genau eine Abbildung $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, die obige rekursive Definition erfüllt.*

Beweis. Beginnen wir mit der Eindeutigkeit. Seien $+$ und $\boxplus$ zwei Funktionen, die die rekursive Definition erfüllen. Setzen wir $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : (m + n = m \boxplus n)\}$. Natürlich ist $0 \in M$ wegen $n + 0 = n = n \boxplus 0$. Sei nun $n \in N$, dann haben wir für $m \in \mathbb{N}$ die Gleichung $m + S(n) = S(m + n) = S(m \boxplus n)$ wegen $n \in N$ und $S(m \boxplus n) = m \boxplus S(n)$, und daher $S(n) \in M$. Aus Korollar 5.1.3 folgt $M = \mathbb{N}$, und daher ist $+ = \boxplus$ als Teilmenge von $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$. Wir dürfen noch nicht von Abbildung reden, da wir die Abbildungseigenschaft noch nicht nachgewiesen haben. Dies können wir mit einem ählichen Induktionsargument erreichen.

Sei für jedes $m \in \mathbb{N}$ die „Abbildung" $+_m : \mathbb{N} \to \mathbb{N}$ definiert durch $+_0(n) = n$ und $+_{S(m)}(n) = S(+_m(n))$. Dies macht $+_m$ zu einer Relation, aber wir werden unten die Abbildungseigenschaft nachweisen:
Sei $M := \{m \in \mathbb{N} \mid \forall n \in \mathbb{N} : \forall j \leq m : \exists! k \in \mathbb{N} : (+_j(n) = k)\}$. Wegen $\forall n \in \mathbb{N} : (+_0(n) = n)$ folgt sofort $0 \in M$. Ist $m \in M$, dann ist $+_0(n) = n$ eindeutig. Sei also $j \leq m$. Dann

existiert für beliebiges $n \in \mathbb{N}$ genau ein k mit $+_j(n) = k$. Also ist für $S(j)$ die Beziehung $+_{S(j)}(n) = S(+_j(n)) = S(k)$ erfüllt. Somit ist auch $S(m) \in M$, da für $j \in \mathbb{N}$ mit $j \leq S(m)$ entweder $j = 0$ ist oder ein $j' \in \mathbb{N}$ existiert mit $j = S(j')$ und $j' \leq m$. Somit impliziert Korollar 5.1.3 aber $M = \mathbb{N}$. Daher ist für jedes $m \in \mathbb{N}$ die Relation $+_m$ tatsächlich eine Abbildung, und $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ist dann als Abbildung definiert durch $n + m = +_m(n)$ für alle $m, n \in \mathbb{N}$. $\square$

Mit ähnlichen Induktionsbeweisen zeigt man noch, dass die arithmetische Operation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ rekursiv definiert werden kann durch

$$\begin{aligned} n \cdot 0 &= 0 \\ n \cdot S(m) &= (n \cdot m) + n \end{aligned}$$

Theorem 5.1.7. *Die natürlichen Zahlen* $(\mathbb{N}, +, \cdot)$ *bilden einen kommutativen Halbring mit* 0 *und* 1.

Beweis. Zeigen wir zunächst, dass $(\mathbb{N}, +)$ eine kommutative Halbgruppe ist.

BH1: $\forall n \in \mathbb{N} : S(m) + n = m + S(n)$.
Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : S(m) + n = m + S(n)\}$. Es gilt $S(0) + 0 = S(0)$ und $0 + S(0) = S(0 + 0) = S(0)$ und daher $0 \in M$. Sei nun $n \in M$. Wir betrachten $S(n)$ und erhalten für $m \in \mathbb{N}$ die Beziehung $S(m)+S(n) = S(S(m)+n) = S(m+S(n)) = m + S(S(n))$ nach Definition von $+$ und weil $n \in M$. Daher ist auch $S(n) \in M$ und Korollar 5.1.3 liefert uns $M = \mathbb{N}$.

BH2: $\forall n \in \mathbb{N} : 0 + n = n$.
Sei $M := \{n \in \mathbb{N} \mid 0+n = n\}$. Dann ist $0 \in M$ wegen $0+0 = 0$. Sei nun $n \in M$ und betrachten wir $S(n)$. Wir erhalten $0 + S(n) = S(0 + n) = S(n)$ aus der Definition von $+$ und weil $n \in M$. Daraus und aus der Definition folgt, dass 0 ein Nullelement ist.

KG(+): $\forall n, m \in \mathbb{N} : n + m = m + n$.
Diese Beziehung zeigen wir ebenfalls mit Induktion. Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : m + n = n + m\}$. Wegen BH2 und der Definition von $+$ gilt für alle $n \in \mathbb{N}$ die Gleichung $0 + n = n + 0$ und daher $0 \in M$. Sei nun $n \in M$. Dann rechnen wir für beliebiges $m \in \mathbb{N}$ wie folgt: $S(n)+m = n+S(n) = S(n+m) = S(m+n) = m+S(n)$. Zweimal haben wir die Definition von $+$ verwendet und je einmal die Tatsache $n \in M$ und BH1. Daher ist $S(n) \in M$, und wegen Korollar 5.1.3 gilt $M = \mathbb{N}$. Daher ist $+$ kommutativ.

AG(+): $\forall k, m, n \in \mathbb{N} : (k + n) + m = k + (n + m)$.
Ein weiterer Induktionsbeweis wird uns das Assoziativgesetz zeigen. Wir definieren $M := \{m \in \mathbb{N} : \forall k, n \in \mathbb{N} : (k + n) + m = k + (n + m)\}$, und wieder gilt $0 \in M$, diesmal wegen $(k + n) + 0 = k + n = k + (n + 0)$. Ist $m \in M$, dann rechnen wir für beliebige $k, n \in \mathbb{N}$

$$\begin{aligned} (k + n) + S(m) = S((k + n) + m) = S(k + (n + m)) = \\ = k + S(n + m) = k + (n + S(m)). \end{aligned}$$

Das beweist $S(m) \in M$ und damit $M = \mathbb{N}$ wegen Korollar 5.1.3. Also ist $+$ assoziativ und $(\mathbb{N}, +)$ ein kommutatives Monoid.

BH3: $\forall n \in \mathbb{N} : 0 \cdot n = 0$.
Induktion mit $M = \{n \in \mathbb{N} \mid 0 \cdot n = 0\}$. $0 \in M$ wegen der Definition $0 \cdot 0 = 0$. Ist $n \in M$, so ist auch $S(n) \in M$ wegen $0 \cdot S(n) = (0 \cdot n) + 0 = 0 + 0 = 0$. Korollar 5.1.3 impliziert wieder $M = \mathbb{N}$.

BH4: $\forall n \in \mathbb{N} : S(0) \cdot n = n \cdot S(0) = n$, also $S(0)$ ist Einselement.
Die erste Gleichung $n \cdot S(0) = n \cdot 0 + n = 0 + n = n$ folgt direkt aus den Definitionen von $\cdot$ und $+$. Die zweite Gleichung benötigt einen Induktionsbeweis. Sei $M := \{n \in \mathbb{N} \mid S(0) \cdot n = n\}$. Es ist $0 \in M$ nach Definition von $\cdot$, und ist $n \in M$, so können wir rechnen

$$S(0) \cdot S(n) = (S(0) \cdot n) + S(0) = n + S(0) = S(n + 0) = S(n).$$

Daher ist $S(n) \in M$ und $M = \mathbb{N}$ wegen Korollar 5.1.3.

BH5: $\forall n, m \in \mathbb{N} : S(n) \cdot m = n \cdot m + m$.
Dieser erste Schritt zur Kommutativität folgt aus Korollar 5.1.3 nach Definition von $M := \{m \in \mathbb{N} \mid \forall n \in \mathbb{N} : S(n) \cdot m = n \cdot m + m\}$. Es gilt nämlich wegen $S(n) \cdot 0 = 0 = (n \cdot 0) + 0$, dass $0 \in M$ ist. Gilt nun $m \in M$, dann haben wir für beliebiges $n \in \mathbb{N}$

$$\begin{aligned} S(n) \cdot S(m) &= (S(n) \cdot m) + S(n) = (n \cdot m) + m + S(n) = \\ &= (n \cdot m) + S(m) + n = (n \cdot m) + n + S(m) = \\ &= (n \cdot S(m)) + S(m) \end{aligned}$$

und damit $S(m) \in M$.

KG($\cdot$): $\forall m, n \in \mathbb{N} : m \cdot n = n \cdot m$.
Diesmal setzen wir $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : m \cdot n = n \cdot m\}$. Es ist wegen der Definition von $\cdot$ und BH3 $0 \in M$. Ist $n \in M$, so auch $S(n)$ wegen $m \cdot S(n) = (m \cdot n) + m = (n \cdot m) + m = S(n) \cdot m$. Hier haben wir die Definition und BH5 verwendet. Es ist also $M = \mathbb{N}$ wegen Korollar 5.1.3.

DG: $\forall k, m, n \in \mathbb{N} : k \cdot (m + n) = (k \cdot m) + (k \cdot n)$.
Sei $M = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N} : k \cdot (m+n) = (k \cdot m) + (k \cdot n)\}$. Dann ist $0 \in M$ wegen $0 \cdot (m + n) = 0 = 0 + 0 = (0 \cdot m) + (0 \cdot n)$. Haben wir $k \in M$, so ist auch $S(k) \in M$ wegen Definitionen, Eigenschaften von $+$ und BH4

$$\begin{aligned} S(k) \cdot (m + n) &= (k \cdot (m + n)) + (m + n) = (k \cdot m) + (k \cdot n) + m + n = \\ &= (k \cdot m) + m + (k \cdot n) + n = (S(k) \cdot m) + (S(k) \cdot n). \end{aligned}$$

Aus Korollar 5.1.3 erhalten wir $M = \mathbb{N}$.

AG($\cdot$): $\forall k, m, n \in \mathbb{N} : (k \cdot m) \cdot n = k \cdot (m \cdot n)$.
Setzen wir diesmal $M := \{n \in \mathbb{N} \mid \forall k, m \in \mathbb{N} : (k \cdot m) \cdot n = k \cdot (m \cdot n)\}$. Es ist $0 \in M$ erfüllt, weil $(k \cdot m) \cdot 0 = 0 = k \cdot 0 = k \cdot (m \cdot 0)$. Ist nun $n \in M$ und sind $k, m \in \mathbb{N}$ beliebig, so rechnen wir nach dem zuvor bewiesenen

$$\begin{aligned} (k \cdot m) \cdot S(n) &= ((k \cdot m) \cdot n) + (k \cdot m) = (k \cdot (m \cdot n)) + (k \cdot m) = \\ &= k \cdot ((m \cdot n) + m) = k \cdot (m \cdot S(n)). \end{aligned}$$

Verwenden wir ein letztes Mal Korollar 5.1.3, so erhalten wir $M = \mathbb{N}$.

Somit haben wir alle erforderlichen Eigenschaften eines kommutativen Halbrings mit 0 und 1 nachgewiesen. □

Die Vorrangregel $\cdot$ vor $+$ führen wir ein, um uns überflüssige Klammerung zu ersparen. Wir haben nun die natürlichen Zahlen mit ihren Rechenoperationen eingeführt. Wir lassen in Zukunft auch das Multiplikationszeichen weg, wenn dadurch keine Zweideutigkeit entsteht.

Theorem 5.1.8. *Die Ordnungsrelation $\leq$ und die arithmetischen Operationen $+$ und $\cdot$ sind verträglich.*

(1) $\forall k, m, n \in \mathbb{N} : (m \leq n \Rightarrow k + m \leq k + n)$,
(2) $\forall k, \ell, m, n \in \mathbb{N} : ((m \leq n \wedge k \leq \ell) \Rightarrow k + m \leq \ell + n)$,
(3) $\forall k, m, n \in \mathbb{N} : (n + k \leq n + m \Rightarrow k \leq m)$,

(4) $\forall k, m, n \in \mathbb{N} : (m \leq n \Rightarrow km \leq kn)$,
(5) $\forall k, m, n \in \mathbb{N} : ((n \neq 0 \wedge nk \leq nm) \Rightarrow k \leq m)$.

Beweis. Im gesamten Beweis definieren wir eine Menge M und beweisen $0 \in M$ und die Implikation $n \in M \implies S(n) \in M$. Dann verwenden wir Korollar 5.1.3, um $M = \mathbb{N}$ zu schließen.

Zu Beginn beweisen wir die Hilfsbehauptung $\forall m, n \in \mathbb{N} : (m \leq n \Leftrightarrow S(m) \leq S(n))$. Es gelten

$$\begin{aligned} m \leq n \Rightarrow m \in n \vee m = n \Rightarrow S(m) \subseteq n \vee S(m) = S(n) \Rightarrow \\ \Rightarrow (S(m) \subseteq S(n) \wedge S(m) \neq S(n)) \vee S(m) = S(n) \Rightarrow \\ \Rightarrow S(m) \in S(n) \vee S(m) = S(n) \Rightarrow S(m) \leq S(n). \end{aligned}$$

und

$$\begin{aligned} S(m) \leq S(n) \Rightarrow S(m) \in S(n) \vee S(m) = S(n) \Rightarrow S(m) \in n \cup \{n\} \vee m = n \Rightarrow \\ \Rightarrow S(m) \in n \vee S(m) = n \vee m = n \Rightarrow m \in n \vee m = n \Rightarrow m \leq n, \end{aligned}$$

was die Hilfsbehauptung zeigt.

(1) $M := \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N} : (m \leq n \Rightarrow k + m \leq k + n)\}$. Trivial ist $0 \in M$. Für $k \in M$ wissen wir

$$m \leq n \Rightarrow k + m \leq k + n \Rightarrow S(k + m) \leq S(k + n) \Rightarrow S(k) + m \leq S(k) + n.$$

Daher ist $S(k) \in M$.

(2) Es gilt $k \leq \ell$ und daher ist $k+m \leq \ell+m$. Wegen $m \leq n$ gilt außerdem $\ell+m \leq \ell+n$. Aus der Transitivität von $\leq$ folgt schließlich $k + m \leq \ell + n$.

(3) Sei $M := \{n \in \mathbb{N} \mid \forall k, m \in \mathbb{N} : (n + k \leq n + m \Rightarrow k \leq m)\}$. Es gilt wieder trivialerweise $0 \in M$ und für $n \in M$ finden wir wegen

$$S(n) + k \leq S(n) + m \Rightarrow S(n + k) \leq S(n + m) \Rightarrow n + k \leq n + m \Rightarrow k \leq m$$

und $S(n) \in M$.

(4) $M := \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N} : (m \leq n \Rightarrow km \leq kn)\}$. Trivial sind $0 \in M$, da $0 \leq 0$, und $S(0) \in M$. Für $k \in M$ wissen wir

$$m \leq n \Rightarrow km \leq kn \Rightarrow km + m \leq kn + n \Rightarrow S(k)m \leq S(k)n.$$

Daher ist $S(k) \in M$.

(5) Sei $M := \{k \in \mathbb{N} \mid \forall n, m \in \mathbb{N} : ((n \neq 0 \wedge nk \leq nm) \Rightarrow k \leq m)\}$. Es gilt trivialerweise $0 \in M$, und für $k \in M$ finden wir

$$nS(k) \leq nm \Rightarrow nk + n \leq nm. \tag{5.4}$$

Nun unterscheiden wir zwei Fälle. Ist $m = 0$, so muss $nk + n = 0$ sein, da die einzige Zahl $z \in \mathbb{N}$ mit $z \leq 0$ die 0 ist. Das ist aber nur möglich, wenn $n = 0$ ist; dies ist aber nicht erlaubt. Also gilt $m \neq 0$, und damit existiert $m' \in \mathbb{N}$ mit $m = S(m')$. Wir folgern in Gleichung (5.4) weiter

$$\begin{aligned} nk + n \leq nS(m') \Rightarrow nk + n \leq nm' + n \Rightarrow nk \leq nm' \Rightarrow \\ \Rightarrow k \leq m' \Rightarrow S(k) \leq S(m') = m. \end{aligned}$$

Daher ist auch $S(k) \in M$ und $M = \mathbb{N}$.

□

Theorem 5.1.9. *Im Halbring $(\mathbb{N}, +, \cdot)$ gelten die folgenden Regeln:*

(1) *Aus $nm = 0$ folgt bereits $n = 0$ oder $m = 0$.*
(2) *Aus $n + m = n + k$ folgt $m = k$.*

(3) *Aus $nm = nk$ für $n \neq 0$ folgt $m = k$.*

Beweis.

(1) Sei $n \neq 0$ und $m \neq 0$. Dann gibt es $m', n' \in \mathbb{N}$ mit $n = S(n')$ und $m = S(m')$ und wir erhalten $mn = S(m')S(n') = m'S(n') + S(n') = m'n' + m' + S(n') = S(m'n' + m' + n') \neq 0$ wegen PA3.

(2) Sei $M := \{n \in \mathbb{N} \mid \forall m, k \in \mathbb{N} : (n + m = n + k \Rightarrow m = k)\}$. Dann ist $0 \in M$ weil aus $0 + m = 0 + k$ trivialerweise $m = k$ folgt. Sei nun $n \in M$. Dann gilt wegen Definitionen und PA4

$$S(n) + m = S(n) + k \Rightarrow S(n + m) = S(n + k) \Rightarrow n + m = n + k \Rightarrow m = k.$$

Daher ist $S(n) \in M$ und $M = \mathbb{N}$ wegen Korollar 5.1.3.

(3) Aus $nm = nk$ können wir $nm \leq nk$ folgern, und daraus wegen Theorem 5.1.8 Punkt (5) auch $m \leq k$. Da wir analog auch $nk \leq nm$ und daraus $k \leq m$ schließen können, folgt der Rest aus der Antisymmetrie der Ordnungsrelation.

Damit hätten wir alle Behauptungen bewiesen. □

5.2. Die ganzen Zahlen $\mathbb{Z}$

Die ganzen Zahlen sind die zweite Zahlenmenge, die in der Schule eingeführt wird. Um keine Probleme mit der Umkehrung der Addition, der Subtraktion $-$ zu erhalten, führt man die *negativen Zahlen* ein, die Ergebnisse, wenn man größere Zahlen von kleineren subtrahiert. Zu jeder natürlichen Zahl n gibt es eine negative Zahl $-n$ mit $n + (-n) = 0$. Auf diese Weise wird $\mathbb{Z}$ zu einer abelschen Gruppe bezüglich der Addition. Wir haben

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}.$$

Zusammen mit der Addition $+$ und der Multiplikation $\cdot$ bildet $\mathbb{Z}$ einen Integritätsbereich. Ferner kann man die Totalordnung von $\mathbb{N}$ auf $\mathbb{Z}$ fortsetzen, indem man erklärt $-n \leq -m :\Leftrightarrow m \leq n$ und $-m \leq 0$ für alle natürlichen Zahlen m. Diese Ordnungsrelation erfüllt dann dieselben Verträglichkeitsbedingungen **O1** und **O2** wie sie schon in $\mathbb{N}$ gelten.

Die ganzen Zahlen sind gleich mächtig wie $\mathbb{N}$. Es gilt also $|\mathbb{Z}| = \aleph_0$.

5.2.1. Mengentheoretische Konstruktion von $\mathbb{Z}$. Machen wir nun den nächsten Schritt und versuchen wir eine mengentheoretische Konstruktion der ganzen Zahlen.

Gehen wir dazu von $\mathbb{N}$ aus. Bis jetzt ist dies ja die einzige unendliche Zahlenmenge, die wir aus den Axiomen konstruiert haben. Bilden wir $\mathbb{N} \times \mathbb{N}$, die Paare natürlicher Zahlen. Definieren wir eine Relation $\sim$ auf $\mathbb{N} \times \mathbb{N}$ durch

$$(m, n) \sim (m', n') :\Longleftrightarrow m + n' = m' + n$$

Proposition 5.2.1. *Die Relation $\sim$ ist eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$.*

Beweis. Die Reflexivität ist offensichtlich erfüllt, ebenso wie die Symmetrie. Kommen wir zur Transitivität. Seien $(m, n) \sim (m', n')$ und $(m', n') \sim (m'', n'')$. Dann gelten $m + n' = m' + n$ und $m' + n'' = m'' + n'$. Daher wissen wir $m + n' + m'' = m' + n + m''$ und daraus wiederum folgt $m + m' + n'' = m' + n + m''$. Verwenden wir nun Eigenschaft 2 aus Theorem 5.1.9, so erhalten wir $m + n'' = m'' + n$ und $(m, n) \sim (m'', n'')$. □

Wir definieren $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/_\sim$ als Faktormenge bezüglich der oben definierten Relation. Nun wollen wir die Operationen $+$ und $\cdot$ und die Relation $\leq$ auch auf $\mathbb{Z}$ definieren.

+: Wir definieren

$$[(m_1, m_2)] + [(n_1, n_2)] := [(m_1 + n_1, m_2 + n_2)].$$

Dies ist wohldefiniert. Seien (m_1, m_2) und (m_1', m_2') zwei verschiedene Repräsentanten von $[(m_1, m_2)]$. Dann gilt $m_1 + m_2' = m_1' + m_2$ und wir erhalten

$$\begin{aligned}(m_1 + n_1) + (m_2' + n_2) &= (m_1 + m_2') + (n_1 + n_2) = \\ &= (m_1' + m_2) + (n_1 + n_2) = \\ &= (m_1' + n_1) + (m_2 + n_2).\end{aligned}$$

Daher ist $(m_1 + n_1, m_2 + n_2) \sim (m_1' + n_1, m_2' + n_2)$. Analog weist man die wohldefiniertheit im zweiten Term nach.

$\cdot$: Für die Multiplikation setzen wir

$$[(m_1, m_2)] \cdot [(n_1, n_2)] := [(m_1 n_1 + m_2 n_2, m_1 n_2 + m_2 n_1)].$$

Auch das ist wohldefiniert, wie man leicht nachrechnet.

$\leq$: Die Ordnungsrelation führt man auch zurück auf die Relation in $\mathbb{N}$:

$$[(m_1, m_2)] \leq [(n_1, n_2)] :\iff m_1 + n_2 \leq n_1 + m_2.$$

Diese Relation ist wohldefiniert, was man leicht nachrechnet. Sie ist auch offensichtlich reflexiv. Sie ist symmetrisch, weil aus $[(m_1, m_2)] \leq [(n_1, n_2)]$ und $[(n_1, n_2)] \leq [(m_1, m_2)]$ und den Eigenschaften von $\leq$ auf $\mathbb{N}$ die Beziehung $m_1 + n_2 = n_1 + m_2$, also $(m_1, m_2) \sim (n_1, n_2)$ und daher $[(m_1, m_2)] = [(n_1, n_2)]$ folgt.

Die Transitivität erhält man so: $[(m_1, m_2)] \leq [(n_1, n_2)]$ impliziert $m_1 + n_2 \leq n_1 + m_2$, und aus $[(n_1, n_2)] \leq [(k_1, k_2)]$ folgt $n_1 + k_2 \leq k_1 + n_2$. Aus Theorem 5.1.8 erhalten wir

$$m_1 + n_2 + k_2 \leq n_1 + m_2 + k_2 \leq k_1 + n_2 + m_2,$$

woraus schließlich $m_1 + k_2 \leq k_1 + m_2$ folgt, also $[(m_1, m_2)] \leq [(k_1, k_2)]$.

Jetzt haben wir die Grundoperationen definiert. Es bleibt noch, ihre Eigenschaften zu beweisen.

Theorem 5.2.2. *Die ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ sind ein Integritätsbereich.*

Beweis. Verifizieren wir zuerst, dass $(\mathbb{Z}, +)$ eine abelsche Gruppe ist:

G1: Es gilt $([(m_1, m_2)] + [(n_1, n_2)]) + [(k_1, k_2)] = [(m_1, m_2)] + ([(n_1, n_2)] + [(k_1, k_2)])$, weil die Operation komponentenweise definiert ist und $+$ auf $\mathbb{N}$ assoziativ ist.

G2: Das Element $[(0, 0)]$ ist neutrales Element, wie man sofort einsieht.

G3: Sei $[(m_1, m_2)] \in \mathbb{Z}$ beliebig. Dann ist das Element $[(m_2, m_1)]$ ein Inverses bezüglich der Addition.
Es gilt $[(m_1, m_2)] + [(m_2, m_1)] = [(m_1 + m_2, m_1 + m_2)] = [(0, 0)]$.

G4: Das Kommutativgesetz ist erfüllt, weil es in $(\mathbb{N}, +)$ gilt und die Operation in $\mathbb{Z}$ komponentenweise auf Repräsentanten definiert ist.

Nun müssen wir zeigen, dass $(\mathbb{Z}, \cdot)$ ein kommutatives Monoid ist:

M1: Es gilt $([(m_1, m_2)][(n_1, n_2)])[(k_1, k_2)] = [(m_1, m_2)]([(n_1, n_2)][(k_1, k_2)])$. Das sieht man nach langer aber einfacher Rechnung ein.

M2: Das Element $[(1, 0)]$ ist Einselement. Das ist leicht.

M3: Es gilt das Kommutativgesetz $[(m_1, m_2)][(n_1, n_2)] = [(n_1, n_2)][(m_1, m_2)]$. Das folgt unmittelbar aus der Definition.

D: Ebenso mühsam aber einfach nachzurechnen wie das Assoziativgesetz ist das Distributivgesetz.

Was bleibt, ist die Freiheit von Nullteilern zu zeigen. Seien $[(m_1, m_2)]$ und $[(n_1, n_2)]$ zwei Elemente von $\mathbb{Z}$ mit $[(m_1, m_2)][(n_1, n_2)] = [(0, 0)]$. Aus dieser Beziehung folgt mit Hilfe der Definitionen von $\cdot$ und $\sim$ die Beziehung

$$m_1 n_1 + m_2 n_2 = m_1 n_2 + m_2 n_1. \tag{5.5}$$

Hilfsbehauptung: Wir zeigen nun, dass für je vier Zahlen $m, n, k, \ell \in \mathbb{N}$ aus

$$mk + n\ell = m\ell + nk \quad \wedge \quad m \neq n$$

schon $k = \ell$ folgt. Wie immer beweisen wir das mit vollständiger Induktion. Sei

$$M := \{n \in \mathbb{N} \mid \forall k, \ell, m \in \mathbb{N} : \big((mk + n\ell = m\ell + nk \wedge m \neq n) \Rightarrow k = \ell\big)\}.$$

Dann gilt $0 \in M$, weil

$$mk + 0\ell = m\ell + 0k \Rightarrow mk = m\ell \Rightarrow k = \ell \quad \text{wegen } m \neq n = 0 \text{ und Theorem 5.1.9.}$$

Sei nun $n \in M$. Dann untersuchen wir

$$mk + S(n)\ell = m\ell + S(n)k$$

Für $m = 0$ haben wir $0k+S(n)\ell = 0\ell+S(n)k$, woraus sofort $\ell = k$ folgt wegen Theorem 5.1.9 (3). Sei also nun $m \neq 0$ und $m \neq S(n)$. Dann existiert $m' \in \mathbb{N}$ mit $S(m') = m$, und wir können unter Verwendung von Theorem 5.1.9 rechnen

$$\begin{aligned} mk + S(n)\ell &= m\ell + S(n)k \\ mk + n\ell + \ell &= m\ell + nk + k \\ S(m')k + n\ell + \ell &= S(m')\ell + nk + k \\ m'k + k + n\ell + \ell &= m'\ell + \ell + nk + k \\ m'k + n\ell &= m'\ell + nk. \end{aligned}$$

Falls $n \neq m'$ gilt, dann können wir aus $n \in M$ schon $\ell = k$ folgern. Das ist aber der Fall, weil $S(m') = m \neq S(n)$ vorausgesetzt war. Daher ist auch $S(n) \in M$ und aus Korollar 5.1.3 folgt $M = \mathbb{N}$ und die Hilfsbehauptung.

Kehren wir zurück zu unserer Beziehung (5.5). Aus der Hilfsbehauptung erhalten wir für $m_1 \neq m_2$ die Folgerung $n_1 = n_2$, also $[(n_1, n_2)] = [(0, 0)]$. Gilt andererseits $m_1 = m_2$, so bedeutet das $[(m_1, m_2)] = [(0, 0)]$ und wir schließen die Nichtexistenz von Nullteilern. $\square$

Wir können sehr leicht nachrechnen, dass für die Elemente $[(n, 0)]$ dieselben Rechenregeln gelten wie für natürliche Zahlen n. Außerdem sind alle diese Zahlen verschieden ($n \neq m \Rightarrow [(n, 0)] \neq [(m, 0)]$). Es ist also $\mathbb{N} \subseteq \mathbb{Z}$ mit dieser Identifikation. Wir schreiben in Zukunft auch n für diese Elemente. Es ist nun das Inverse bzgl. $+$ von n die Klasse $[(0, n)]$, und wir schreiben für dieses Element von $\mathbb{Z}$ kurz $-n$. Die Elemente $[(n, 0)]$ und $[(0, n)]$ für $n \in \mathbb{N}$ sind auch schon alle Elemente in $\mathbb{Z}$, da

$$([m_1, m_2]) = m_1 + (-m_2) = \begin{cases} ([m_1 - m_2, 0]) & \text{falls } m_1 \geq m_2 \\ ([0, m_2 - m_1]) & \text{falls } m_1 < m_2. \end{cases}.$$

Damit haben wir endlich die uns vertraute Form der ganzen Zahlen als „$\pm\mathbb{N}$" erreicht.

Es gilt für alle $n, m \in \mathbb{N}$, dass $[(n, 0)] \leq [(m, 0)]$ genau dann, wenn $n \leq m$. Das folgt direkt aus der Definition. Ebenfalls aus der Definition folgt sogleich $[(0, n)] \leq [(0, m)]$, dann und nur dann wenn $m \leq n$ ist. Schließlich kann man noch aus der Definition ablesen, dass für $\mathbb{N} \ni n \neq 0$ die Ungleichungen $[(0, n)] < [(0, 0)] < [(n, 0)]$ gelten. Die natürlichen Zahlen entsprechen also genau den *positiven* Elementen von $\mathbb{Z}$, und die Elemente $-n$ sind die *negativen* Elemente (die negativen Zahlen).

Theorem 5.2.3. *Für die Ordnungsrelation von $\mathbb{Z}$ finden wir die folgenden Eigenschaften.*

(1) $\forall m, n \in \mathbb{Z} : (m \le n \implies -m \ge -n)$,
(2) $\forall k, m, n \in \mathbb{Z} : (m \le n \Rightarrow m + k \le n + k)$,
(3) $\forall m, n \in \mathbb{Z} : ((m > 0 \land n > 0) \Rightarrow mn > 0)$,
(4) $\forall k, m, n \in \mathbb{Z} : ((k > 0 \land m \le n) \Rightarrow km \le kn)$,
(5) $\forall k, m, n \in \mathbb{Z} : ((k < 0 \land m \le n) \Rightarrow km \ge kn)$,
(6) $\forall k, m, n \in \mathbb{Z} : ((k > 0 \land km \le kn) \Rightarrow m \le n)$

Beweis.

(1) Sind die Vorzeichen von m und n verschieden, so wissen wir $m \le 0 \le n$ und daher $-m \ge 0 \ge -n$. Sind m und n positiv, so sind $-m = [(0, m)]$ und $-n = [(0, n)]$. Wegen $m \le n$ gilt nach Definition von $\le$ auf $\mathbb{Z}$ die Beziehung $-m \ge -n$. Haben wir umgekehrt $m \le n \le 0$, so impliziert das analog zu oben $-m \ge -n$.
(2) Sind $m = [(m_1, m_2)]$, $n = [(n_1, n_2)]$ und $k = [(k_1, k_2)]$, so erhalten wir wegen Theorem 5.1.8

$$\begin{aligned} m &\le n \\ [(m_1, m_2)] &\le [(n_1, n_2)] \\ m_1 + n_2 &\le m_2 + n_1 \\ m_1 + k_1 + n_2 + k_2 &\le m_2 + k_2 + n_1 + k_1 \\ [(m_1 + k_1, m_2 + k_2)] &\le [(n_1 + k_1, n_2 + k_2)] \\ m + k &\le n + k \end{aligned}$$

(3) Dies folgt aus Theorem 5.1.8.(4) und der Nullteilerfreiheit.
(4) Ist $m \ge 0$, so folgt aus Theorem 5.1.8.(4) sofort $km \ge 0 = k0$. Gilt nun $m \le n$, so folgt aus (2) $0 \le n - m$ und aus dem schon bewiesenen $0 \le k(n - m) = kn - km$ und wir erhalten wieder aus (2) die gesuchte Ungleichung $km \le kn$.
(5) Für $k \le 0$ ist $-k \ge 0$ und alles weitere folgt aus (4).
(6) Gilt $km \le kn$, so erhalten wir aus (2) die Beziehung $0 \le k(n - m)$. Weil $k > 0$ gilt, können wir aus Theorem 5.1.8.(5) $0 \le n - m$ und damit wegen (2) $m \le n$ schließen.

□

Proposition 5.2.4. *Ist $k \ne 0$, so folgt aus $km = kn$ schon $m = n$ für beliebige $m, n \in \mathbb{Z}$.*

Beweis. Es gilt $km = kn \implies 0 = km - kn \implies 0 = k(m - n)$. Weil $k \ne 0$ gilt, muss wegen der Nullteilerfreiheit $m - n = 0$, also $m = n$ gelten. □

5.3. Die rationalen Zahlen $\mathbb{Q}$

Die rationalen Zahlen sind die nächst umfassendere von früher bekannte Zahlenmenge. Ebenso wie man die ganzen Zahlen konstruiert, um die Subtraktion für alle Zahlen durchführen zu können, muss man für die Umkehrung der Multiplikation wieder die Zahlenmenge erweitern.

Man geht von den ganzen Zahlen zu den Bruchzahlen über. Man führt also Ausdrücke der Form

$$q = \frac{m}{n}$$

ein. Hier entdeckt man die ersten beiden Schwierigkeiten, die bei der naiven Einführung der ganzen Zahlen nicht aufgetreten sind. Erstens schafft man es nicht, dem Ausdruck $\frac{m}{0}$ Sinn zu geben, ohne Widersprüche zu verursachen. Zweitens bemerkt man, dass es notwendig ist, Ausdrücke der Form $\frac{m}{n}$ und $\frac{km}{kn}$ für gleich zu erklären ($\frac{1}{2} = \frac{2}{4}$). Mathematisch heißt das, man muss bei der Einführung von $\mathbb{Q}$ *Äquivalenzklassen* bilden und die Null im Nenner verbieten!

Man definiert also $\mathbb{Q}$ als die Äquivalenzklassen von Brüchen der Form $\frac{m}{n}$ ganzer Zahlen mit $n \neq 0$. Man findet, dass es in jeder Äquivalenzklasse einen Bruch gibt, sodass m und n teilerfremd sind und weiters $n > 0$ gilt.

Zusammen mit der Addition $+$ und $\cdot$ bildet $\mathbb{Q}$ einen Körper. Außerdem ist auf $\mathbb{Q}$ eine Ordnungsrelation $\leq$ definiert, für die $\mathbb{Q}$ ein geordneter Körper ist.

Definition 5.3.1. *Ein Körper $(K, +, \cdot)$, der auch eine geordnete Menge $(K, \leq)$ ist, heißt* geordneter Körper*, falls die Eigenschaften*

O1: $\forall q, r, s \in K : (q \leq r \Rightarrow q + s \leq r + s)$,
O2: $\forall q, r \in K : ((q > 0 \wedge r > 0) \Rightarrow qr > 0)$.

erfüllt sind. Wir schreiben dann $(K, +, \cdot, \leq)$.

Die Ordnungsrelation muss also mit den Rechenoperationen **verträglich** sein. Aus den Ordnungsaxiomen können wir auch bereits die bekannten Rechengesetze für Ungleichungen herleiten, wie „das Ungleichheitszeichen dreht sich um, wenn man mit einer negativen Zahl multipliziert“.

Proposition 5.3.2. *In einem geordneten Körper $(K, +, \cdot, \leq)$ gelten folgende Aussagen.*

(1) *Ist $x \leq 0$ dann gilt $-x \geq 0$.*
(2) *Ist $x \geq 0$ und $y \leq z$, dann folgt $xy \leq xz$.*
(3) *Gelten $x < 0$ und $y \leq z$, so ist $xy \geq xz$.*
(4) *Für $x \neq 0$ ist $x^2 > 0$ und daher $1 > 0$.*
(5) *Ist $0 < x < y$, dann folgt $0 < y^{-1} < x^{-1}$.*

Beweis.

(1) Wegen (O1) gilt $x \leq 0 \implies (-x) + x \leq 0 + (-x) \implies 0 \leq -x$.
(2) Für $y = z$ wissen wir $xy = xz$. Ist $y < z$, so ist $0 < z - y$. Für $x = 0$ gilt wieder $0 = xy = xz = 0$. Ist schließlich $x > 0$, dann folgt aus (O2) $0 < x(z - y) = xz - xy$ und somit ist $xy < xz$.
(3) Dies folgt aus (1) und (2).
(4) Ist $x > 0$, so gilt $x^2 = x \cdot x > 0$ wegen (O2). Für $x < 0$ ist $-x > 0$ und $x^2 = (-x)(-x) > 0$. Es ist $1 \neq 0$ und $1^2 = 1$.
(5) Ist $x > 0$, so ist $x^{-1} > 0$. Wäre das nicht so, hätten wir $1 = xx^{-1} < 0$ im Widerspruch zu (4). Gilt $0 < x < y$, so wissen wir $x^{-1}y^{-1} > 0$, und daher folgt

$$\begin{aligned} x &< y \\ x(x^{-1}y^{-1}) &< y(x^{-1}y^{-1}) \\ y^{-1} &< x^{-1}. \end{aligned}$$

□

Proposition 5.3.3. *Die Menge $\mathbb{N}$ ist in $\mathbb{Q}$ nach oben unbeschränkt.*

Beweis. Angenommen, $\mathbb{N}$ sei in $\mathbb{Q}$ beschränkt. Dann existieren positive natürliche Zahlen k und m mit der Eigenschaft, dass $\forall n \in \mathbb{N} : n \leq \frac{m}{k}$. Das ist gleichbedeutend mit der Aussage, dass $\forall n \in \mathbb{N} : nk \leq m$ wegen Proposition 5.3.2.(2). Nachdem k positiv ist, muss $nk \geq n$ sein, weil $k \geq 1$ gilt ($k = k' + 1$, daher $nk = nk' + n$ mit $n \geq 0$ und $k' \geq 0$, also $nk' \geq 0$, was $nk \geq n$ impliziert) und daher existiert eine positive natürliche Zahl m so, dass $\forall n \in \mathbb{N} : n \leq m$. Es ist aber $m + 1 > m$, ein Widerspruch. Daher ist $\mathbb{N}$ in $\mathbb{Q}$ unbeschränkt. □

Die Menge Q ist abzählbar; es gilt also $|\mathbb{Q}| = \aleph_0$ (vgl. Kapitel 3). Außerdem besitzt $\mathbb{Q}$ keinen nicht-trivialen Unterkörper.

5.3.1. Mengentheoretische Konstruktion von $\mathbb{Q}$. Wenn wir die ganzen Zahlen konstruiert haben, steht uns nichts im Wege, dieselbe Konstruktion so ähnlich noch einmal durchzuführen. Im folgenden bezeichne $\mathbb{Z}_+ := \{n \in \mathbb{Z} \mid n > 0\}$ die Menge der positiven Elemente in $\mathbb{Z}$, also der natürlichen Zahlen ungleich 0.

Betrachten wir auf der Menge $\mathbb{Z} \times \mathbb{Z}_+$ die Relation

$$(m_1, m_2) \sim (n_1, n_2) :\iff m_1 n_2 = m_2 n_1.$$

Insbesondere gilt für jede positive natürliche Zahl n die Relation $(m_1, m_2) \sim (nm_1, nm_2)$.

Proposition 5.3.4. *Es gilt wieder $\sim$ ist eine Äquivalenzrelation auf $\mathbb{Z} \times \mathbb{Z}_+$.*

Beweis.

Reflexivität: ist offensichtlich,

Symmetrie: erfüllt, weil Definition symmetrisch ist,

Transitivität: Seien $(m_1, m_2) \sim (n_1, n_2)$ und $(n_1, n_2) = (k_1, k_2)$. Dann sind $m_1 n_2 = m_2 n_1$ und $n_1 k_2 = n_2 k_1$. Multiplizieren wir die erste Gleichung mit k_2, so erhalten wir $m_1 n_2 k_2 = m_2 n_1 k_2$. Jetzt können wir die zweite Gleichung einsetzen und erhalten $m_1 n_2 k_2 = m_2 n_2 k_1$. Nachdem $n_2 \neq 0$ gilt und $\mathbb{Z}$ ein Integritätsbereich ist, folgt $m_1 k_2 = m_2 k_1$, also $(m_1, m_2) \sim (k_1, k_2)$.

□

Die Menge der rationalen Zahlen $\mathbb{Q}$ ist definiert als Faktormenge $\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}_+/_\sim$.

Wenn wir die Operationen

$$[(m_1, m_2)] + [(n_1, n_2)] := [(m_1 n_2 + m_2 n_1, m_2 n_2)]$$
$$[(m_1, m_2)] \cdot [(n_1, n_2)] := [(m_1 n_1, m_2 n_2)]$$

definieren, so sind diese wohldefiniert und es gilt der folgende Satz

Theorem 5.3.5. *Die Menge der rationalen Zahlen $(\mathbb{Q}, +, \cdot)$ ist ein Körper mit Nullelement $[(0, 1)]$ und Einselement $[(1, 1)]$. Die Menge aller Elemente der Form $[(n, 1)]$ für $n \in \mathbb{Z}$ entspricht $\mathbb{Z}$ mit allen seinen Eigenschaften (aka ist **isomorph zu** $\mathbb{Z}$).*

Beweis. Beginnen wir mit der Wohldefiniertheit von $+$. Sei $(m_1', m_2') \in [(m_1, m_2)]$. Dann haben wir $m_1' m_2 = m_1 m_2'$ und

$$\begin{aligned}
[(m_1', m_2')] + [(n_1, n_2)] &= [(m_1' n_2 + m_2' n_1, m_2' n_2)] = [((m_1' n_2 + m_2' n_1) m_2, m_2' n_2 m_2)] = \\
&= [(m_1' n_2 m_2 + m_2' n_1 m_2, m_2' n_2 m_2) = [(m_2' m_1 n_2 + m_2' n_1 m_2, m_2' n_2 m_2)] = \\
&= [(m_2'(m_1 n_2 + n_1 m_2), m_2' n_2 m_2)] = [(m_1 n_2 + n_1 m_2, n_2 m_2)] = \\
&= [(m_1, m_2)] + [(n_1, n_2)].
\end{aligned}$$

Die Wohldefiniertheit im zweiten Term zeigt man analog.

Nun rechnen wir die Gruppenaxiome für $+$ nach

K1: Seien $q = [(q_1, q_2)]$, $[(r_1, r_2)]$ und $[(s_1, s_2)]$. Wir rechnen

$$\begin{aligned}
(q + r) + s &= [(q_1 r_2 + q_2 r_1, q_2 r_2)] + [(s_1, s_2)] = [((q_1 r_2 + q_2 r_1) s_2 + s_1 q_2 r_2, q_2 r_2 s_2)] = \\
&= [(q_1 r_2 s_2 + q_2 r_1 s_2 + s_1 q_2 r_2, q_2 r_2 s_2)] = [(q_1 r_2 s_2 + q_2(r_1 s_2 + r_2 s_1), q_2 r_2 s_2)] = \\
&= [(q_1, q_2)] + [(r_1 s_2 + r_2 s_1, r_2 s_2)] = q + (r + s)
\end{aligned}$$

K2: Die Definition von $q + r$ ist symmetrisch in q und r.

K3: Es gilt $[(q_1, q_2)] + [(0, 1)] = [(1q_1 + 0q_2, 1q_2)] = [(q_1, q_2)]$. Daher ist $0 = [(0, 1)]$ das neutrale Element.

K4: Wir rechnen $[(q_1, q_2)] + [(-q_1, q_2)] = [(q_1 q_2 - q_1 q_2, q_2^2)] = [(0, q_2^2)] = [(0, 1)] = 0$. Das inverse Element von $[(q_1, q_2)]$ ist also $[(-q_1, q_2)]$.

Die Wohldefiniertheit der Multiplikation erkennen wir aus der folgenden Rechnung. Sei $(m'_1, m'_2) \in [(m_1, m_2)]$ und deshalb $m'_1 m_2 = m_1 m'_2$. Dann finden wir

$$[(m'_1, m'_2)][(n_1, n_2)] = [(m'_1 n_1, m'_2 n_2)] = [(m'_1 n_1 m_2, m'_2 n_2 m_2)] = \\ = [(m'_2 m_1 n_1, m'_2 n_2 m_2)] = [(m_1 n_1, n_2 m_2)] = [(m_1, m_2)][(n_1, n_2)].$$

Die Wohldefiniertheit im zweiten Faktor zeigt man analog.

Die Gruppenaxiome für $\cdot$ kommen nun.

K5, K6: Die Multiplikation ist komponentenweise definiert, und die Multiplikation ganzer Zahlen ist kommutativ und assoziativ.

K7: Das Element $1 := [(1, 1)] \neq [(0, 1)]$ ist offensichtlich Einselement.

K8: Ist $q = [(q_1, q_2)] \neq 0$, dann ist $q_1 \neq 0$ und wir finden $q^{-1} = [(q_2, q_1)]$, falls $q_1 > 0$ und $q^{-1} = [(-q_2, -q_1)]$ für $q_1 < 0$. Dass dann q^{-1} das Inverse von q ist, ist einfach einzusehen.

Das Distributivgesetz sieht man so ein.

K9: Für $q = [(q_1, q_2)]$, $r = [(r_1, r_2)]$ und $s = [(s_1, s_2)]$ rechnen wir

$$\begin{aligned} q(r+s) &= [(q_1, q_2)]\big([(r_1, r_2)] + [s_1, s_2]\big) = [(q_1, q_2)][(r_1 s_2 + r_2 s_1, r_2 s_2)] = \\ &= [(q_1(r_1 s_2 + r_2 s_1), q_2 r_2 s_2)] = [(q_1 r_1 s_2 + q_1 r_2 s_1, q_2 r_2 s_2)] = \\ &= [(q_1 r_1 q_2 s_2 + q_2 r_2 q_1 s_1, q_2^2 r_2 s_2)] = [(q_1 r_1, q_2 r_2)] + [(q_1 s_1, q_2 s_2)] = \\ &= [(q_1, q_2)][r_1, r_2] + [(q_1, q_2)][(s_1, s_2)] = qr + qs \end{aligned}$$

Daher ist $\mathbb{Q}$ ein Körper. □

Führen wir darüber hinaus die Relation $\leq$ ein, indem wir fordern

$$[(m_1, m_2)] \leq [(n_1, n_2)] :\Longleftrightarrow\ m_1 n_2 \leq n_1 m_2,$$

so ist dies wohldefiniert. Hätten wir etwa $(m'_1, m'_2) \in [(m_1, m_2)]$ gewählt, so ist $m_1 m'_2 = m'_1 m_2$ und wir haben

$$\begin{aligned} m_1 n_2 &\leq n_1 m_2 \\ m_1 m'_2 n_2 &\leq n_1 m_2 m'_2 \\ m'_1 m_2 n_2 &\leq n_1 m_2 m'_2 \\ m'_1 n_2 &\leq n_1 m'_2 \quad \text{wegen } m_2 > 0 \text{ und Theorem 5.2.3.} \end{aligned}$$

Analog zeigen wir die Wohldefiniertheit auf der rechten Seite.

Theorem 5.3.6. *Die Relation $\leq$ macht $\mathbb{Q}$ zu einem geordneten Körper.*

Beweis. Wir müssen die Bedingungen O1 und O2 nachweisen:

O1: Seien $q = [(q_1, q_2)]$, $r = [(r_1, r_2)]$ und $s = [(s_1, s_2)]$. Dann gilt

$$\begin{aligned} q \leq r \implies &q_1 r_2 \leq q_2 r_1 \implies q_1 s_2 r_2 \leq r_1 s_2 q_2 \implies \\ \implies &(q_1 s_2 + s_1 q_2) r_2 \leq (r_1 s_2 + s_1 r_2) q_2 \implies \\ \implies &(q_1 s_2 + s_1 q_2) r_2 s_2 \leq (r_1 s_2 + s_1 r_2) q_2 s_2 \implies \\ \implies &[(q_1 s_2 + s_1 q_2, q_2 s_2)] \leq [(r_1 s_2 + s_1 r_2, r_2 s_2)] \implies q + s \leq r + s. \end{aligned}$$

O2: Sei $q = [(q_1, q_2)] > 0$, dann folgt $q_1 > 0$. Für $r = [(r_1, r_2)]$ gilt analog $r_1 > 0$. Daher ist $qr = [(q_1 r_1, q_2 r_2)] > 0$, weil $q_1 r_1 > 0$ gilt wegen Theorem 5.2.3.

□

Wenn wir zu guter Letzt die Schreibweise

$$\frac{m}{n} := \begin{cases} [(m,n)] & \text{für } n > 0 \\ [(-m,-n)] & \text{für } n < 0 \end{cases}$$

erklären, dann haben wir die „Bruchzahlen“ wieder eingeführt und die gewohnte Notation von $\mathbb{Q}$ zurückgewonnen.

Auch die ganzen Zahlen $\mathbb{Z}$ können wir in $\mathbb{Q}$ wiederfinden. Wenn wir die Elemente der Form $[(n,1)]$ betrachten, so sehen wir, dass für $m \neq n$ auch $[(m,1)] \neq [(n,1)]$ gilt. Die Rechenoperationen in $\mathbb{Z}$ gelten auch: $[(m,1)] + [(n,1)] = [(m+n,1)]$ und $[(m,1)][(n,1)] = [(mn,1)]$. Die Abbildung $\iota : \mathbb{Z} \to \mathbb{Q}$ mit $\iota : z \mapsto [(z,1)]$ ist ein injektiver Ringhomomorphismus. Wir können also $\mathbb{Z} \cong \iota(\mathbb{Z}) \subseteq \mathbb{Q}$ als Teilring (sogar Teil-Integritätsbereich) sehen. Wir werden Elemente der Form $[(m,1)]$ daher weiterhin mit der ganzen Zahl m identifizieren.

5.4. Die reellen Zahlen $\mathbb{R}$

Die reellen Zahlen sind die vorletzte Zahlenmenge, die wir genauer untersuchen wollen. Weil einige wichtige Beziehungen in $\mathbb{Q}$ nicht berechnet werden können (etwa die Länge der Diagonale des Einheitsquadrates oder die Fläche des Einheitskreises), bleibt uns keine Wahl als die Zahlenmenge ein weiteres Mal zu vergrößern.

Der Körper $\mathbb{Q}$ ist auch „löchrig“ im folgenden Sinn. Betrachten wir die beiden disjunkten Mengen

$$A = \{x \in \mathbb{Q} \mid x > 0 \wedge x^2 < 2\}$$
$$B = \{x \in \mathbb{Q} \mid x > 0 \wedge x^2 > 2\},$$

dann ist deren Vereinigung $A \cup B = \mathbb{Q}_+$. Wir würden aber vom Gefühl erwarten, dass zwischen den beiden Mengen noch eine Zahl sein sollte. Das ist natürlich nicht möglich, da diese Zahl die Gleichung $x^2 = 2$ erfüllen würde, was bekanntermaßen in den rationalen Zahlen nicht möglich ist.

Um die Löcher zu „stopfen“, müssen wir zu $\mathbb{Q}$ irrationale Zahlen hinzufügen und erhalten den geordneten Körper $(\mathbb{R}, +, \cdot, \leq)$, den wir auch als **Zahlengerade** repräsentieren. Die rationalen Zahlen sind ein geordneter Unterkörper von $\mathbb{R}$.

Die reellen Zahlen bilden die Grundlage der Analysis, und daher müssen wir einige wichtige Eigenschaften von $\mathbb{R}$ ableiten.

Definition 5.4.1. *Eine geordnete Menge M ist* ordnungsvollständig *(hat die* Supremums–Eigenschaft*), wenn zu jeder nichtleeren nach oben beschränkten Teilmenge $E \subseteq M$ das Supremum $\sup E \in M$ existiert.*

Um diese Eigenschaft vernünftig anwenden zu können, müssen wir zuerst einige äquivalente Formulierungen beweisen.

Proposition 5.4.2. *Sei M eine geordnete Menge. Dann sind äquivalent:*

(1) *M ist ordnungsvollständig.*
(2) *Jede nach unten beschränkte nichtleere Teilmenge $F \subseteq M$ besitzt ein Infimum $\inf F \in M$.*
(3) *Für je zwei nichtleere Teilmengen E und F von M mit*

$$\forall a \in E : \forall b \in F : a \leq b$$

gibt es ein Element $m \in M$ mit

$$\forall a \in E : \forall b \in F : a \leq m \leq b.$$

Beweis. Wir beginnen mit (1)$\Rightarrow$(2). Sei $F \subseteq M$ und $F \neq \emptyset$. Wir definieren

$$E := \{x \in M \mid \forall f \in F : x \leq f\}.$$

Die Menge E ist nach oben beschränkt, weil jedes Element in F eine obere Schranke für E ist. Außerdem ist E nichtleer, da es eine untere Schranke von F gibt, und E ist die Menge aller unteren Schranken von F. Nach Voraussetzung existiert das Supremum $\alpha = \sup E \in M$. Wir zeigen nun, dass $\alpha = \inf F$ gilt. Nachdem E die Menge aller unteren Schranken von F ist, ist α größer oder gleich allen unteren Schranken von E. Wir müssen also nur zeigen, dass α eine untere Schranke von F ist. Angenommen, das ist nicht der Fall. Dann gäbe es ein $f \in F$ mit $f < \alpha$. Weil E die Menge der unteren Schranken von F ist, gilt $\forall e \in E : e \leq f$. Daher ist f eine obere Schranke von E, ein Widerspruch zur Supremumseigenschaft von α. Daher ist α tatsächlich eine untere Schranke von F, also $\inf F$.
(2)$\Rightarrow$(3): Seien E und F Mengen wie in der Voraussetzung. Wegen (2) existiert $m := \inf F$. Klarerweise ist $m \leq b$ für alle $b \in F$. Es ist außerdem $\forall a \in E : a \leq m$, denn wäre das nicht der Fall, so gäbe es ein $e \in E$ mit $e > m$. Wegen der Eigenschaften von E und F ist aber e eine untere Schranke von F, was der Infimumseigenschaft von m widerspricht. Daher gilt (3).
(3)$\Rightarrow$(1): Sei E eine nach oben beschränkte Menge. Wir definieren die Menge F aller oberen Schranken von E als

$$F := \{x \in M \mid \forall e \in E : e \leq x\} \neq \emptyset.$$

Nach Voraussetzung existiert dann ein $m \in M$ mit $e \leq m \leq f$ für alle $e \in E$ und $f \in F$. Daher ist m eine obere Schranke von E. Sei $\alpha < m$. Dann ist $\alpha \notin F$, also keine obere Schranke. Daher ist m das Supremum von E. □

Beispiel 5.4.3. *Die Menge der rationalen Zahlen ist* nicht *ordnungsvollständig. Betrachten wir nämlich die Teilmengen A und B von $\mathbb{Q}$, die definiert sind durch*

$$A = \{x \in \mathbb{Q} \mid x > 0 \wedge x^2 < 2\},$$
$$B = \{x \in \mathbb{Q} \mid x > 0 \wedge x^2 > 2\}.$$

Es gilt $\forall a \in A : \forall b \in B : a < b$, $1 \in A$ und $2 \in B$. Das folgt aus den Eigenschaften der Ordnungsrelation:

$$b - a = \frac{b^2 - a^2}{b + a} > 0.$$

Wäre $\mathbb{Q}$ ordnungsvollständig, dann gäbe es ein Element $m \in \mathbb{Q}$ mit $a \leq m \leq b$ für alle $a \in A$ und $b \in B$. Definieren wir nun $c := m - \frac{m^2-2}{m+2} = \frac{2m+2}{m+2} > 0$. Damit gilt

$$c^2 - 2 = \frac{2(m^2 - 2)}{(m + 2)^2}.$$

Ist nun $m^2 > 2$, dann folgen $c^2 > 2$ und $c < m$, also ist $c \in B$ mit $c < m$, ein Widerspruch. Andererseits gelten für $m^2 < 2$ sowohl $c^2 < 2$ als auch $c > m$. Das impliziert wegen $c \in A$ und $c > m$ ebenfalls einen Widerspruch. Folglich muss $c^2 = 2$ sein, was aber in $\mathbb{Q}$ unmöglich ist wegen Theorem 3.2.4.

Theorem 5.4.4 (Richard Dedekind). *Es existiert bis auf Isomorphie genau ein ordnungsvollständiger geordneter Körper $\mathbb{R}$, der $\mathbb{Q}$ als geordneten Unterkörper besitzt. Wir nennen $\mathbb{R}$ die Menge der reellen Zahlen und die Elemente der Menge $\mathbb{R} \setminus \mathbb{Q}$ die irrationalen Zahlen.*

Beweis. In Abschnitt 5.4.1. □

Man kann sich auf den Standpunkt von Hilbert stellen, der eine saubere axiomatische Einführung der reellen Zahlen als ordnungsvollständigen geordneten Körper den mengentheoretischen Konstruktionen vorzog, und pragmatisch das Theorem 5.4.4 zur Definition erheben. Was auch immer man tut, die folgenden Ergebnisse folgen nur aus den Eigenschaften und nicht aus der speziellen mengentheoretischen Konstruktion.

Definition 5.4.5. *Für $x \in \mathbb{R}$ definieren wir den* Absolutbetrag *von x durch*

$$|x| = \begin{cases} x & \text{falls } x \geq 0 \\ -x & \text{falls } x < 0. \end{cases}$$

Proposition 5.4.6.

(1) *Zu je zwei reellen Zahlen $x, y \in \mathbb{R}$ mit $x > 0$ existiert eine natürliche Zahl n so, dass*

$$nx > y$$

*gilt. Das heißt, $\mathbb{R}$ besitzt die **archimedische Eigenschaft**.*

(2) *Zwischen je zwei reellen Zahlen $x, y \in \mathbb{R}$ mit $x < y$ gibt es eine rationale Zahl $q \in \mathbb{Q}$ und eine irrationale Zahl $r \in \mathbb{R} \setminus \mathbb{Q}$:*

$$x < q < y \quad \text{und} \quad x < r < y.$$

*Man sagt auch $\mathbb{Q}$ **und** $\mathbb{R} \setminus \mathbb{Q}$ **liegen dicht in** $\mathbb{R}$.*

Beweis. Wir beginnen mit der archimedischen Eigenschaft.
(1) Sei $A := \{nx \mid n \in \mathbb{N}\}$. Wäre die archimedische Eigenschaft nicht erfüllt, dann wäre y eine obere Schranke von A. Damit wäre A nach oben beschränkt und hätte ein Supremum, weil $\mathbb{R}$ die Supremumseigenschaft besitzt. Sei $\alpha = \sup A$. Wegen $x > 0$ ist $\alpha - x < \alpha$, also ist $\alpha - x$ keine obere Schranke von A. Somit existiert eine natürliche Zahl n mit $\alpha - x < nx$. Dann ist aber $\alpha < (n+1)x$, ein Widerspruch dazu, dass α obere Schranke von A ist. Also gilt die archimedische Eigenschaft.

(2) Die Dichtheit von $\mathbb{Q}$ folgt direkt. Sei $x < y$ und damit $y - x > 0$. Wegen der archimedischen Eigenschaft gibt es eine natürliche Zahl n so, dass $n(y-x) > 1$ ist. Wir können auch natürliche Zahlen m_1 und m_2 finden mit $m_1 > nx$ und $m_2 > -nx$. Wir haben jetzt

$$-m_2 < nx < m_1,$$

was die Existenz einer ganzen Zahl m impliziert mit

$$m - 1 \leq nx \leq m \quad \text{und} \quad -m_2 \leq m \leq m_1.$$

Die Kombination aller dieser Ungleichungen liefert

$$nx < m \leq 1 + nx < ny$$
$$x < \tfrac{m}{n} < y,$$

wobei die letzte Ungleichung aus $n > 0$ folgt. Setzen wir $q = \frac{m}{n}$, so haben wir alles bewiesen, was behauptet wurde.

Wenden wir das Argument zweimal an, so können wir rationale Zahlen q_1 und q_2 an mit $x < q_1 < q_2 < y$. Wir definieren

$$r := q_1 + \frac{q_2 - q_1}{2}\sqrt{2} > q_1.$$

Die Zahl r ist irrational, weil $\sqrt{2}$ irrational ist. Außerdem ist

$$q_2 - r = (q_2 - q_1)(1 - \tfrac{1}{\sqrt{2}}) > 0,$$

und deswegen gilt $x < q_1 < r < q_2 < y$. □

Eine weitere Eigenschaft von $\mathbb{R}$ betrifft das Wurzelziehen. Es folgt nämlich aus der Ornungsvollständigkeit.

Proposition 5.4.7. *Für alle $a \in \mathbb{R}$ mit $a > 0$ und alle positiven $n \in \mathbb{N}$ gibt es genau ein $x \in \mathbb{R}$ mit $x > 0$ und $x^n = a$.*

Beweis. Beweisen wir zuerst die Eindeutigkeit: Sind $x \neq y$ zwei Lösungen, so ist o.B.d.A. $x < y$. Mit den Ordnungseigenschaften und vollständiger Induktion folgt dann für jedes $n \in \mathbb{N}$, dass $x^n < y^n$, also $x^n \neq y^n$.

Die Existenzaussagen ist für $n = 1$ oder $a \in \{0, 1\}$ trivial. Seien also zunächst $a > 1$ und $n \geq 2$. Dann definieren wir

$$A := \{x \in \mathbb{R} \mid x > 0 \wedge x^n \leq a\},$$

Weil $1 \in A$ liegt und $\forall x \in A : x < a$ gilt ($x \geq a \Rightarrow x^n \geq a^n > a$), wissen wir, dass $s = \sup A$ existiert.

Wir wollen jetzt beweisen, dass $s^n = a$ gilt.

Fall 1: Ist $s^n < a$, so definieren wir $b := (1 + s)^n - s^n > 0$ und wählen $0 < \varepsilon < \min\{1, \frac{a-s^n}{b}\}$. Dann folgt

$$(s+\varepsilon)^n = \sum_{k=0}^{n-1} \binom{n}{k} s^k \varepsilon^{n-k} + s^n \leq \varepsilon \sum_{k=0}^{n-1} \binom{n}{k} s^k + s^n = \varepsilon b + s^n < a,$$

ein Widerspruch zur Supremumseigenschaft von s.

Fall 2: Ist $s^n > a$, so definieren bzw. wählen wir

$$c := \sum_{\substack{j \\ 0 \leq 2j-1 \leq n}} \binom{n}{2j-1} s^{n-2j+1} > 0, \text{ und } 0 < \varepsilon < \min\{1, \tfrac{s^n-a}{c}\}.$$

Dann rechnen wir nach

$$\begin{aligned}
(s-\varepsilon)^n &= s^n + \sum_{k=0}^{n-1} \binom{n}{k} s^{n-k} (-\varepsilon)^k \\
&\geq s^n + \sum_{k=0,\ k \text{ gerade}}^{n-1} \binom{n}{n-k} (-1)^k \varepsilon^k s^{n-k} \\
&= s^n + \sum_{\substack{j \\ 0 \leq 2j-1 \leq n}} (-1)^{2j-1} \binom{n}{n-(2j-1)} s^{n-2j+1} \varepsilon^{2j-1} \\
&\geq s^n - \varepsilon \sum_{\substack{j \\ 0 \leq 2j-1 \leq n}} \binom{n}{2j-1} s^{n-2j+1} \\
&= s^n - \varepsilon c > a.
\end{aligned}$$

Dies widerspricht ebenfalls der Tatsache, dass $s = \sup A$ gilt.

Deshalb muss $s^n = a$ gelten, was wir zeigen wollten.

Ist schließlich $a < 1$, dann ist $\frac{1}{a} > 1$. Wir können also ein $y \in \mathbb{R}$ finden mit $y^n = \frac{1}{a}$. Dann aber gilt für $x = \frac{1}{y}$, dass $x^n = a$ ist. $\square$

Es gibt auch bei den irrationalen Zahlen noch gewisse Unterschiede. Die Zahl $\sqrt{2}$ tritt als Nullstelle eines Polynoms mit rationalen Koeffizienten auf. Es ist $\sqrt{2}$ nämlich Nullstelle von $x^2 - 2$.

Definition 5.4.8. *Eine reelle Zahl r heißt* algebraisch, *wenn es $n \in \mathbb{N}$ und rationale Zahlen $a_0, \dots, a_n$ gibt mit*

$$\sum_{i=0}^{n} a_i r^i = 0.$$

Eine bis Cantor ungelöste Frage war, ob alle irrationalen Zahlen algebraisch sind. Er hat diese Frage für die damalige Zeit recht überraschend gelöst, denn jedes rationale Polynom n–ten Grades besitzt höchstens n Nullstellen. Ferner gibt es nur abzählbar viele rationale Polynome, die also insgesamt höchstens abzählbar viele Nullstellen besitzen können. Die Mächtigkeit der Menge $\mathbb{R}_a$ der algebraischen Zahlen ist also $\aleph_0$.

Cantor hat aber auch bewiesen, dass $|\mathbb{R}| = c > \aleph_0$ gilt. Aus diesem Grund ist $\mathbb{R}_t := \mathbb{R} \setminus \mathbb{R}_a \neq \emptyset$, ja es gilt sogar $|\mathbb{R}_t| = c$. Die Elemente von $\mathbb{R}_t$ heißen **transzendente Zahlen**. Z.B. sind π und e transzendent. Ersteres hat übrigens Ferdinand Lindemann (1852–1939) im April 1882 bewiesen.

5.4.1. Die mengentheoretische Konstruktion von $\mathbb{R}$. Das einzige, das uns noch fehlt in userer Untersuchung über die reellen Zahlen ist der Beweis von Theorem 5.4.4. Wir werden diesen gesamten Abschnitt dafür opfern und $\mathbb{R}$ aus $\mathbb{Q}$ durch mengentheoretische Mechanismen konstruieren. Zu diesem Zweck werden wir die von Dedekind erfundenen Schnitte verwenden. Es gibt viele äquivalente Verfahren zur Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$. Die Dedekindschen Schnitte sind nicht die einleuchtendste Methode aber jedenfalls diejenige, die nur Mengenoperationen verwendet.

Definition 5.4.9. *Eine nichtleere nach unten beschränkte Teilmenge $S \subseteq \mathbb{Q}$ heißt **Schnitt** (von $\mathbb{Q}$), falls*

$$\textbf{\textit{S1}}: \quad \forall q \in \mathbb{Q} \setminus S : \forall s \in S : s \geq q, \quad \text{und}$$
$$\textbf{\textit{S2}}: \quad \forall s \in S : \exists s' \in S : s > s'.$$

Motivierend kann man erklären, dass ein Schnitt ein halboffenes Intervall $]\,a, +\infty\,[\cap \mathbb{Q}$ mit $a \in \mathbb{R}$ ist. Noch dürfen wir das allerdings nicht sagen.

Proposition 5.4.10.

(1) *Sei S ein Schnitt. Es gilt*
$$\forall S \in s : \forall q \in \mathbb{Q} : (s \leq q \Rightarrow q \in S).$$
Ist also eine rationale Zahl größer als ein Element des Schnittes, dann liegt sie im Schnitt.

(2) *Zu jeder positiven rationalen Zahl ε gibt es $q, r \in \mathbb{Q}$ mit $q \in S$, $r \in \mathbb{Q} \setminus S$ und $q - r \leq \varepsilon$.*

Beweis.

(1) Seien $s \in S$ und $q \in \mathbb{Q}$ mit $s \leq q$. Ist $q \notin S$, dann liegt natürlich $q \in \mathbb{Q} \setminus S$ und daher gilt $\forall s' \in S : s' \geq q$. Daher ist auch $s \geq q$, und weil $\leq$ eine Ordnungsrelation ist, folgt $s = q$. Das ist ein Widerspruch zu $q \notin S$. Daher ist $q \in S$, und wir sind fertig.

(2) Sei $0 < \varepsilon \in \mathbb{Q}$. Weil S ein Schnitt ist, gibt es $q \in S$ und $r \in \mathbb{Q} \setminus S$. Ist $q - r \leq \varepsilon$, dann sind wir fertig. Andernfalls sei $n \in \mathbb{N}$ so groß, dass $n > \frac{q-r}{\varepsilon}$ gilt. Solch ein n existiert wegen Proposition 5.3.3. Wir bilden nun die Menge
$$M := \{r + k\tfrac{q-r}{n} \mid k \in \{0, \dots, n\}\} \subseteq \mathbb{Q}.$$

Für $q \in M \cap S$ und $r \in M \cap (\mathbb{Q} \setminus S)$. Es existiert ein kleinstes Element $q_m \in M \cap S$, weil M endlich ist. Dann ist $r_m := q_m - \frac{q-r}{n} \in M \cap (\mathbb{Q} \setminus S)$, und wir haben zwei rationale Zahlen q_m und r_m wie benötigt gefunden, da $q_m - r_m = \frac{q-r}{n} < \varepsilon$ gilt.

□

Definition 5.4.11. *Sei $R \subseteq \mathbb{P}\mathbb{Q}$ die Menge aller Schnitte von $\mathbb{Q}$. Wir definieren auf R die Relation $\leq$ durch*

$$S \leq T := S \supseteq T. \tag{5.6}$$

Proposition 5.4.12. *Die Relation $\leq$ macht R zu einer totalgeordneten Menge.*

Beweis. Wir müssen die Ordnungseigenschaften überprüfen. Halbordnung ist eigentlich klar, da $\supseteq$ eine Halbordnung auf $\mathbb{P}\mathbb{Q}$ bildet, doch wir schreiben alles noch einmal auf:

Reflexivität: Es für jede Menge $S \supseteq S$.

Symmetrie: Sind $S \supseteq T$ und $T \supseteq S$ erfüllt, so ist $S = T$.

Transitivität: Seien $S \supseteq T$ und $T \supseteq U$. Ist $u \in U$, dann ist $u \in T$, und daher gilt $u \in S$. Das impliziert $S \supseteq U$.

Es bleibt zu zeigen, dass $\leq$ eine Totalordnung ist. Seien S und T zwei Schnitte und $S \neq T$. Ist $S \not\leq T$, dann ist $S \not\supseteq T$, und daher gibt es ein $t \in T$ mit $t \notin S$. In diesem Fall liegt $t \in \mathbb{Q} \setminus S$, also ist für alle $s \in S$ die Ungleichung $s \geq t$ erfüllt. Wegen Proposition 5.4.10.(1) bedeutet das aber $s \in T$, und das impliziert $S \subseteq T$, also $S \geq T$. Damit sind je zwei Schnitte vergleichbar, und $\leq$ ist eine Totalordnung auf R. □

Definition 5.4.13. *Als nächstes führen wir die Abbildung $+ : R \times R \to \mathbb{P}\mathbb{Q}$ durch*

$$S + T := \{s + t \mid s \in S \wedge t \in T\} \quad \text{für } S, T \in R$$

ein.

Proposition 5.4.14. *Diese Abbildung führt sogar wieder nach R. Es ist also $S + T$ wieder ein Schnitt:*

Beweis.

- Sind $s \in S$ und $t \in T$, dann ist $s + t \in S + T$, also ist $S + T \neq \emptyset$.
- Sei σ untere Schranke von S und τ untere Schranke von T. Für beliebiges $x \in S+T$ gibt es $s \in S$ und $t \in T$ mit $x = s + t$. Aus den Eigenschaften von $\leq$ auf $\mathbb{Q}$ folgt ferner $x = s + t \leq \sigma + \tau$. Daher ist $S + T$ nach unten beschränkt.
- Betrachten wir $q \in \mathbb{Q} \setminus (S + T)$. Sei $s \in S$ gegeben, wir wissen $\forall t \in T : s + t \neq q$. Wir formen das um zu $\forall t \in T : t \neq q - s$, und daher ist $q - s \in \mathbb{Q} \setminus T$. Weil T ein Schnitt ist, folgt $\forall t \in T : t \geq q - s$. Bringen wir s zurück auf die linke Seite, ergibt das $\forall t \in T : s+t \geq q$, darum gilt für alle $x \in S+T$, dass $x \geq q$, also ist Eigenschaft S1 erfüllt.
- Sei $x \in S + T$ beliebig. Dann existieren $s \in S$ und $t \in T$ mit $s + t = x$. Weil S und T Schnitte sind, gibt es $s' \in S$ und $t' \in T$ mit $s > s'$ und $t > t'$. Daher ist $x' = s' + t' \in S + T$, und es gilt $x > x'$. Das weist Eigenschaft S2 nach.

□

Das beweist, dass $(R, +)$ ein Gruppoid bildet. Bevor wir die weiteren Eigenschaften nachweisen, betrachten wir noch ein Klasse spezieller Schnitte.

Definition 5.4.15. *Ein Schnitt S heißt **rational**, falls er ein Infimum besitzt.*

Proposition 5.4.16. *Ein Schnitt S ist genau dann rational, wenn es ein $q \in \mathbb{Q}$ gibt mit*

$$S = \mathbb{S}_q := \{q' \in \mathbb{Q} \mid q' > q\}. \tag{5.7}$$

Beweis. Sei S ein Schnitt von der Form (5.7). Nun ist q eine untere Schranke von S, und falls $q' \in \mathbb{Q}$ mit $q' > q$, dann ist q' keine untere Schranke von S. Es ist nämlich $q' > \frac{1}{2}(q' + q) > q$, und daher $\frac{1}{2}(q' + q) \in S$. Daher ist q das Infimum von S und S rational.

Nun sei S ein rationaler Schnitt. Es existiert $q = \inf S$, und wir definieren $\mathbb{S}_q = \{q' \in \mathbb{Q} \mid q' > q\}$. Weil q untere Schranke von S ist, folgt $S \subseteq \mathbb{S}_q$. Sei nun $t \in \mathbb{S}_q$. Falls $t \notin S$ gilt, wissen wir, dass $\forall s \in S : s \geq t$. Daher ist t eine untere Schranke von S mit $t > q$. Das widerspricht der Infimumseigenschaft von q. Daher ist $t \in S$ und $S = \mathbb{S}_q$. □

Auf diese Weise sehen wir, dass für je zwei rationale Zahlen q und r die zugehörigen rationalen Schnitte $\mathbb{S}_q$ und $\mathbb{S}_r$ genau dann gleich sind, wenn $q = r$. Die Abbildung $\iota : \mathbb{Q} \to R$ mit $\iota : q \mapsto \mathbb{S}_q$ ist also injektiv. Auf diese Weise wird $\mathbb{Q}$ in R eingebettet, und wir können in Zukunft die rationale Zahl q mit dem Schnitt $\mathbb{S}_q$ identifizieren.

Proposition 5.4.17. $(G, +)$ *ist eine abelsche Gruppe.*

Beweis. Wir weisen sukzessive alle Eigenschaften nach:

AG: Seien S, T und U Schnitte.

$$\begin{aligned}(S+T)+U &= \{x+u \mid x \in S+T, u \in U\} = \{(s+t)+u \mid s \in S, t \in T, u \in U\} = \\ &= \{s+(t+u) \mid s \in S, t \in T, u \in U\} = \{s+y \mid s \in S, y \in T+U\} = \\ &= S+(T+U).\end{aligned}$$

KG: Für zwei Schnitte S und T sind die Mengen $S + T$ und $T + S$ gleich, weil die Addition in $\mathbb{Q}$ kommutativ ist.

Nullelement: Der rationale Schnitt $0 := \{q \in \mathbb{Q} \mid q > 0\} = \mathbb{S}_0$ ist das Nullelement. Sei nämlich T ein beliebiger Schnitt. Dann erhalten wir

$$0 + T = \{s + t \mid s \in 0, t \in T\}.$$

Wir müssen nachweisen, dass $0 + T = T$ gilt. Sei $x \in 0 + T$, dann gibt es $s \in 0$ und $t \in T$ mit $s + t = x$. Wegen $s > 0$ ist $x > t$ und damit gilt $x \in T$, also $0 + T \subseteq T$. Umgekehrt sei $t \in T$. Weil T ein Schnitt ist, gibt es ein $t' \in T$ mit $t' < t$. Setzen wir nun $s = t - t'$, dann ist $s \in 0$ und $t = s + t' \in S + T$, was wiederum $T \subseteq 0 + T$ beweist.

Inverse: Betrachten wir wieder einen Schnitt S. Wir definieren

$$-S := \{q \in \mathbb{Q} \mid \forall s \in S : q > -s \wedge \forall t \in \mathbb{Q} : (t = \inf S \Rightarrow q \neq -t)\}$$

den zu S negativen Schnitt. Wir behaupten $S + (-S) = 0$. Zuerst müssen wir aber zeigen, dass $-S$ tatsächlich ein Schnitt ist.

Sei q' eine untere Schranke von S. Dann gilt $\forall s \in S : q = q' - 1 < s$ und deshalb $\forall s \in S : -q > -s$, also ist $-S$ nichtleer. Für ein beliebiges Element $s \in S$ folgt, dass jedes Element $s' \in -S$ die Ungleichung $s' \geq -s$ erfüllem muss, also is $-s$ eine untere Schranke von $-S$.

Sei nun $q \in \mathbb{Q} \setminus (-S)$. Dann gibt es $s \in S$ mit $q \leq -s$, also $-q \geq s$. Weil S ein Schnitt ist, folgt $-q \in S$. Darum gilt aber $\forall t \in (-S) : t > q$. Das beweist S1.

S2 beweisen wir indirekt. Sei $q \in (-S)$ gegeben mit $\forall t \in (-S) : q \leq t$. Dann ist q eine untere Schranke von $-S$, also ein Minimum und erst recht ein Infimum von $-S$. Das ist aber unmöglich wegen der Definition von $-S$. Falls $\tilde{s} := \inf S$ existiert, dann ist $-\tilde{s}$ das Supremum der Menge $\tilde{S} := \{-s \mid s \in S\}$, des Komplements von $-S$, und damit das Infimum von $-S$. Nach Definition ist $-\tilde{s} \notin (-S)$.

Sei $x \in S + (-S)$, dann existieren $s \in S$ und $t \in -S$ mit $s + t = x$. Dass $t \in -S$ liegt, impliziert $t > -s$ und damit auch $x = s + t > 0$. Daher ist $S + (-S) \subseteq 0$. Nun sei $y > 0$. Wir suchen gemäß Proposition 5.4.10.(2) zwei rationale Zahlen q und r

mit $q \in S$, $r \in Q \setminus S$ und $q - r < y$. Es gilt $\forall s \in S : s > r$, und daher ist $-r \in -S$. Wir definieren $r' := q - r$ und wissen $r' < y$, also $y - r' > 0$. Weil S ein Schnitt ist, bedeutet das $s := y - r' + q \in S$. Setzen wir nun zusammen, so haben wir $-r \in -S$ und $s \in S$ mit

$$-r + s = -r + y - r' + q = -r + y - q + r + q = y.$$

Das impliziert $y \in S + (-S)$ und daher ist $0 = S + (-S)$.

□

Die Verträglichkeit von $+$ und $\leq$, also O1 beweisen wir als nächstes (siehe Definition 5.3.1).

Proposition 5.4.18. *Für je drei Elemente S, T und U von R gilt*

$$S \leq T \implies S + U \leq T + U.$$

Beweis. Seien drei Schnitte S, T und U gegeben mit $S \leq T$. Sei $y \in T + U$. Dann existieren $t \in T$ und $u \in U$ mit $y = t + u$. Weil $s \leq T$ gilt, wissen wir $S \supseteq T$ und damit $t \in S$. Daher ist $t + u = y$ auch in $S + U$, was wiederum $S + U \leq T + U$ bestätigt. □

Ein Schnitt S heißt positiv, falls $S > 0$ gilt. Er heißt nichtnegativ, falls $S \geq 0$ erfüllt ist. Analog führen wir die Bezeichnungen negativ und nichtpositiv ein. Für einen negativen Schnitt S ist $-S$ positiv. Das folgt aus der Verträglichkeit von $+$ und $\leq$ in Proposition 5.4.18.

Es fehlt zum Körper die zweite Operation.

Definition 5.4.19. *Wir definieren die Abbildung $\cdot : R \times R \to \mathbb{P}\mathbb{Q}$ wie folgt: Für zwei nichtnegative Schnitte S und T sei*

$$S \cdot T := \{st \mid s \in S \wedge t \in T\}.$$

Darüber hinaus erklären wir

$$S \cdot T := \begin{cases} -((-S) \cdot T) & \text{falls } S < 0 \text{ und } T \geq 0 \\ -(S \cdot (-T)) & \text{falls } S \geq 0 \text{ und } T < 0 \\ (-S) \cdot (-T) & \text{falls } S < 0 \text{ und } T < 0. \end{cases}$$

Wegen der Bemerkungen vor der Definition ist die Abbildung $\cdot$ wohldefiniert.

Proposition 5.4.20. *Die Abbildung $\cdot$ ist eine Verknüpfung auf R. Es gilt $(R, +, \cdot)$ ist ein Körper.*

Beweis. Zuerst müssen wir beweisen, dass für nichtnegative Schnitte S und T die Menge $S \cdot T$ wieder ein Schnitt ist. Es existiert $s \in S$ und $t \in T$, daher ist $st \in S \cdot T$, welches somit nichtleer ist.

Weil S und T nichtnegativ sind, folgt $0 \supseteq S$ und $0 \supseteq T$, und daher ist $0 \in \mathbb{Q}$ untere Schranke von S und T. Wir erhalten $\forall s \in S : 0 \leq s$ und $\forall t \in T : 0 \leq t$. Wegen Proposition 5.3.2.(2) gilt $\forall s \in S : \forall t \in T : 0 \leq st$, und daher ist $S \cdot T$ nach unten beschränkt.

Sei $q \in \mathbb{Q} \setminus (S \cdot T)$. Ist $s \in S$ beliebig, dann gilt $\forall t \in T : st \neq q$, und daher haben wir wegen $s > 0$ auch $\forall t \in T : t \neq q/s$. Das wiederum bedingt, dass $q/s \in \mathbb{Q} \setminus T$ liegt, weshalb $\forall t \in T : t \geq q/s$. Umgeformt bedeutet das $\forall t \in T : ts \geq q$, was S1 impliziert.

Für $y \in S \cdot T$ existieren $s \in S$ und $t \in T$ mit $y = st$. Ferner gibt es $s' \in S$ mit $s' < s$ und $t' \in T$ mit $t' < t$. Weil alle Zahlen s, s', t, t' größer Null sind, folgt aus Proposition 5.3.2 $s't' < st$, woraus S2 folgt.

Für nichtnegative Schnitte ist das Produkt also wieder ein Schnitt. In den anderen Fällen wird die Definition auf ein Produkt nichtnegativer Schnitte zurückgeführt, und daher ist $\cdot$ tatsächlich eine Verknüpfung auf R.

Wir wissen bereits, dass $(R, +)$ eine abelsche Gruppe ist. Der Rest der Körperaxiome muss noch nachgewiesen werden. Beginnen wir mit den Aussagen über die Multiplikation, doch zuvor wollen wir noch ein Hilfsresultat über positive Schnitte beweisen.

Lemma: Sei S ein positiver Schnitt. Es gibt ein $q > 0$ in $\mathbb{Q}$, das untere Schranke von S ist.

Beweis: Wegen $S > 0$ folgt, dass $0 \supsetneq S$ gilt, und daher existiert ein $q \in 0$ mit $q \notin S$, also $q \in \mathbb{Q} \setminus S$. Es gilt $0 < q$, weil $q \in 0$ und $\forall s \in S : q \leq S$, wegen S1. □

AG: Das Assoziativgesetz für positive Schnitte folgt direkt aus dem Assoziativgesetz für die Multiplikation rationaler Zahlen. Seien S, T und U nichtnegative Schnitte.

$$\begin{aligned}(S \cdot T) \cdot U &= \{xu \mid x \in S \cdot T, u \in U\} = \{(st)u \mid s \in S, t \in T, u \in U\} = \\ &= \{s(tu) \mid s \in S, t \in T, u \in U\} = \{sy \mid s \in S, y \in T \cdot U\} = \\ &= S \cdot (T \cdot U).\end{aligned}$$

Seien nun S, T und U beliebig. Mit einer Anzahl einfacher Fallunterscheidungen kann man das Assoziativgesetz auf den positiven Fall zurückführen. Sei etwa $S < 0$, $T \geq 0$ und $U \geq 0$. Dann folgt

$$\begin{aligned}(S \cdot T) \cdot U &= -((-S) \cdot T) \cdot U = -(((-S) \cdot T) \cdot U) = -((-S) \cdot (T \cdot U)) = \\ &= -(-S) \cdot (T \cdot U) = S \cdot (T \cdot U).\end{aligned}$$

All die anderen sechs Fälle beweist man analog.

KG: Auch die Kommutativität für nichtnegative Schnitte folgt aus der Kommutativität der Multiplikation in $\mathbb{Q}$. Für beliebige Schnitte folgt sie aus der Symmetrie von Definition 5.4.19.

Einselement: Wir definieren $1 := \mathbb{S}_1 = \{x \in \mathbb{Q} \mid x > 1\}$ und behaupten, dass 1 das Einselement bezüglich der Multiplikation ist. Es gilt $1 \neq 0$, und wir betrachten einen nichtnegativen Schnitt S. Für $s \in 1 \cdot S$ gibt es $t \in 1$ und $s' \in S$ mit $s = ts'$. Weil $t > 1$ ist, folgt aus Proposition 5.3.2, dass $s > s'$ und damit auch $s \in S$ gilt. Daher ist $1 \cdot S \subseteq S$.

Sei nun umgekehrt $s \in S$ gegeben. Wir können $s' \in S$ finden mit $0 < s' < s$, weil S ein nichtnegativer Schnitt ist. Aus Proposition 5.3.2 folgt, dass $t = \frac{s}{s'} > 1$ ist, also $t \in 1$, und außerdem wissen wir $ts' = s$. Daher ist auch $S \subseteq 1 \cdot S$.

Für negatives S gilt $1 \cdot S = -(1 \cdot (-S)) = -(-S) = S$.

Inverse: Sei S ein positiver Schnitt. Wir definieren

$$S^{-1} := \{q \in \mathbb{Q} \mid \forall s \in S : q > \tfrac{1}{s} \wedge \forall t \in \mathbb{Q} : (t = \inf S \Rightarrow q \neq \tfrac{1}{t})\}$$

und behaupten das multiplikative Inverse zu S gefunden zu haben.

Zuerst müssen wir beweisen, dass S^{-1} ein Schnitt ist. Wegen des Lemmas existiert eine positiver rationale Zahl q', die untere Schranke von S ist. Die Zahl $q = \frac{q'}{2}$ erfüllt dann für alle $s \in S$, dass $s > q$ und daher $\frac{1}{s} < \frac{1}{q}$, also ist $\frac{1}{q} \in S^{-1}$.

Sei $q \in \mathbb{Q} \setminus S^{-1}$. O.b.d.A. gilt $q > 0$, denn alle Elemente von S^{-1} sind positiv. Es folgt, dass es ein $s \in S$ gibt, für das $q \leq \frac{1}{s}$ erfüllt ist. Aus den Eigenschaften der Ordnungsrelationen folgt aber dann $\frac{1}{q} \geq s$, und daher ist $\frac{1}{q} \in S$. Daher gilt $\forall t \in S^{-1} : t > q$. Das zeigt S1.

S2 folgt wieder aus der Definition von S^{-1}. Ist $q \in S^{-1}$ gegeben mit $\forall s \in S^{-1} : q \leq s$, dann ist q Minimum also Infimum von S^{-1}. Aus der Definition von S^{-1} kann man aber ablesen, dass S^{-1} sein (eventuell existierendes) Infimum nicht enthalten darf.

Nachdem wir jetzt gezeigt haben, dass S^{-1} tatsächlich ein Schnitt ist, müssen wir beweisen, dass S^{-1} das Inverse von S ist. Sei also $q \in S \cdot S^{-1}$. Dann existieren

$s \in S$ und $t \in S^{-1}$ mit $st = q$. Weil $t \in S^{-1}$ folgt, dass $t > \frac{1}{s}$, und daher ist $st > 1$, woraus $S \cdot S^{-1} \subseteq 1$ folgt.

Sei umgekehrt $y \in 1$ gegeben. Wir definieren $\varepsilon = y - 1 > 0$ und wählen uns gemäß dem Lemma eine positive untere Schranke r' von S. Außerdem können wir wegen Proposition 5.4.10.(1) zwei rationale Zahlen $\tilde{r}$ und s mit $r \in \mathbb{Q} \setminus S$ und $s \in S$ und $s - \tilde{r} < r'\varepsilon$ finden. Sei $r = \max\{\tilde{r}, r'\}$. Dann ist immer noch $r \in \mathbb{Q} \setminus S$ und $s - r < r'\varepsilon$. Für r und s gilt darüber hinaus noch

$$\tfrac{s}{r} - 1 < \tfrac{r'\varepsilon}{r} < \varepsilon \quad \text{also} \quad \tfrac{s}{r} < 1 + \varepsilon = y.$$

Wir definieren $t := \frac{yr}{s} > 1$. Dann sind $s < st =: s' \in S$ und $\frac{1}{r} \in S^{-1}$ und weiters

$$s'\tfrac{1}{r} = \tfrac{st}{r} = \tfrac{yrs}{rs} = y,$$

also ist $y \in S \cdot S^{-1}$, und das impliziert $S \cdot S^{-1} = 1$.

Ist S negativ, dann definieren wir $S^{-1} := -((-S)^{-1})$, und wir haben

$$S \cdot S^{-1} = (-S) \cdot (-S^{-1}) = (-S) \cdot (-S)^{-1} = 1.$$

Zu guter letzt fehlt noch das **Distributivgesetz**. Wir beginnen wieder mit nichtnegativen Schnitten S, T und U. Wegen der Distributivität in $\mathbb{Q}$ gilt

$$\begin{aligned}(S+T) \cdot U &= \{xu \mid x \in S+T, u \in U\} = \{(s+t)u \mid s \in S, t \in T, u \in U\} = \\ &= \{su + tu \mid s \in S, t \in T, u \in U\} = \{y + z \mid y \in S \cdot U, z \in T \cdot U\} = \\ &= S \cdot U + T \cdot U.\end{aligned}$$

Für die sieben übrigen Fälle sei als Beispiel einer bewiesen: Mit $U < 0$ und $S \geq 0$ und $T \geq 0$ gilt

$$\begin{aligned}(S+T) \cdot U &= -((S+T) \cdot (-U)) = -(S \cdot (-U) + T \cdot (-U)) = \\ &= -(S \cdot (-U)) + (-(T \cdot (-U))) = S \cdot U + T \cdot U.\end{aligned}$$

Das beweist, dass $(R, +, \cdot)$ ein Körper ist. □

Proposition 5.4.21. *Der Körper $(R, +, \cdot)$ ist geordnet bezüglich $\leq$.*

Beweis. Es genügt O2 zu beweisen, denn O1 haben wir in Proposition 5.4.18 bereits nachgewiesen. Seien also $S > 0$ und $T > 0$. Dann gibt es positive untere Schranken $\underline{s}$ von S und $\underline{t}$ von T, und daher ist $\underline{st} > 0$ eine untere Schranke von $S \cdot T$. Das impliziert $S \cdot T > 0$. □

Nachdem wir nachgewiesen haben, dass die Menge aller Schnitte R einen geordneten Körper bildet, bleibt noch die letzte Eigenschaft nachzuweisen.

Proposition 5.4.22. *Der geordnete Körper $(R, +, \cdot, \leq)$ ist ordnungsvollständig.*

Beweis. Sei E eine nach unten beschränkte Teilmenge von R. Sei $Q \in R$ eine untere Schranke von E, und sei $\alpha \in \mathbb{Q}$ untere Schranke von Q.

Wir betrachten die Menge

$$S := \bigcup_{T \in E} T,$$

die Vereinigung aller Elemente von E.

Wir zeigen zuerst, dass S ein Schnitt ist. Es ist klar, dass S nichtleer ist, denn jedes $T \in E$ ist nichtleer. Außerdem ist α untere Schranke von jedem $T \in E$ (weil $T \subseteq Q$), und daher auch untere Schranke der Vereinigung.

Nun wählen wir ein $q \in \mathbb{Q} \setminus S$. Für dieses Element gilt, dass $\forall T \in E : q \notin T$, also $\forall T \in E : q \in \mathbb{Q} \setminus T$. Für ein beliebiges $s \in S$ gilt nun, dass $\exists T \in E : s \in T$, und daher muss $q \leq s$ sein, was S1 beweist.

Schließlich gilt S2, weil für beliebiges $s \in S$ wieder ein $T \in E$ existiert mit $s \in T$. Da T ein Schnitt ist, gibt es ein $s' \in T$, sodass $s' < s$ gilt. Nun ist aber s' in der Vereinigung aller T, also $s' \in S$.

Wir beschließen den Beweis mit der Behauptung, dass $S = \inf E$ gilt. Offensichtlich ist S untere Schranke von E, da $S \supseteq T$ für alle $T \in E$ erfüllt ist. Sei nun $U \in R$ ein Schnitt mit $U > S$. Dann ist $S \supsetneq U$, und daher existiert ein $s \in S$ mit $s \notin U$. Nun muss es aber ein $T \in E$ geben mit $s \in T$, woraus folgt, dass $U \not\supseteq T$ gilt, also ist U keine untere Schranke von E. Daher stimmt tatsächlich $S = \inf E$ und R ist ordnungsvollständig. □

Lemma 5.4.23. *Sei $(S, +, \cdot, \leq)$ ein ordnungsvollständiger geordneter Körper mit geordnetem Unterkörper $\mathbb{Q}$. Dann ist jedes Element $b \in S$ das Infimum der Menge*

$$\mathbb{T}_b := \{s \in \mathbb{Q} : b < s\}.$$

Beweis. Die Menge $\mathbb{T}_b$ ist durch b nach unten beschränkt, und daher existiert das Infimum $\inf \mathbb{T}_b =: b' \in S$. Angenommen, es gilt $b' > b$. Aus Proposition 5.4.6, für deren Beweis wir nur die Eigenschaften geordneter Körper und Ordnungsvollständigkeit verwendet haben, folgt, dass es ein $q \in \mathbb{Q}$ gibt mit $b < q < b'$. Dann ist aber $q \in \mathbb{T}_b$, und daher ist b' keine untere Schranke von $\mathbb{T}_b$. Das ist ein Widerspruch, also ist $b' = b$. □

Proposition 5.4.24. *Sei $(S, +, \cdot, \leq)$ ein weiterer ordnungsvollständiger geordneter Körper, der $\mathbb{Q}$ als geordneten Unterkörper enthält, dann sind S und R isomorph.*

Beweis. Die Abbildung $f : S \to R$ gegeben durch $f : s \mapsto \mathbb{T}_s$ ist ein monotoner Körperisomorphismus.

Zunächst ist f wohldefiniert, denn jedes $\mathbb{T}_s$ ist ein Schnitt von $\mathbb{Q}$: Dass $\mathbb{T}_s$ nichtleer ist, folgt aus der Unbeschränktheit von $\mathbb{Q}$ in S. Weil s eine untere Schranke von $\mathbb{T}_s$ ist, existiert auch eine rationale Zahl $\tilde{s} < s$, die untere Schranke von $\mathbb{T}_s$ ist. Gilt $q \in \mathbb{Q} \setminus \mathbb{T}_s$, dann muss $q \leq s$ sein wegen der Definition von $\mathbb{T}_s$. Daher ist q ebenfalls untere Schranke von $\mathbb{T}_s$, was S1 beweist. Ist schließlich $r \in \mathbb{T}_s$ eine rationale Zahl, dann können wir wieder Proposition 5.4.6 verwenden, um eine rationale Zahl r' zu erhalten, mit $s < r' < r$, also $r' \in \mathbb{T}_s$, gleichbedeutend mit der Gültigkeit von S2.

Zuerst zeigen wir die Injektivität von f. Seien $s \neq s'$ zwei Elemente von S. O.B.d.A. ist $s > s'$. Dann gilt $\mathbb{T}_s \subsetneq \mathbb{T}_{s'}$, weil es eine rationale Zahl zwischen s und s' gibt (wieder Proposition 5.4.6). Daher ist $f(s) \neq f(s')$.

Die Abbildung f ist surjektiv. Ist T ein beliebiger Schnitt von $\mathbb{Q}$, dann ist $T \subseteq S$ nichtleer und nach unten beschränkt, besitzt also ein Infimum $s \in S$. Sei $t \in T$, dann gilt $t > s$, weil wegen der Schnitteigenschaft S2 die Menge T ihr Infimum nicht enthält. Daher ist $t \in \mathbb{T}_s$. Sei umgekehrt $t \in \mathbb{T}_s$ und damit $t > s$. Ist $t \notin T$, dann folgt aus der Schnitteigenschaft S1, dass $\forall t' \in T : t \leq t'$, also ist t eine untere Schranke von T mit $t > s$, was der Infimumseigenschaft von s widerspricht. Darum gilt $T = \mathbb{T}_s = f(s)$.

Es bleibt zu zeigen, dass f ein Körperhomomorphismus ist.

- Seien $s, t \in S$. Dann ist $f(s) + f(t) = \mathbb{T}_s + \mathbb{T}_t$. Es gilt

$$\begin{aligned}\mathbb{T}_s + \mathbb{T}_t &= \{s' + t' \mid s' \in \mathbb{T}_s, t' \in \mathbb{T}_t\} = \{s' + t' \mid s' > s \wedge t' > t\} = \\ &= \{s' + t' \mid s' + t' > s + t\} = \mathbb{T}_{s+t} = f(s + t).\end{aligned}$$

- Für $s \in S$ folgt

$$\begin{aligned}-f(s) = -\mathbb{T}_s &= \{s' \in \mathbb{Q} \mid \forall t \in \mathbb{T}_s : s' > -t \ \wedge \ \forall t' \in \mathbb{Q} : (t' = \inf \mathbb{T}_s \Rightarrow s' \neq -t')\} = \\ &= \{s' \in \mathbb{Q} \mid s' > -s\} = \mathbb{T}_{-s} = f(-s).\end{aligned}$$

- Sind wieder $s, t \in S$. Dann folgt für $s \geq 0$ und $t \geq 0$, dass
$$\mathbb{T}_s \cdot \mathbb{T}_t = \{s't' \mid s' \in \mathbb{T}_s, t' \in \mathbb{T}_t\} = \{s't' \mid s' > s \wedge t' > t\} =$$
$$= \{s't' \mid s't' > st\} = \mathbb{T}_{st} = f(st).$$
Falls $s < 0$ ist und $t \geq 0$ gilt, ist $st = -((-s)t)$ und aus dem bereits Bewiesenen folgt
$$f(st) = f(-((-s)t)) = -f((-s)t) = -(f(-s)f(t)) = -(-(f(s))f(t)) = f(s)f(t).$$
Der letzte Fall $s < 0$, $t < 0$ ist einfacher:
$$f(st) = f((-s)(-t)) = f(-s)f(-t) = (-f(s))(-f(t)) = f(s)f(t).$$
- Zuletzt sei wieder $s \in S$ mit $s > 0$.
$$f(s)^{-1} = \mathbb{T}_s^{-1} = \{s' \in \mathbb{Q} \mid \forall t \in \mathbb{T}_s : s' > \tfrac{1}{t} \wedge \forall t' \in \mathbb{Q} : (t' = \inf \mathbb{T}_s \Rightarrow s' \neq \tfrac{1}{t'})\} =$$
$$= \{s' \in \mathbb{Q} \mid s' > \tfrac{1}{s}\} = \mathbb{T}_{s^{-1}} = f(s^{-1}).$$
Ist hingegen $s < 0$, dann erhalten wir
$$f(s^{-1}) = f(-((-s)^{-1})) = -f((-s)^{-1}) = -(f(-s)^{-1}) = (-f(-s))^{-1} = f(s)^{-1}.$$

Daher ist f ein Körperisomorphismus, und tatsächlich sind S und R isomorph. □

Ab nun bezeichnen wir den bis auf Isomorphie eindeutig bestimmten ordnungsvollständigen geordneten Körper R mit $\mathbb{R}$ und nennen ihn die **Menge der reellen Zahlen**.

5.5. Die komplexen Zahlen $\mathbb{C}$

Kommen wir nun zu einer Zahlenmenge, die in der Schule oft vernachlässigt wird, und die darüber hinaus einige philosophische Fragen aufzuwerfen scheint.

Wir erinnern uns, dass die Geschichte der Algebra mit Büchern begonnen hat, in denen unter anderem die Lösung linearer und quadratischer Gleichungen beschrieben wurde. Begonnen hat das in einer Zeit als nur die positiven rationalen Zahlen bekannt waren. Bereits die Lösung der quadratischen Gleichung
$$x^2 = 0 \tag{5.8}$$
bereitet da Schwierigkeiten. Gegen Ende 14. Jahrhunderts setzte sich in Europa die 0 als eigenständige Zahl durch, doch die alte Welt musste ein weiteres Jahrhundert warten bis auch die negativen Zahlen akzeptiert waren. Von diesem Zeitpunkt an war Gleichung (5.8) lösbar, ebenso wie etwa
$$x^2 + 3x + 2 = 0. \tag{5.9}$$
Die Tatsache, dass die rationalen Zahlen nicht genügen, ist seit Hippasos von Metapont (5. Jahrhundert v.Chr.) bekannt, der die Irrationalität von $\sqrt{2}$ als Diagonallänge des Einheitsquadrates erkannte. (Dafür wurde er übrigens, sagt die Geschichte, von einer Gruppe Pythagoreer im Meer ertränkt). Die Polynomgleichung
$$x^2 = 2, \tag{5.10}$$
die aus dem Satz von Pythagoras folgt, ist also in den rationalen Zahlen nicht lösbar.

Daher wurde in der Mathematik schon früh auf die reellen Zahlen zurückgegriffen, allerdings ohne eine wirkliche Definition als Zahlenmenge anzugeben. Das haben erst Cantor und Dedekind im Jahre 1871 auf äquivalente aber unterschiedliche Weise getan.

Ist nun aber jede quadratische Gleichung lösbar? Die Antwort ist, wie wir alle wissen, nein. Die Gleichung
$$x^2 + 1 = 0 \tag{5.11}$$
hat keine reelle Lösung.

Die komplexen Zahlen wurden in der Mathematik schon einige Zeit verwendet, allerdings ohne richtige Definition. So ist bekannt, dass Girolamo Cardano (1501–1576) während er die Formeln für die Nullstellen von Polynomen dritten und vierten Grades erarbeitete, die komplexen Zahlen vor Augen hatte. Er verwarf sie allerdings wieder als „zu subtil und daher nutzlos“.

Auch Leonhard Euler (1707–1783) kannte bereits die komplexen Zahlen. Er führte 1748 auch die „Zahl“ i als Bezeichnung ein in seiner berühmten Arbeit „Introductio in analysin infinitorum“, wo auch die Formel

$$e^{ix} = \cos x + i \sin x$$

das erste Mal auftaucht.

Der erste jedoch, der eine mathematische Arbeit über die komplexen Zahlen verfasst hat, in der eine Definition derselben (die reellen Zahlen vorausgesetzt) vorkommt, war Caspar Wessel (1745–1818). Er hat 1799 in der Königlich Dänischen Akademie seine Arbeit veröffentlicht (übrigens als erstes Nichtmitglied, und es war seine einzige(!) mathematische Arbeit), in der er die geometrische Interpretation der komplexen Zahlen vorstellte. Er entwickelte diese Zahlen übrigens während er Oldenburg trigonometrisch vermaß (triangulierte), und es ist sicher, dass er bereits 1787 die komplexen Zahlen entwickelt hatte (unwissend, dass solche Zahlen bereits in Verwendung waren). Mit Hilfe dieser brillianten mathematischen Idee gelang es ihm als erstem, eine genaue Landkarte Dänemarks herzustellen.

Leider wurde seine Arbeit in Mathematikerkreisen nicht gelesen, und so wurde im Jahr 1806 die geometrische Interpretation von dem Schweizer Jean Robert Argand (1768–1822) wiederentdeckt und erneut neuentwickelt von Johann Carl Friedrich Gauss (1777–1855) im Jahre 1831, der übrigens interessanterweise eine weitere Arbeit von Wessel, nämlich die Triangulierung von Oldenburg im Jahr 1824 wiederholte.

Was sind also diese „mystischen“ komplexen Zahlen, die die Mathematiker so lange in Atem gehalten haben? Als moderne Mathematiker mit geschultem algebraischem Blick können wir den Zahlen den Mythos nehmen.

Wir beginnen mit der Menge $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ und definieren auf ihr zwei Verknüpfungen

$$\begin{aligned}(a_0, a_1) + (b_0, b_1) &:= (a_0 + b_0, a_1 + b_1)\\ (a_0, a_1) \cdot (b_0, b_1) &:= (a_0 b_0 - a_1 b_1, a_0 b_1 + a_1 b_0).\end{aligned}$$

Zuerst untersuchen wir die algebraischen Eigenschaften von $(\mathbb{C}, +, \cdot)$:

Theorem 5.5.1. *$(\mathbb{C}, +, \cdot)$ ist ein Körper.*

Beweis. Um dieses Theorem zu beweisen, müssen wir die Körperaxiome nachrechnen.

AG(+): Das folgt aus der komponentenweisen Definition von $+$ und der Tatsache, dass $(\mathbb{R}, +)$ eine abelsche Gruppe ist.

KG(+): Hier trifft dasselbe Argument zu wie für das Assoziativgesetz.

Nullelement: Es gilt, dass $(0, 0)$ das neutrale Element bezüglich $+$ ist. $(a_0, a_1) + (0, 0) = (a_0 + 0, a_1 + 0) = (a_0, a_1)$.

Inverse(+): Das Inverse zu (a_0, a_1) ist $(-a_0, -a_1)$, wie man sehr leicht nachrechnet.

AG(·): Seien (a_0, a_1), (b_0, b_1) und (c_0, c_1) gegeben. Dann gilt

$$\begin{aligned}&(a_0, a_1)\big((b_0, b_1)(c_0, c_1)\big) =\\ &\quad = (a_0, a_1)(b_0 c_0 - b_1 c_1, b_0 c_1 + b_1 c_0)\\ &\quad = (a_0 b_0 c_0 - a_0 b_1 c_1 - a_1 b_0 c_1 - a_1 b_1 c_0, a_0 b_0 c_1 + a_0 b_1 c_0 + a_1 b_0 c_0 - a_1 b_1 c_1)\\ &\quad = (a_0 b_0 - a_1 b_1, a_0 b_1 + a_1 b_0)(c_0, c_1)\\ &\quad = \big((a_0, a_1)(b_0, b_1)\big)(c_0, c_1).\end{aligned}$$

KG(·): Dieses Gesetz folgt aus der Symmetrie der Definition von · und dem Kommutativgesetz in $(\mathbb{R}, \cdot)$.

Einselement: Das Einselement ist $(1, 0)$, eine sehr einfache Rechnung.

Inverse(·): Ist $(a_0, a_1) \neq (0, 0)$, dann ist das Element

$$(\tfrac{a_0}{a_0^2+a_1^2}, \tfrac{-a_1}{a_0^2+a_1^2})$$

das Inverse zu (a_0, a_1). Beachte, dass für reelle Zahlen a_0 und a_1 der Nenner $a_0^2 + a_1^2$ nur dann verschwinden kann, wenn beide Zahlen gleich 0 sind. Das haben wir aber ausgeschlossen. Es gilt

$$(a_0, a_1)\left(\frac{a_0}{a_0^2 + a_1^2}, \frac{-a_1}{a_0^2 + a_1^2}\right) = \left(\frac{a_0^2 + a_1^2}{a_0^2 + a_1^2}, \frac{-a_0a_1 + a_1a_0}{a_0^2 + a_1^2}\right) = (1, 0).$$

□

Die reellen Zahlen sind ein Unterkörper von $\mathbb{C}$, wie man leicht sieht, indem man die Abbildung $\iota : \mathbb{R} \to \mathbb{C}$ mit $\iota : r \mapsto (r, 0)$ betrachtet. Sehr einfache Rechnungen genügen, um $(r, 0) + (s, 0) = (r + s, 0)$ und $(r, 0)(s, 0) = (rs, 0)$ nachzuweisen und weiters $-(r, 0) = (-r, 0)$ sowie $(r, 0)^{-1} = (\frac{1}{r}, 0)$ zu zeigen. In Zukunft werden wir also die reellen Zahlen mit den komplexen Elementen $(r, 0)$ identifizieren und im weiteren wieder r für diese Zahlen schreiben. Außerdem sehen wir, dass $(r, 0)(a_0, a_1) = (ra_0, ra_1)$ gilt.

Interessant wird es, wenn man die Eigenschaften anderer Elemente betrachtet:

$$(0, 1)(0, 1) = (-1, 0),$$

und damit finden wir in $\mathbb{C}$ eine Nullstelle des Polynoms $x^2 + 1$. Um die Schreibweise zu vereinfachen, führen wir eine Abkürzung für $(0, 1)$ ein, indem wir sagen

Definition 5.5.2. *Es gelte die Bezeichnung*

$$i := (0, 1).$$

Wir nennen i die imaginäre Einheit.

Wir haben schon nachgerechnet, dass $i^2 = -1$ gilt, und es folgt aus der Struktur von $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ und der komponentenweisen Definition der Addition, dass sich jedes Element (a_0, a_1) von $\mathbb{C}$ eindeutig schreiben lässt als $(a_0, a_1) = (a_0, 0) + a_1(0, 1)$ oder mit Hilfe der Abkürzungen aus Definition 5.5.2 als $(a_0, a_1) = a_0 + ia_1$.

Damit gewinnen wir Eulers Schreibweise für die komplexen Zahlen zurück. Mythisches oder Philosophisches haben wir dazu nicht benötigt.

In der Mathematik bezeichnet man die komplexe Variable üblicherweise mit z und die Komponenten mit $z = x + iy$. Wir nennen $x =: \Re z = \operatorname{Re} z$ den **Realteil** von z und $y =: \Im z = \operatorname{Im} z$ den **Imaginärteil** von z.

Die komplexen Zahlen lassen sich als Elemente von $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ klarerweise auch als Punkte in der Ebene deuten. Das führt auf die Definition von Wessel, Argand und Gauss. Auch die Polarkoordinatenrepräsentation durch Länge und Winkel ist auf diese geometrische Interpretation zurückzuführen, siehe Abbildung 5.1:

Bemerkung 5.5.3 (Polardarstellung komplexer Zahlen)**.** *Führen wir in der komplexen Ebene* Polarkoordinaten *ein, so läßt sich jede komplexe Zahl $z = x + iy$ als*

$$z = r(\cos\varphi + i \sin\varphi)$$

schreiben (siehe Abbildung 5.1). Hier ist der Radius *r durch den* Betrag *$|z|$ von z gegeben, d.h. $r = |z| := \sqrt{x^2 + y^2}$. Der Winkel φ wird auch* Argument *von z genannt und es gilt* $\tan\varphi = \frac{y}{x}$.

Die Darstellung von z in Polarschreibweise ist in bezug auf r eindeutig. Der Winkel φ ist zu gegebenem $z \neq 0$ allerdings nur bis auf Addition von ganzzahligen Vielfachen von 2π

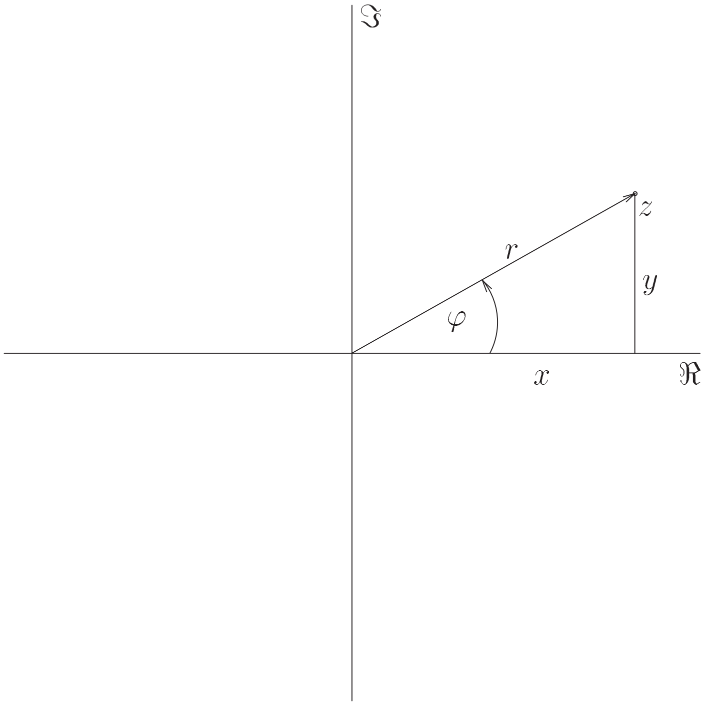

ABBILDUNG 5.1. Die komplexe Ebene

bestimmt. Ist $z = 0$, dann ist der Winkel gänzlich unbestimmt; $z = 0(\cos\varphi + i\sin\varphi)$ für beliebiges φ.

Das Multiplizieren komplexer Zahlen ist in der Polardarstellung besonders einfach. Es gilt nämlich

$$z_1 z_2 = r_1 r_2\big(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)\big),$$

wobei r_i bzw. φ_i der zu z_i $(i = 1, 2)$ gehörige Radius bzw. Winkel ist. Es werden also die Radien multipliziert und die Winkel addiert. Das Inverse von $z \neq 0$ ist ebenfalls sehr einfach zu bestimmen; es gilt $z^{-1} = \frac{1}{r}(\cos(-\varphi) + i\sin(-\varphi))$.

In der cartesischen Darstellung ist die Division ein wenig mühsamer:

$$\frac{a_1 + ib_1}{a_2 + ib_2} = \frac{(a_1 + ib_1)(a_2 - ib_2)}{(a_2 + ib_2)(a_2 - ib_2)} = \frac{a_1 a_2 + b_1 b_2 + i(a_2 b_1 - a_1 b_2)}{a_2^2 + b_2^2} = \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + i\frac{a_2 b_1 - a_1 b_2}{a_2^2 + b_2^2}.$$

In diesem Fall haben wir den „Bruch“ oben und unten mit derselben komplexen Zahl multipliziert, der **konjugiert komplexen** Zahl zu $a_2 + ib_2$, also mit $\overline{a_2 + ib_2} := a_2 - ib_2$. Wie wir im Nenner sehen können, in dem das Quadrat des Betrags von $a_2 + ib_2$ auftaucht, gilt für jede komplexe Zahl z

$$z\overline{z} = |z|^2,$$

und außerdem

$$\begin{aligned}\overline{\overline{z}} &= z,\\ \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_2},\\ \overline{z_1 z_2} &= \overline{z_1}\,\overline{z_2}.\end{aligned}$$

Wir wollen nun untersuchen, ob es uns gelingt, die Ordnungsrelation von $\mathbb{R}$ auf $\mathbb{C}$ auszudehnen, sodass wieder O1 und O2 gelten. Folgendes erstaunliches Resultat kommt dabei heraus.

Theorem 5.5.4. *Es gibt keine Ordnungsrelation auf $\mathbb{C}$, mit der $(\mathbb{C}, +, \cdot)$ ein geordneter Körper wird.*

Beweis. Angenommen, es gäbe eine Ordnungsrelation $\leq$, die alle notwendigen Eigenschaften aufweist. Dann gilt jedenfalls $-1 < 0 < 1$ wegen Proposition 5.3.2.(1) und (4).

Wegen $i \neq 0$ folgt aber wieder wegen Proposition 5.3.2.(4), dass $-1 = i^2 > 0$, ein Widerspruch. Daher existiert keine solche Ordnungsrelation. □

Nun aber zurück zu den Polynomen. Für ein beliebiges quadratisches Polynom mit komplexen Koeffizienten α_i können wir jetzt jedenfalls die Nullstellen ausrechnen. Sei nämlich

$$p(z) = \alpha_2 z^2 + \alpha_1 z + \alpha_0,$$

dann kann man alle Nullstellen von p mit Hilfe der wohlbekannten Formel

$$z_{1,2} = \frac{-\alpha_1 \pm \sqrt{\alpha_1^2 - 4\alpha_2\alpha_0}}{2\alpha_2}$$

berechnen.

Beispiel 5.5.5. *Sei das Polynom*

$$z^2 - (3 - 8i)z - 13 - 11i$$

gegeben. Die Nullstellen bestimmen wir wie folgt:

$$\begin{aligned} z_{1,2} &= \frac{3 - 8i \pm \sqrt{(3-8i)^2 + 4(13+11i)}}{2} \\ &= \frac{3 - 8i \pm \sqrt{-55 - 48i + 52 + 44i}}{2} \\ &= \frac{3 - 8i \pm \sqrt{-3 - 4i}}{2} \end{aligned}$$

Wir müssen nun die Wurzel aus $-3-4i$ ziehen, wofür sich zwei Möglichkeiten anbieten. Zum einen können wir in Polarkoordinaten verwandeln und $\sqrt{(r,\varphi)} = (\sqrt{r}, \frac{\varphi}{2})$ verwenden. Zum anderen ist es möglich, die Wurzel direkt zu ziehen. Dazu verwenden wir einen unbestimmten Ansatz. *Sei $\sqrt{-3-4i} = a + ib$. Dann gilt*

$$\begin{aligned} (a + ib)^2 &= -3 - 4i \\ a^2 - b^2 + 2iab &= -3 - 4i. \end{aligned}$$

Das führt zu dem Gleichungssystem

$$\begin{aligned} a^2 - b^2 &= -3 \\ 2ab &= -4. \end{aligned}$$

Mit einem kleinen Trick können wir den Lösungsweg abkürzen. Wir wissen, dass

$$a^2 + b^2 = |a + ib|^2 = |(a+ib)^2| = |-3-4i| = \sqrt{9+16} = 5$$

gilt, und aus dieser erhalten wir durch Addition bzw. Subtraktion mit der oberen Gleichung:

$$\begin{aligned} 2a^2 &= 2 \\ 2b^2 &= 8. \end{aligned}$$

Wir haben also $a = \pm 1$ und $b = \pm 2$, und aus der Beziehung $2ab = -4$ erhalten wir die Lösungen

$$\sqrt{-3-4i} = \pm(1 - 2i).$$

Setzen wir das in die Lösungsformel ein, dann erhalten wir

$$\begin{aligned} z_{1,2} &= \frac{3-8i \pm (1-2i)}{2} \\ z_1 &= 2-5i \\ z_2 &= 1-3i. \end{aligned}$$

Für quadratische Polynome haben die komplexen Zahlen also das Nullstellenproblem erledigt, doch wir wissen noch immer nicht, ob wir dasselbe für beliebige Polynome tun können. Die Frage ist, ob jedes nichtkonstante komplexe Polynom eine Nullstelle besitzt, ob also $\mathbb{C}$ **algebraisch abgeschlossen** ist. Dieses Problem hat J.C.F. Gauss 1799 in seiner Dissertation gelöst:

Theorem 5.5.6 (Fundamentalsatz der Algebra)**.** *Sei $p(z)$ ein beliebiges nichtkonstantes Polynom mit komplexen Koeffizienten:*

$$p(z) = \sum_{i=0}^{n} a_i z^i \quad \text{mit } a_i \in \mathbb{C},\ n > 1,\ a_n \neq 0.$$

Dann existiert ein $\alpha \in \mathbb{C}$ mit $p(\alpha) = 0$, es gibt also immer wenigstens eine (komplexe) Nullstelle.

Beweis. Der Beweis dieses Satzes würde das Lehrziel dieses Skriptums sprengen, und daher lassen wir ihn aus. Übrigens gibt es viele — über 100 — verschiedenen Beweise für diesen Satz. In jedem guten Buch über Funktionentheorie (komplexe Analysis) ist einer zu finden; siehe etwa [**Remmert, Schumacher 2001**]. □

Es lässt sich sogar noch ein klein wenig mehr sagen, denn wenn man eine Nullstelle eines Polynoms gefunden hat, dann kann man mit Hilfe der Polynomdivision folgenden Satz beweisen:

Theorem 5.5.7. *Sei p ein komplexes Polynom n–ten Grades und α eine Nullstelle von p. Dann gibt es ein Polynom q vom Grad $n-1$, und es gilt*

$$p(z) = q(z)(z-\alpha).$$

Man kann also einen Linearfaktor (das $z-\alpha$) abspalten.

Beweis. Ebenfalls in guten Funktionentheorie-Büchern nachzulesen. □

Fasst man die beiden Theoreme 5.5.6 und 5.5.7 zusammen, dann kann man die wichtige Folgerung über Polynome und ihre Nullstellen beweisen:

Korollar 5.5.8. *Sei p ein komplexes Polynom vom Grad n. Dann existieren genau n Linearfaktoren $z-\alpha_i$ mit $i = 1, \dots, n$, sodass*

$$p(z) = \prod_{i=1}^{n} z - \alpha_i.$$

Das Polynom zerfällt also über $\mathbb{C}$ in genau n Linearfaktoren.

Beweis. Nach dem Fundamentalsatz der Algebra hat p eine Nullstelle, die man nach Theorem 5.5.7 abspalten kann. Übrig bleibt ein Polynom q, dessen Grad um 1 kleiner ist als der von p. Auf q kann man wieder den Fundamentalsatz anwenden, usw. Das Korollar folgt mittels vollständiger Induktion. □

Das ist sehr praktisch, doch leider gibt es keine Möglichkeit, für allgemeine Polynome hohen Grades diese Linearfaktoren (d.h. die Nullstellen) zu bestimmen. Nils Henrik Abel (1802–1829) hat nämlich im Jahr 1824 den folgenden Satz bewiesen:

Theorem 5.5.9 (Abel). *Für jedes $n \geq 5$ existiert ein Polynom p mit rationalen Koeffizienten vom Grad n, das eine reelle Nullstelle r besitzt mit der Eigenschaft, daß r nicht geschrieben werden kann als algebraischer Ausdruck, der rationale Zahlen, Additionen, Subtraktionen, Multiplikationen, Divisionen und k–te Wurzeln enthält. Anders ausgedrückt existiert keine Formel und damit kein endlicher algebraischer Algorithmus, der aus den Koeffizienten eines Polynoms vom Grad $n \geq 5$ die Nullstellen berechnet.*

Beweis. Der Beweis dieses Satzes gehört in die höhere Algebra und kann unter dem Kapitel Galoistheorie z.B. in [**Scheja, Storch 1988**] nachgelesen werden. □

5.6. Die Quaternionen $\mathbb{H}$

Eine letzte interessante Frage kann man noch über Zahlenmengen stellen, die sich direkt aus der Definition von $\mathbb{C}$ als Körperstruktur auf $\mathbb{R}\times\mathbb{R}$ ergibt. Kann man z.B. auf $\mathbb{R}\times\mathbb{R}\times\mathbb{R} = \mathbb{R}^3$ auch eine Körperstruktur einführen?

Die Suche nach der Antwort auf diese Frage hat auch den Mathematiker Sir William Rowan Hamilton (1805–1865), einen der bedeutendsten Wissenschafter seiner Epoche beschäftigt, und im Jahr 1843 präsentierte er schließlich die Arbeit „On a new Species of Imaginary Quantities connected with a theory of Quaternions“ bei einem Treffen der Royal Irish Academy.

Doch Hamilton hatte es nicht geschafft, auf $\mathbb{R}^3$ eine Körperstruktur einzuführen. Er hatte zwar keine Probleme gehabt, auf jedem $\mathbb{R}^n$ durch komponentenweise Definition eine Addition zu erklären, die eine abelsche Gruppe ergab, doch die Multiplikation hatte nicht gelingen wollen. Was er dann zusammengebracht hat, war eine algebraische Struktur im $\mathbb{C}^2 = \mathbb{R}^4$ zu definieren.

Sei $\mathbb{H} = \mathbb{C} \times \mathbb{C}$ gegeben. Wir definieren Verknüpfungen auf $\mathbb{H}$ durch

$$\begin{aligned}(z_0, z_1) + (w_0, w_1) &:= (z_0 + w_0, z_1 + w_1)\\ (z_0, z_1)(w_0, w_1) &:= (z_0 w_0 - z_1\overline{w_1}, z_0 w_1 + z_1\overline{w_0}).\end{aligned}$$

Wir können die algebraischen Eigenschaften von $(\mathbb{H}, +, \cdot)$ untersuchen. Wegen der komponentenweisen Definition der Addition folgt sofort, dass $(\mathbb{H}, +)$ eine abelsche Gruppe ist.

Die Multiplikation ist assoziativ:

$$\begin{aligned}\big((z_0, z_1)(w_0, w_1)\big)(t_0, t_1) &= (z_0 w_0 - z_1\overline{w_1}, z_0 w_1 + z_1\overline{w_0})(t_0, t_1) =\\ &= (z_0 w_0 t_0 - z_1\overline{w_1}t_0 - z_0 w_1\overline{t_1} - z_1\overline{w_0}\overline{t_1}, z_0 w_0 t_1 - z_1\overline{w_1}t_1 + z_0 w_1\overline{t_0} + z_1\overline{w_0}\overline{t_0}) =\\ &= (z_0, z_1)(w_0 t_0 - w_1\overline{t_1}, w_0 t_1 + w_1\overline{t_0}) =\\ &= (z_0, z_1)\big((w_0, w_1)(t_0, t_1)\big),\end{aligned}$$

das Element $(1, 0)$ ist das Einselement bezüglich der Multiplikation (das ist leicht), und jedes Element verschieden von $0 = (0, 0)$ besitzt ein Inverses:

$$(z_0, z_1)^{-1} = \left(\frac{z_0}{|z_0|^2 + |z_1|^2}, \frac{-z_1}{|z_0|^2 + |z_1|^2}\right).$$

Beidseitig gelten die Distributivgesetze, doch das Kommutativgesetz bezüglich der Multiplikation ist **nicht** erfüllt. Eine algebraische Struktur dieser Art nennt man **Schiefkörper**.

Die Quaternionen der Form $(z, 0)$ bilden einen Körper, der isomorph zu $\mathbb{C}$ ist, und daher werden wir diese Elemente in Zukunft auch mit den komplexen Zahlen identifizieren und wieder z schreiben.

Wenn wir spezielle Elemente betrachten, erhalten wir erstaunliche Ergebnisse:

$$(0,1)(0,1) = (-1,0)$$
$$(0,i)(0,i) = (-1,0).$$

Die Quaternionen enthalten also noch zwei „Wurzeln“ von -1. Wir schreiben $j := (0,1)$ und $k := (0,i)$ und erhalten so die Rechenregeln

$$\begin{array}{lll} i^2 = -1, & j^2 = -1, & k^2 = -1, \\ ij = k, & jk = i, & ki = j, \\ ji = -k, & kj = -i, & ik = -j. \end{array}$$

Aus der Definition der Quaternionen lässt sich leicht zeigen, dass man jedes $q \in \mathbb{H}$ eindeutig schreiben kann als $z_0 + z_1 j$ (Achtung auf die Reihenfolge!) mit komplexen Koeffizienten z_0 und z_1 oder als $q = a_0 + a_1 i + a_2 j + a_3 k$ mit reellen Koeffizienten a_i.

Der Betrag einer Quaternione ist

$$|(z_0, z_1)| = \sqrt{|z_0|^2 + |z_1|^2},$$

und die konjugierte Quaternione ist

$$\overline{(z_0, z_1)} = (z_0, -z_1).$$

Es gilt analog zu den komplexen Zahlen $|q|^2 = q\overline{q}$.

Interessant ist vielleicht noch eine weitere Darstellung der Quaternionen als Paar (a, A) mit eine reellen Zahl a und einem Vektor $A \in \mathbb{R}^3$. In diesem Fall lassen sich die Operationen hinschreiben als

$$(a, A) + (b, B) = (a + b, A + B)$$
$$(a, A)(b, B) = (ab - AB, aB + Ab + A \times B),$$

also fast so wie die Operationen in $\mathbb{C}$, bis auf den Term $A \times B$ in der Definition der Multiplikation. An dieser Definition kann man auch schon erahnen, dass Quaternionen etwas mit Drehungen zu tun haben.

Die Frage, die sich die Mathematiker jetzt stellten war, ob niemand klug genug war, die richtige Definition einer Multiplikation zu finden, oder ob die Schwierigkeiten einen mathematischen Grund haben.

Arthur Cayley (1821–1895) hat versucht, die Methode noch einmal anzuwenden und auf $\mathbb{H} \times \mathbb{H} \cong \mathbb{R}^8$ eine Multiplikation einzuführen. Es gelang ihm, die Cayley-Zahlen oder Oktaven oder Okternionen $\mathbb{O}$ zu definieren, doch deren algebraische Eigenschaften lassen doch deutlich mehr zu wünschen übrig als die der Quaternionen. Okternionen sind nicht einmal mehr ein Schiefkörper. Es besitzt zwar jedes Element ein eindeutiges Inverses, doch die Multiplikation ist nicht assoziativ! Solch eine algebraische Struktur, in der über einer abelschen Gruppe eine Multiplikation definiert wird, die die Distributivität erfüllt und wo Einselement und Inverse existieren, heißt (nichtassoziative) **Divisionsalgebra**.

Ein tiefer Satz aus der Differentialgeometrie besagt nun, dass Divisionsalgebren über $\mathbb{R}^n$ nur in den Dimensionen 1, 2, 4 und 8 existieren, und in jeder dieser Dimensionen genau eine, nämlich $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ und $\mathbb{O}$. Es war also nicht Unfähigkeit, die die Mathematiker des 19. Jahrhunderts daran gehindert hat, über allen $\mathbb{R}^n$ eine Körperstruktur zu finden, sondern sie haben nach nicht Existentem gestrebt.

Damit beenden wir unseren Ausflug in die Welt der Zahlen. Beginnend von $\mathbb{N}$, der Klasse von Zahlen, deren Geschichte ihren Ursprung bereits in grauer Vorzeit hat, haben wir sie basierend auf den neuen mathematischen Grundlagen neu entdeckt. Weiter ging es über die ganzen zu den rationalen Zahlen und darauf aufbauend zu den reellen Zahlen, der Grundlage der Analysis. Auf der Suche nach den Nullstellen der Polynome sind wir zu den komplexen Zahlen und Gauss' fundamentalem Theorem gelangt. Selbst die Frage, ob wir damit schon alle Zahlensysteme gefunden haben, die $\mathbb{R}$ als Unterkörper haben und in denen man dividieren kann, haben wir untersucht. Wir haben alle dieser Strukturen gefunden, und daher ist es jetzt an der Zeit, Neuland zu entdecken und zu erkunden, was Generationen von Mathematikern aus den hier präsentierten Prinzipien geschaffen haben.

Ich hoffe, dass die Reise in die Grundlagen der modernen Mathematik wenigstens ein bisschen Freude bereitet hat. Ich wünsche allen noch viel Vergnügen mit all den Theorien, Strukturen und Anwendungen, die im Verlauf des Studiums noch kommen mögen.

Literaturverzeichnis

[Behrends 2003] Behrends, E., *Analysis, Band 1*, Ein Lehrbuch für den sanften Wechsel von der Schule zur Uni, Vieweg, Braunschweig/Wiesbaden, 2003.

[Beutelspacher 1999] Beutelspacher, A., *Das ist o.B.d.A. trivial*, Tips und Tricks zur Formulierung mathematischer Gedanken, Vieweg, Braunschweig/Wiesbaden, 1999.

[Bishop 1967] Bishop, E., *Foundations of constructive analysis*, McGraw–Hill, New York, 1967.

[Bronstein et al. 1989] Bronstein, I.N.; Semendjajew, K.A., *Taschenbuch der Mathematik*, Verlag Harri Deutsch, Thun, 1989.

[Cigler, Reichel 1987] Cigler, J.; Reichel, H.C., *Topologie*, B.I. Hochschultaschenbücher, Mannheim/Wien/Zürich, 1987.

[Heuser 1986] Heuser, H., *Lehrbuch der Analysis, Teil 1*, B.G. Teubner, Stuttgart, 1986.

[O'Connor, Robertson 1996] O'Connor, J.J; Robertson, E.F., *A history of set theory*, `http://www-groups.dcs.st-and.ac.uk/history/HistTopics/Beginnings_of_set_theory.html`, 1996.

[Remmert, Schumacher 2001] Remmert, R.; Schumacher, *Funktionentheorie 1*, Springer Verlag, 2001.

[Scheja, Storch 1988] Scheja, G.; Storch, U., *Lehrbuch der Algebra*, Teubner Verlag, Stuttgart, 1988.