Grundlagen der Mathematik

Thomas Peters
Thomas' Mathe-Seiten
www.mathe-seiten.de

29. September 2004

Inhaltsverzeichnis

Tabellenverzeichnis

1 Logik

1.1 Aussagen und Aussageformen

Mathematik zu betreiben ist nüchtern betrachtet nichts weiter, als aus wahren Aussagen weitere wahre Aussagen zu folgern. Die Regeln, nach denen dieses Folgern abläuft, werden duch die Logik bestimmt. Dabei ist es offenkundig, dass man nicht bei „nichts“ anfangen kann zu folgern, sondern dass man auf gewissen Grundtatsachen aufbauen muss, über die man sich geeinigt hat und die per Definition als wahr angenommen werden. Diese Grundtatsachen heißen *Axiome* der mathematischen Theorie.

Eine mathematische *Aussage* ist ein Satz, der entweder wahr oder falsch ist. Dies ist das Prinzip vom ausgeschlossenen Dritten (*tertium non datur*). Wir bezeichnen den Wahrheitswert einer Aussage A als w für wahr und f für falsch. Eine *Aussageform* ist ein Satz, der eine *Aussagevariable* x enthält und erst dann wahr oder falsch wird, wenn man für x ein entsprechendes Objekt der mathematischen Theorie einsetzt. Ein Beispiel für eine Aussageform wäre $A(x)$: x ist eine ganze Zahl. $A(x)$ wird zu einer Aussage, wenn man für x konkrete Zahlen einsetzt, bspw. wäre $A(2)$ wahr und $A(\sqrt{2})$ falsch.

Die Logik beschäftigt sich nun mit der Manipulation und Verknüpfung von Aussagen. Die einfachste Manipulation ist die *Negation*. Die Negation der Aussage A wird mit $\neg A$ bezeichnet und kehrt den Wahrheitswert von A um. Man verdeutlicht sich den Einfluss logischer Operationen auf Aussagen gerne in einer Wahrheitswertetafel (siehe Tabelle 1.1). Offensichtlich gilt für die Negation $\neg(\neg A) = A$.

A	$\neg A$
w	f
f	w

Tabelle 1.1: Wahrheitswertetafel für $\neg A$.

Eine höhere Komplexitätsstufe erreicht man durch die Verknüpfung zweier Aussagen durch sog. zweistellige logische Operationen. Da hier zwei Aussagen verknüpft werden, welche jeweils unabhängig voneinander wahr oder falsch sein können, gibt es insgesamt 16 verschiedene Verknüpfungen. Alle diese Verknüpfungen können jedoch zusammen mit der Negation aus einer einzigen zweistelligen Verknüpfung gewonnen werden. Wir wählen dazu die *Disjunktion* $A \vee B$, welche genau dann wahr ist, wenn A oder B wahr sind[1]. Tabelle 1.2 zeigt die Wahrheitswertetafel.

[1] nicht: „entweder oder“!

A	B	$A \vee B$	$A \wedge B$
w	w	w	w
w	f	w	f
f	w	w	f
f	f	f	f

Tabelle 1.2: Wahrheitswertetafel für $A \vee B$ und $A \wedge B$.

Ebenso wird man eine Verknüpfung brauchen, welche genau dann wahr ist, wenn A und B wahr sind. Diese Verknüpfung heißt *Konjunktion* und wird mit $A \wedge B$ bezeichnet. Man erhält sie formal als $\neg(\neg A \vee \neg B)$.

Nachdem wir nun die beiden grundlegenden zweistelligen Verknüpfungen definiert haben, machen wir uns an unser ursprüngliches Ziel, nämlich aus bekannten Aussagen neue folgern zu können. Wir brauchen also eine Verknüpfung, welche angibt, wann die Folgerung „A impliziert B“ wahr sein soll. Es ist klar, dass man aus etwas Wahrem nichts Falsches folgern darf. Subtiler ist da schon die Frage, welchen Wahrheitswert die Folgerung haben soll, wenn die *Voraussetzung* A von vornherein falsch ist. Man hat sich darauf geeinigt, eine solche Folgerung grundsätzlich als wahr zu definieren. Es gilt daher der Merksatz: Aus etwas Falschem kann man alles folgern! Die so definierte Verknüpfung heißt *Implikation* und hat die in Tabelle 1.3 dargestellten Wahrheitswerte. Die Werte entsprechen der Verknüpfung $\neg A \vee B$.

A	B	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	w	w
w	f	f	f
f	w	w	f
f	f	w	w

Tabelle 1.3: Wahrheitswertetafel für $A \Rightarrow B$ und $A \Leftrightarrow B$.

Da die Wahrheitswerte der Implikation erfahrungsgemäß für Verwirrung sorgen, werden wir sie uns noch etwas genauer ansehen. Am besten sieht man den Sinn dieser Definition an einem Beispiel. Es sei $A(x)\colon x$ ist größer als 5 und $B(x)\colon x$ ist positiv. Es leuchtet unmittelbar ein, dass die Folgerung $A \Rightarrow B$ wahr sein sollte. Der Wahrheitsgehalt der Implikation hängt aber maßgeblich von x ab. Hier können zwei Fälle auftreten. Erstens: x ist tatsächlich größer als 5. Da 5 größer ist als 0, ist auch x größer als 0 und somit positiv. Die Implikation stimmt also. Zweitens: x ist nicht größer als 5. Dann ist die Implikation dank unserer Definition trotzdem wahr, und zwar unabhängig davon, ob x positiv ist oder nicht! Man sieht also, dass diese Konvention durchaus Sinn macht.

Die letzte unverzichtbare zweistellige logische Operation ist die *Äquivalenz*. Zwei Aussagen A und B heißen äquivalent, wenn sowohl $A \Rightarrow B$ als auch $B \Rightarrow A$ wahr sind. Man setzt also $A \Leftrightarrow B$ als $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Wir schließen diesen Abschnitt mit einer Interpretation der eher technischen Einführung der Implikation. In der Implikation $A \Rightarrow B$ heißt die Aussage A *hinreichende Bedingung* für B

und B *notwendige Bedingung* für A. Denn wenn A gilt, so muss, sofern die Implikation $A \Rightarrow B$ wahr ist, auch B wahr sein. A ist in diesem Sinne hinreichend für B. Gilt umgekehrt B nicht, so kann auch A nicht gelten, denn aus A würde ja B folgen! Also ist B notwendig für A. Es ist damit $A \Rightarrow B$ äquivalent zu $(\neg B) \Rightarrow (\neg A)$. Diese Umformulierung der Implikation heißt Kontraposition und ist ein wichtiges Beispiel einer Tautologie, womit wir uns im nächsten Abschnitt beschäftigen werden.

1.2 Tautologien

Eine Aussageform heißt *Tautologie* oder *Wahrform*, wenn sie unabhängig von den Werten der Aussagevariablen immer wahr ist. Entsprechend heißt eine Aussageform *Kontradiktion* oder *Falschform*, wenn sie immer falsch ist. Schließlich heißt sie *Neutralität* oder *Neutralform*, wenn sie weder Wahrform noch Falschform ist. Ein einfaches Beispiel für eine Tautologie wäre $A(x) \vee \neg A(x)$, für eine Kontradiktion $A(x) \wedge \neg A(x)$ und für eine Neutralform $A(x) \vee B(x)$.

Wir betrachten nun einige wichtige Beispiele für Tautologien. Ganz am Anfang hatten wir schon

$$\neg(\neg A) \Leftrightarrow A$$

kennengelernt. Die Negation der Negation einer Aussage ist wieder die Aussage selbst. Beweisen kann man diese und alle anderen aufgeführten Tautologien, indem man die Wahrheitswertetafeln der Aussagen links und rechts vom Äquivalenzzeichen erstellt und feststellt, dass die Wahrheitswerte übereinstimmen. Wir werden deshalb darauf verzichten. Um sich bei größeren Ausdrücken unnötige Klammern zu sparen, legt man fest, dass die Negation am stärksten bindet, dann kommen gleichwertig Disjunktion und Konjunktion, und am geringsten bindet Implikation und Äquivalenz. Nun halten wir fest, dass für die Disjunktion und die Konjunktion die *Kommutativgesetze*

$$A \vee B \Leftrightarrow B \vee A, \qquad A \wedge B \Leftrightarrow B \wedge A$$

gelten. Desweiteren gelten die *Assoziativgesetze*

$$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C), \qquad (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C),$$

welche besagen, dass man bei mehreren Disjunktionen oder Konjunktionen hintereinander die Klammern weglassen kann, sowie die *Distributivgesetze*

$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C), \qquad A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C).$$

Nun gibt es eine Reihe von Tautologien, die dabei behilflich sind, längere logische Ausdrücke zu vereinfachen. Dazu gehören die *Idempotenzgesetze*

$$A \vee A \Leftrightarrow A, \qquad A \wedge A \Leftrightarrow A,$$

sowie die *Absorptionsgesetze*

$$A \vee (A \wedge B) \Leftrightarrow A, \qquad A \wedge (A \vee B) \Leftrightarrow A.$$

Außerdem untersuchen wir noch, wie die Negation einer Disjunktion bzw. einer Konjunktion aussieht. Dies führt auf die *de Morgan'schen Regeln*

$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B, \qquad \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B.$$

Desweiteren gibt es einige Tautologien, die bei Beweisen sehr nützlich sind. Dazu gehören wie gesagt die *Kontraposition*

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A),$$

der *Kettenschluss*

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C),$$

der *direkte Schluss* (*modus ponens*)

$$A \wedge (A \Rightarrow B) \Rightarrow B,$$

sowie der *indirekte Schluss* (*modus tollens*)

$$(A \Rightarrow B) \wedge \neg B \Rightarrow \neg A.$$

Die Nützlichkeit dieser Tautologien werden wir schon im nächsten Abschnitt kennenlernen.

1.3 Quantoren

Für die Verknüpfung von Aussagen mit den bisherigen Regeln sind uns noch Grenzen gesetzt. So können wir zwar die Aussagen $A(1)$ und $A(2)$ durch $A(1) \wedge A(2)$ verknüpfen, dies geht aber nur solange, wie wir eine endliche Anzahl von Aussagen haben. Man möchte aber auch unendlich viele Aussagen miteinander verknüpfen können. Wenn wir z. B. die Aussageform $A(x)$ auf alle reellen Zahlen im Intervall $[1, 2]$ anwenden wollen, so haben wir keine Chance[2]. Man führt deshalb den *Allquantor* $\forall$ ein, welcher genau dann wahr ist, wenn $A(x)$ für alle betrachteten x gilt. In unserem Fall wäre

$$\bigwedge_{x \in [1,2]} : A(x)$$

die gesuchte Verknüpfung. Für endlich viele $x \in X$ mit $X = \{x_1, \ldots, x_n\}$ gilt dann

$$\bigwedge_{x \in X} : A(x) \Leftrightarrow A(x_1) \wedge \cdots \wedge A(x_n).$$

Wir fragen uns nun nach der Negation der Aussage $\bigwedge_x : A(x)$. Wenn die Aussage nicht für alle x gilt, dann muss es offenkundig ein x geben, für dass $A(x)$ nicht gilt, was äquivalent ist dazu, dass für dieses x dann $\neg A(x)$ gilt. Diese Existenz liefert formal der *Existenzquantor* $\exists$. Es gilt also

$$\neg \bigwedge_{x \in X} : A(x) \Leftrightarrow \bigvee_{x \in X} : \neg A(x).$$

[2] Die Anzahl der reellen Zahlen in $[1, 2]$ ist nicht nur unendlich, sondern sogar überabzählbar.

Der Existenzquantor sagt nur, dass es so ein x geben muss, er sagt nicht wieviele. Oft kommt es vor, dass dieses x eindeutig bestimmt ist. Man schreibt dann $\exists!$ für die Eindeutigkeit. Analog wie für den Allquantor findet man auch für den Existenzquantor im Falle endlich vieler Aussagen

$$\underset{x\in X}{\exists}: A(x) \Leftrightarrow A(x_1) \vee \cdots \vee A(x_n).$$

Die Negation des Existenzquantors ergibt den Allquantor für die negierte Aussage, denn gibt es kein x mit $A(x)$, so muss $A(x)$ für alle x falsch bzw. $\neg A(x)$ für alle x wahr sein:

$$\neg \underset{x\in X}{\exists}: A(x) \Leftrightarrow \underset{x\in X}{\forall}: \neg A(x).$$

Wir haben damit die de Morgan'schen Regeln aus dem letzten Abschnitt auf den Fall unendlich vieler Aussagen verallgemeinert. Diese Gesetze sind äußerst wichtig, denn man kann so den Beweis einer Allaussage reduzieren auf den Beweis einer Existenzaussage und umgekehrt, was u. U. sehr viel leichter ist.

Zum Abschluss kommen wir noch auf die Bedeutung der Variablen x zu sprechen. Dieses x ist in der Aussageform $A(x)$ eine sog. *freie Variable*, d. h. ihr Wert ist frei wählbar. Dagegen ist x in der Aussage $\underset{x}{\forall}: A(x)$ eine *gebundene Variable*, denn durch den Allquantor wird aus der Aussageform $A(x)$ eine Aussage, eben die Allaussage. Die Variable x darf deshalb außerhalb des Quantors nicht mehr verwendet werden. Entsprechendes gilt für den Existenzquantor. Dies spielt eine wichtige Rolle bei der Verknüpfung mehrerer Quantoren. Betrachten wir z. B. eine Aussageform $A(x, y)$, die von den zwei Variablen x und y abhängt und den Ausdruck

$$\underset{x\in X}{\exists}: \underset{y\in Y}{\forall}: A(x, y) \Rightarrow \underset{y\in Y}{\forall}: \underset{x\in X}{\exists}: A(x, y).$$

Ist diese Implikation wahr oder falsch? Auf der linken Seite steht, dass es ein $x \in X$ gibt, so dass für alle $y \in Y$ die Aussage $A(x, y)$ wahr ist. Wenn dem so ist, so wird man sicherlich für alle $y \in Y$ ein $x \in X$ finden, so dass $A(x, y)$ gilt (rechte Seite), denn man braucht nur das x nehmen, dessen Existenz die linke Seite der Implikation verbürgt. Dagegen ist die Implikation

$$\underset{y\in Y}{\forall}: \underset{x\in X}{\exists}: A(x, y) \Rightarrow \underset{x\in X}{\exists}: \underset{y\in Y}{\forall}: A(x, y)$$

falsch. Hier steht nämlich links, dass man für jedes $y \in Y$ ein $x \in X$ findet mit $A(x, y)$. Dieses x kann aber selbstverständlich vom jeweiligen y abhängen! Dagegen verlangt die rechte Seite, dass es ein $x \in X$ gibt, so dass für alle $y \in Y$ die Aussage $A(x, y)$ gilt. Dies ist natürlich weit mehr, als die linke Seite hergibt. Die Variable y ist in der Existenzaussage links eine freie Variable, wogegen sie rechts in der Allaussage gebunden ist. Dieser Wechsel ist nicht erlaubt. Dagegen zeigt die erste Implikation, dass man durchaus von einer gebundenen zu einer freien Variablen wechseln darf.

Als Beispiel wählen wir $X = Y = \mathbb{N}$ und $A(x, y)$: $x + y \geq 5$. Die erste Implikation sagt dann

$$\underset{x\in\mathbb{N}}{\exists}: \underset{y\in\mathbb{N}}{\forall}: x + y \geq 5 \Rightarrow \underset{y\in\mathbb{N}}{\forall}: \underset{x\in\mathbb{N}}{\exists}: x + y \geq 5.$$

Diese Implikation ist wahr, denn $x = 5$ leistet das Gewünschte. Als Gegenbeispiel zur zweiten Implikation nehmen wir $X = Y = \mathbb{Z}$, $A(x, y)\colon x + y = 0$ und betrachten

$$\underset{y\in\mathbb{Z}}{\forall}: \underset{x\in\mathbb{Z}}{\exists}: x + y = 0 \Rightarrow \underset{x\in\mathbb{Z}}{\exists}: \underset{y\in\mathbb{Z}}{\forall}: x + y = 0.$$

Links braucht man nur $x = -y$ zu wählen, wohingegen es mit Sicherkeit kein $x \in \mathbb{Z}$ gibt, so dass die rechte Seite erfüllt wäre.

2 Mengen

2.1 Naive Mengenlehre

Es hat sich in der Mathematik als konstruktiv und äußerst nützlich erwiesen, das gesamte Universum der Mathematik auf dem Fundament der Mengenlehre zu bauen. Mengen bilden sozusagen die übergeordnete Struktur schlechthin, welche sich wie ein roter Faden durch alle Bereiche zieht. Dies zeigt, wie mächtig der Begriff der Menge ist. Doch vor allzu unbeschwertem — machmal sagt man auch „naivem“ — Umgang mit dem Mengenbegriff muss gewarnt werden. Auftauchende Paradoxien haben die noch in den Kinderschuhen steckende Mengenlehre in eine tiefe Krise gestürzt. Dennoch wählen wir zunächst einen intuitiven Einstieg, um uns mit dem Mengenbegriff vertrauter zu machen, und betrachten erst später die Axiome, die uns dieses Handeln ermöglichten.

Bei der exakten Definition des Mengenbegriffs stößt man unweigerlich auf Schwierigkeiten. Denn Mengen sind die elementarste Einheit in der Mathematik, man kann zu ihrer Definition nicht etwas noch Elementareres nehmen, sie „sind einfach da“. Für uns ist daher eine *Menge* eine Ansammlung von Objekten, den *Elementen* der Menge. Von jedem Objekt x muss man eindeutig sagen können, ob es Element einer Menge M ist oder nicht. Im ersten Fall schreibt man $x \in M$, im zweiten Fall $x \notin M$. Eine Menge ist eindeutig durch die Angabe aller ihrer Elemente bestimmt. Wenn man die Elemente explizit angeben kann, so schreibt man sie in geschweiften Klammern. Bspw. ist die Menge $M := \{1\}$[1] die Menge, die als einziges Element die 1 enthält. Die Menge, die kein Element enthält, heißt *leere Menge* und hat eine besondere Bezeichnung, nämlich $\emptyset$. Es ist also

$$\emptyset := \{\}.$$

Man sagt, dass die Menge M *(unechte) Teilmenge* der Menge N ist, wenn jedes Element der Menge M auch Element der Menge N ist und schreibt dann $M \subseteq N$. Oder etwas formaler ausgedrückt[2]

$$M \subseteq N :\Leftrightarrow \bigvee_{x \in M} : x \in N.$$

Entsprechend definiert man $M \nsubseteq N$. Da wir noch nicht so viel Übung mit der Formalisierung von Umgangssprache haben, geben wir am Anfang noch wörtliche und formale Definition gleichzeitig. Zwei Mengen M und N heißen gleich, wenn $M \subseteq N$ und $N \subseteq M$ gilt

$$M = N :\Leftrightarrow M \subseteq N \wedge N \subseteq M.$$

[1] Das zeichen $:=$ bedeutet „wird gesetzt als“, „wird definiert als“.
[2] Das Zeichen $:\Leftrightarrow$ bedeutet „wird definiert als“, „definitionsgemäß genau dann wenn“

Sind sie nicht gleich, so sind sie ungleich ($M \neq N$). M heißt *echte Teilmenge* von N (in Zeichen $M \subset N$), wenn $M \subseteq N$, aber nicht $M = N$ gilt

$$M \subset N :\Leftrightarrow M \subseteq N \wedge M \neq N.$$

Die Bedeutung von $M \not\subset N$ sollte klar sein. Ist M (echte) Teilmenge von N, so heißt N (echte) *Obermenge* von M

$$N \supseteq M :\Leftrightarrow M \subseteq N, \qquad N \supset M :\Leftrightarrow M \subset N.$$

Analog setzt man $N \not\supseteq M$ und $N \not\supset M$.

Wir werden in der Regel das Zeichen $\subseteq$ statt $\subset$ benutzen, wenn es nicht wesentlich ist, eine strikte Enthaltensrelation zu haben. Genauso verfahren wir übrigens mit $\leq$ und $<$ (siehe Abschnitt 3.1).

Nach so vielen Definitionen nun zu einem Beispiel. Betrachtet werde die Menge $M := \{1, 2, 3, 4, 5\}$. Dann ist $M = \{5, 4, 3, 2, 1\}$, denn die Reihenfolge, in der die Elemente aufgezählt werden, spielt keine Rolle. Außerdem ist $\{1, 2, 3\} \subseteq M$ und $\{1, 2, 3\} \subset M$, aber $\{6\} \not\subseteq M$.

Man kann Mengen auch angeben, indem man eine Aussageform $A(x)$ verwendet. Man muss dann die Elemente x aus einer gewissen *Grundmenge* N nehmen und setzt dann

$$M = \{\, x \in N \mid A(x) \,\}.$$

Im Beispiel wäre $\{1, 2, 3\} = \{\, x \in M \mid x \leq 3 \,\}$. Natürlich ist die Aussageform $A(x)$ nicht eindeutig bestimmt, denn es ist $\{\, x \in M \mid x < 4 \,\}$ die gleiche Menge.

Die Menge aller Teilmengen von M heißt die *Potenzmenge* von M und wird mit $\mathcal{P}(M)$ bezeichnet. Bei ihrer Definition bekommen wir jedoch Probleme. Wir könnten sie zwar definieren als

$$\mathcal{P}(M) := \{\, N \mid N \subseteq M \,\},$$

aber es ist überhaupt nicht klar, aus welcher Grundmenge man die Mengen N zu nehmen hat. Aus der Menge aller Mengen etwa?

2.2 Axiomatische Mengenlehre

Wir werden gleich sehen, dass es eine solche Menge nicht geben kann. Wir beginnen zunächst jedoch mit einer etwas anderen Überlegung. Stellen wir uns einen Barbier vor, der behauptet, alle Dorfbewohner zu rasieren, die sich nicht selbst rasieren. Rasiert der Barbier sich selbst? Falls ja, so gehört er zu den Bewohnern, die sich selbst rasieren, also rasiert er sich nach seiner eigenen Aussage nicht selbst. Falls nein, so gehört er zu denen, die sich nicht selbst rasieren, und wird daher nach seiner Aussage von sich selbst rasiert. So oder so kommen wir zu einem Widerspruch. Die Ursache des Widerspruchs liegt in der Selbstbezüglichkeit der Aussage des Barbiers. Wir halten also fest, dass man mit selbstbezüglichen Aussagen sehr vorsichtig sein muss.

Die Existenz der Menge aller Mengen wäre ein Problem, da wir bald zeigen werden, dass man zu jeder Menge eine andere Menge finden kann, die diese nicht enthält. Doch auch obiges Problem hat eine Entsprechung in der Mengenlehre, und zwar in Form der *Russel'schen Antinomie*, bei der man eine Menge M betrachtet, für die gilt: Es ist $x \in M$ genau dann, wenn $M \notin M$ ist. Fragt man nun, ob $M \in M$ gilt (d. h. man betrachtet den Fall $x = M$), so erhält man genau das gerade besprochene Paradoxon.

Um sicher zu gehen, dass derlei Widersprüche in der Mathematik nicht auftreten, hat man die Mengenlehre streng axiomatisch begründet[3]. Wir geben hier einen kurzen Abriss über die wichtigsten[4] Axiome, die der naiven Mengenlehre zugrunde liegen. Konkret besprechen wir eine Variante des *Zermelo-Fraenkel-Axiomensystems*. Um über Mengen reden zu können, müssen wir sichergehen, dass es Mengen überhaupt gibt. Wir beginnen daher mit dem

Axiom 1 (Existenzaxiom): *Es gibt eine Menge.*

Weitere Objekte werden zunächst einmal nicht zugelassen. Insbesondere gibt es keine Elemente, die nicht selbst Mengen sind. Alle Elemente von Mengen müssen also stets selbst Mengen sein. Als nächstes definieren wir, dass eine Menge eindeutig durch ihre Elemente bestimmt ist.

Axiom 2 (Extensionalitätsaxiom): *Mengen, die die gleichen Elemente haben, sind gleich.*

Nun können wir einen ersten Schritt machen, um aus vorhandenen Mengen neue Mengen zu erzeugen.

Axiom 3 (Aussonderungsaxiom): *Sei M eine Menge und $A(x)$ eine Aussageform für die Elemente $x \in M$. Dann gibt es eine Menge[5], die genau die Elemente $x \in M$ enthält, für die $A(x)$ gilt.*

Wir werden gleich die Mächtigkeit dieses Axioms unter Beweis stellen, indem wir unseren ersten Satz beweisen.

Satz 1: *Die leere Menge existiert.*

BEWEIS: Sei M die Menge, deren Existenz Axiom 1 sichert. Betrachte die Menge

$$\emptyset := \{\, x \in M \mid x \neq x \,\}.$$

Offenbar hat die so definierte Menge keine Elemente, denn wäre $x \in \emptyset$, so würde $x \neq x$ folgen, was ein Widerspruch ist. Also gilt $\emptyset = \{\}$. □

Ganz ähnlich beweist man den folgenden

Satz 2: *Sei M eine Menge. Dann gilt $\emptyset \subseteq M$.*

[3] Erst später wurde bewiesen, dass man sich der Widerspruchsfreiheit der Mengenlehre prinzipiell nicht sicher sein kann.

[4] Auf Axiome, die nur innerhalb der Mengenlehre selbst wichtig sind, gehen wir nicht ein.

[5] Die Eindeutigkeit dieser Menge folgt aus Axiom 2.

BEWEIS: Wir müssen die Implikation $x \in \emptyset \Rightarrow x \in M$ zeigen. Da die Voraussetzung aber für alle x falsch ist, ist die Implikation trivialerweise immer wahr. Daraus folgt die Behauptung.□

Wir können nun die Frage beantworten, ob es die Menge aller Mengen gibt. Wenn es sie gäbe, so müsste sie per Definition alle anderen Mengen (und sich selbst!) enthalten. Es gilt aber der

Satz 3: *Für jede Menge M gibt es eine Menge N, so dass $N \notin M$ gilt.*

BEWEIS: Wähle $N := \{\, x \in M \mid x \notin x \,\}$. Nehmen wir an $N \in M$. Es muss $N \in N$ oder $N \notin N$ gelten. Sei zunächst $N \in N$. Dann folgt aus $N \in M$ direkt $N \notin N$. Ist andererseits $N \notin N$, so gilt wegen $N \in M$ doch $N \in N$. Man erhält so oder so einen Widerspruch. Also kann nur $N \notin M$ gelten. □

Nun da wir gesehen haben, dass es die Menge aller Mengen nicht gibt, müssen wir uns die Exitenz der Potenzmenge durch ein Axiom verschaffen.

Axiom 4 (Potenzmengenaxiom): *Zu jeder Menge M gibt es eine Menge $\mathcal{P}(M)$, die genau aus den Teilmengen von M besteht.*

Nun sind wir wieder dort angelangt, wo wir den Bereich der naiven Mengenlehre verlassen hatten. Wir werden aber noch etwas weiter gehen und zusätzliche Axiome angeben, die uns später nützlich erscheinen werden.

Axiom 5 (Paarmengenaxiom): *Zu je zwei Mengen M und N gibt es eine Menge, welche genau M und N als Elemente hat.*

Axiom 6 (Vereinigungsmengenaxiom): *Zu jeder Menge M gibt es eine Menge, die genau aus den Elementen der Elemente von M besteht.*

Diese beiden Axiom werden wir im nächsten Abschnitt benutzen, um wichtige Operationen auf Mengen einzuführen. Wir gehen deshalb hier nicht näher darauf ein.

Wir werden später die Notwendigkeit spüren, auch Mengen mit unendlich vielen Elementen zu betrachten. Diese Mengen können mit unseren bisherigen Mitteln nicht konstruiert werden. Wir wählen unser Axiom aber jetzt bereits so, dass wir es später verwenden können, um in sehr natürlicher Weise die Menge der natürlichen Zahlen zu definieren.

Axiom 7 (Unendlichkeitsaxiom): *Es gibt eine Menge, die $\emptyset$ und mit jedem Element M auch die Menge enthält, die aus M und den Elementen von M besteht.*

Das mit Abstand umstrittenste Axiom der Mengenlehre ist das sogenannte *Auswahlaxiom*. Es gibt viele Analogien zwischen dem Auswahlaxiom und dem Parallelenaxiom aus der euklidischen Geomtrie. Auch hier hat man zunächst versucht, es aus den anderen Axiomen herzuleiten, bis schließlich gezeigt werden konnte, dass es unabhängig von den restlichen Axiomen ist. Seine Einführung hat Vor- und Nachteile. Der Vorteil liegt darin, dass man durch das Auswahlaxiom Sätze von großer Allgemeinheit beweisen kann, wie z. B. dass jeder Vektorraum

eine Basis besitzt[6]. Ein Nachteil ist, dass viele unnatürlich scheinende Sätze gelten, wie etwa das Banach-Tarski-Paradoxon. Dieses Paradoxon besagt anschaulich gesprochen, dass es möglich ist, eine Kugel so in endlich viele Stücke zu zerlegen, dass man die Stücke zu zwei Kugeln gleicher Größe wie die Ausgangskugel wieder zusammensetzen kann. Nichtsdestotrotz werden wir auf das Auswahlaxiom nicht verzichten.

Axiom 8 (Auswahlaxiom): *Das kartesische Produkt einer nichtleeren Familie von nichtleeren Mengen ist nichtleer* [7].

2.3 Operationen auf Mengen

Wir haben im letzten Abschnitt eine Reihe von Axiomen kennengelernt, auf der wir unsere Mengenlehre aufbauen. Wir kümmern uns nun darum, was wir mit diesen Axiomen anfangen können.

Wir konstruieren zunächst die *Vereinigungsmenge* zweier Mengen M und N. Diese soll aus den Elementen von M und N bestehen. Wir bilden daher zunächst mit Hilfe des Paarmengenaxioms die Menge $\{M, N\}$. Nun können wir mit dem Vereinigungsmengenaxiom die Menge bilden, welche aus den Elementen der Elemente von $\{M, N\}$ besteht, was genau die gesuchte Vereingungsmenge ist. Diese Menge wird mit $M \cup N$ bezeichnet.

Weiter kann man die Elemente von M und N suchen, welche in beiden Mengen vorhanden sind. Diese Elemente bilden die *Schnittmenge* von M und N. Man erhält sie leicht aus dem Aussonderungsaxiom über $M \cap N := \{\, x \in M \mid x \in N \,\}$. Zwei Mengen heißen *disjunkt*, falls gilt $M \cap N = \emptyset$.

Die letzte fundamentale Operation ist die Bildung der *Restmenge*. Hier suchen wir die Elemente, die in M aber nicht in N enthalten sind. Dies ist analog $M \setminus N := \{\, x \in M \mid x \notin N \,\}$. Ist $N \subseteq M$, so nennt man $M \setminus N$ auch das *Komplement* von N in M und schreibt dafür $\complement_M N$, oder wenn die Obermenge M klar ist auch kurz $\complement N$.

Betrachten wir nun ein Beispiel. Es sei $M := \{1, 2, 3, 4\}$, $N := \{3, 4, 5\}$. Dann ist $M \cup N = \{1, 2, 3, 4, 5\}$, $M \cap N = \{3, 4\}$ und $M \setminus N = \{1, 2\}$.

Wir können nun ohne große Anstrengung aus den Gesetzen der Logik Rechenregeln für die Mengenoperationen ableiten. Wir halten dies fest in dem folgenden

Satz 4: *Für die Vereinigung und den Schnitt von Mengen M, N und O gelten die folgenden Regeln:*

(i) Kommutativgesetz:

$$M \cup N = N \cup M, \qquad M \cap N = N \cap M$$

(ii) Assoziativgesetz:

$$(M \cup N) \cup O = M \cup (N \cup O), \qquad (M \cap N) \cap O = M \cap (N \cap O)$$

[6] Dieser Satz wird erst dann spektakulär, wenn man Vektorräume mit überabzählbarer Basis betrachtet.

[7] Das kartesische Produkt wird in Abschnitt 2.3, Familien von Mengen in Abschnitt 3.4 eingeführt. Woher der Name Auswahlaxiom kommt, wird in Anhang A beleuchtet.

(iii) Distributivgesetz:

$$M \cup (N \cap O) = (M \cup N) \cap (M \cup O), \qquad M \cap (N \cup O) = (M \cap N) \cup (M \cap O)$$

(iv) Idempotenzgesetz:

$$M \cup M = M, \qquad M \cap M = M$$

(v) Absorptionsgesetz:

$$M \cup (M \cap N) = M, \qquad M \cap (M \cup N) = M$$

(vi) de Morgan-Gesetz:

$$\complement\,(M \cup N) = \complement\,M \cap \complement\,N, \qquad \complement\,(M \cap N) = \complement\,M \cup \complement\,N.$$

BEWEIS: Da die Beweise sehr technischer Natur sind und kaum neue Einsichten bringen, beschränken wir uns auf den Beweis des ersten Distributivgesetzes und des ersten de Morgan-Gesetzes. Wir zeigen also zunächst $M \cup (N \cap O) = (M \cup N) \cap (M \cup O)$.

Sei dazu $x \in M \cup (N \cap O)$. Dann gilt $x \in M$ oder $x \in N \cap O$. Im ersten Fall folgt aus $x \in M$ direkt $x \in M \cup N$ und $x \in M \cup O$, also auch $x \in (M \cup N) \cap (M \cup O)$. Im zweiten Fall ist $x \in N$ und $x \in O$, also zunächst $x \in M \cup N$ und $x \in M \cup O$ und dann erneut $x \in (M \cup N) \cap (M \cup O)$. Damit folgt „$\subseteq$“.

Nun zeigen wir „$\supseteq$“. Sei also $x \in (M \cup N) \cap (M \cup O)$. Dann gilt $x \in M \cup N$ und $x \in M \cup O$. Daraus folgt $x \in M$ oder $x \in N$ und $x \in O$. Also gilt $x \in M \cup (N \cap O)$.

Jetzt beweisen wir $\complement\,(M \cup N) = \complement\,M \cap \complement\,N$.

„$\subseteq$“: Wegen $x \in \complement\,(M \cup N)$ gilt $x \notin M \cup N$, also $x \notin M$ und $x \notin N$. Damit ist $x \in \complement\,M$ und $x \in \complement\,N$, woraus $x \in \complement\,M \cap \complement\,N$ folgt.

„$\supseteq$“: Sei nun $x \in \complement\,M \cap \complement\,N$. Dann gilt $x \in \complement\,M$ und $x \in \complement\,N$, also $x \notin M$ und $x \notin N$. Daraus ergibt sich $x \notin M \cup N$ und schließlich $x \in \complement\,(M \cup N)$. □

Nützlich sind weiter die folgenden Formeln für Restmengen:

Satz 5: *Für die Verknüpfung der Mengen M, N und O gilt*

$$(M \cap N) \setminus O = (M \setminus O) \cap (N \setminus O), \qquad (M \cup N) \setminus O = (M \setminus O) \cup (N \setminus O),$$

$$(M \setminus N) \setminus O = M \setminus (N \cup O), \qquad M \setminus (N \setminus O) = (M \setminus N) \cup (M \cap O),$$

$$M \subseteq N \Leftrightarrow \complement\,N \subseteq \complement\,M$$

$$\complement\,(\complement\,M) = M.$$

BEWEIS: Wir beweisen nur die erste Formel und lassen den Rest als Übungsaufgabe für den Leser.

„$\subseteq$“: Sei also $x \in (M \cap N) \setminus O$. Dann ist $x \in M \cap N$ und $x \notin O \cap (M \cap N)$. Also ist insbesondere $x \in M$ und $x \in N$. Da aber auch $x \notin O \cap M$ und $x \notin O \cap N$ folgt $x \in M \setminus O$ und $x \in N \setminus O$, also $x \in (M \setminus O) \cap (N \setminus O)$.

„$\supseteq$“: Sei nun $x \in (M \setminus O) \cap (N \setminus O)$. Dann gilt $x \in M \setminus O$ und $x \in N \setminus O$. Daraus folgt $x \in M$ und $x \in N$, also $x \in M \cap N$ sowie $x \notin M \cap O$ und $x \notin N \cap O$, was auf $x \notin O \cap (M \cap N)$ führt. Damit ergibt sich $x \in (M \cap N) \setminus O$. □

Die Aufzählung der Elemente einer Menge spielt bekanntlich keine Rolle. So ist etwa $\{x, y\} = \{y, x\}$. Häufig ist aber die Reihenfolge der Elemente von entscheidender Bedeutung. Wir müssen daher eine neue Konstruktion einführen, welche es uns gestattet, die Reihenfolge der Elemente zu unterscheiden. Wir können nach dem Paarmengenaxiom aus der Menge x die Menge $\{x\}$ und zusammen mit der Menge y die Menge $\{x, y\}$ konstruieren. Erneute Anwendung des Paarmengenaxioms ergibt die Menge $\{\{x\}, \{x, y\}\}$. Wir definieren daher das *geordnete Paar* als

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

Man sieht dann leicht $(x, y) \neq (y, x)$ falls $x \neq y$. Weiter definieren wir für drei Elemente das *Tripel*

$$(x, y, z) := ((x, y), z).$$

Wir vereinbaren jedoch, zwischen den Ausdrücken $((x, y), z)$ und $(x, (y, z))$ nicht zu unterscheiden und schreiben in beiden Fällen (x, y, z). Wie ein *n-Tupel*, bestehend aus n geordneten Elementen, zu definieren ist, liegt nun auf der Hand. Man nennt das j-te Element eines solchen Tupels auch die j-te *Komponente* des Tupels.

Nun können wir in Vorbereitung auf das nächte Kapitel das *kartesische Produkt* zweier Mengen M und N definieren. Darunter verstehen wir die Menge aller geordneten Paare von Elementen aus M und N

$$M \times N := \{\, (x, y) \in \mathcal{P}(\mathcal{P}(M \cup N)) \mid x \in M \wedge y \in N \,\}.$$

Das Produkt von drei Mengen ist dann entsprechend

$$M \times N \times O := (M \times N) \times O.$$

Auch hier machen wir keinen Unterschied zwischen $(M \times N) \times O$ und $M \times (N \times O)$, sondern schreiben immer $M \times N \times O$.

Übungsaufgaben

Aufgabe 1: Seien M und N Mengen. Zeige:

a) $M = (M \setminus N) \cup (M \cap N)$

b) $M \cup N = (M \setminus N) \cup N$,

und diese Vereinigungen sind disjunkt.

Aufgabe 2: Zeige:

a) $\{x, y\} = \{x, z\} \Rightarrow y = z$

b) $(x, y) = (a, b) \Leftrightarrow x = a \wedge y = b$.

Aufgabe 3: Seien M, N, O und P Mengen. Zeige:

a) $M \cap (N \setminus O) = (M \cap N) \setminus (M \cap O)$

b) $(M \times O) \cup (N \times P) \subseteq (M \cup N) \times (O \cup P)$.

Gilt statt der zweiten Inklusion auch Gleichheit?

Aufgabe 4: Seien M und N Mengen. Gibt es zu jeder Teilmenge $O \subseteq M \times N$ Teilmengen $P \subseteq M$ und $Q \subseteq N$ mit $O = P \times Q$?

3 Abbildungen

3.1 Relationen

Bevor wir in diesem Kapitel den in der Mathematik absolut fundamentalen Begriff der Abbildung einführen, müssen wir uns mit der Vorstufe der Abbildung beschäftigen, nämlich der Relation.

Definition 1 (Relation): *Seien M und N Mengen. Jede Teilmenge $R \subseteq M \times N$ heißt* Relation *zwischen M und N. Für $(x, y) \in R$ schreibt man auch xRy.*

Wir werden uns nicht lange mit dieser allgemeinen Definition aufhalten und gleich zwei wichtige Spezialfälle betrachten.

Definition 2 (Ordnungsrelation): *Eine Relation $R \subseteq M \times M$ heißt* Ordnungsrelation*, wenn für alle $x, y, z \in M$ gilt*

(i) Reflexivität:

$$xRx$$

(ii) Antisymmetrie:

$$xRy \wedge yRx \Rightarrow x = y$$

(iii) Transitivität:

$$xRy \wedge yRz \Rightarrow xRz.$$

Man sagt dann auch, dass R auf M eine Ordnung *definiert. Eine Ordnung heißt* total*, wenn für alle $x, y \in M$ gilt xRy oder yRx.*

Ist eine Ordnung total, so bedeutet dies, dass man zwei Elemente der Menge stets miteinander vergleichen kann. Ein einfaches Beispiel für eine Ordnungsrelation wäre die kleiner-gleich-Beziehung auf der Menge der reellen Zahlen. Diese Ordnung nennt man auch kanonische[1] Ordnungsrelation auf $\mathbb{R}$, um sie von möglichen weiteren Ordnungsrelationen auf $\mathbb{R}$ zu unterscheiden. Diese Ordnung ist sogar total. Man beachte, dass die kleiner-Beziehung keine Ordnungsrelation definiert, da die Reflexivität verletzt ist!

Ein weiteres Beispiel für eine Ordnungsrelation wäre $\mathcal{P}(M)$ mit $xRy :\Leftrightarrow x \subseteq y$, wobei M eine beliebige Menge ist und $x, y \in \mathcal{P}(M)$.

[1] Der Begriff „kanonisch“ wird in der Mathematik im Sinne von „natürlich“ verwendet, womit gemeint ist, dass es zwar mehrere Objekte von der gleichen Sorte gibt, eines aber in gewisser Weise vor allen anderen ausgezeichnet ist.

Hat man eine Ordnungsrelation R vorliegen, so schreibt man statt R auch gerne $\leq$. Man definiert dann $x < y :\Leftrightarrow x \leq y \wedge x \neq y$. Weiter setzt man $y \geq x :\Leftrightarrow x \leq y$ und $y > x :\Leftrightarrow x < y$.

Eine strikte Ungleichung wird nur selten benötigt. Wir verwenden daher meistens $\leq$, denn man kann damit genauso gut abschätzen und braucht keine Spezialfälle zu betrachten, in denen aus der strikten Ungleichung vielleicht doch eine Gleichung werden könnte. Wenn in den Formeln also ein striktes $<$ auftaucht, so nur dann, wenn es absolut notwendig ist.

Definition 3: *Sei M eine geordnete Menge und $N \subseteq M$ eine Teilmenge. Ein Element $x \in N$ heißt*

(i) Maximum *(bzw.* Minimum*) von N, wenn für alle $y \in N$ gilt $y \leq x$ (bzw. $y \geq x$).*

(ii) maximales *(bzw.* minimales*)* Element *von N, wenn für alle $y \in N$ aus $x \leq y$ (bzw. $x \geq y$) folgt $x = y$.*

Es heißt $x \in M$ obere *(bzw.* untere*)* Schranke *von N, wenn für alle $y \in N$ gilt $y \leq x$ (bzw. $y \geq x$). Die Menge N heißt* nach oben *(bzw.* unten*)* beschränkt*, wenn es eine obere (bzw. untere) Schranke gibt. Sie heißt* beschränkt*, wenn sie nach oben und nach unten beschränkt ist.*

Eine obere (bzw. untere) Schranke x heißt Supremum *(bzw.* Infimum*), wenn für jede weitere obere (bzw. untere) Schranke y gilt $y \geq x$ (bzw. $y \leq x$).*

Das Supremum (bzw. Infimum) ist, wenn es existiert, die kleinste (bzw. größte) obere (bzw. untere) Schranke.

Das Maximum (bzw. Minimum) einer Menge ist, wenn es existiert, eindeutig bestimmt. Denn sind $x, y \in N$ zwei Maxima, so gilt $x \leq y$ und $y \leq x$. Aus der Antisymmetrie von $\leq$ folgt dann $x = y$.

Den Unterschied zwischen Maxima und maximalen Elementen sieht man nur dann, wenn die Ordnung nicht total ist. Die Definition des Maximums erfordert nämlich, dass sich alle $y \in N$ mit x vergleichen lassen. Beim maximalen Element ist nur gefordert, dass es keine $y \in N$ gibt mit $x < y$.

Wir betrachten die Menge $M := \{2, 3, \ldots, 10\}$ und definieren für $x, y \in M$ die Relation $x \leq y$, wenn x die Zahl y teilt, d. h. wenn es eine ganze Zahl z gibt mit $y = xz$. Man rechnet leicht nach, dass $\leq$ in der Tat eine Ordnugnsrelation ist.

Diese Ordnung ist aber nicht total, z. B. sind 3 und 4 nicht vergleichbar. Die Menge M hat offenbar kein Maximum, da keine Zahl durch alle anderen teilbar ist. Dagegen gibt es maximale Elemente, und zwar genau die Primzahlen in M.

Wir führen die Bezeichungen $\max N$ für das Maximum, $\min N$ für das Minimum, $\sup N$ für das Supremum und $\inf N$ für das Infimum der Menge N ein.

Satz 6 (Approximationseigenschaft): *Sei M eine total geordnete Menge, $N \subseteq M$ eine Teilmenge und $x \in M$. Dann ist $x = \sup N$ genau dann, wenn x obere Schranke ist, und wenn es für alle $y \in M$ mit $y < x$ ein $z \in N$ gibt mit $z > y$.*

BEWEIS: Die Kontraposition der Aussage „ist y obere Schranke, so gilt $y \geq x$“ lautet „ist $y < x$, so ist y keine obere Schranke“. Und y ist genau dann keine obere Schranke, wenn es ein $z \in N$ gibt mit $z > y$. □

Die Approximationseigenschaft ist nur eine Umformulierung der Definition des Supremums, aber sie wird in der Analysis viel benutzt. Wie lautet die analoge Charakterisierung des Infimums?

Definition 4 (Äquivalenzrelation): *Eine Relation $R \subseteq M \times M$ heißt* Äquivalenzrelation, *wenn für alle $x, y, z \in M$ gilt*

(i) Reflexivität:

$$xRx$$

(ii) Symmetrie:

$$xRy \Rightarrow yRx$$

(iii) Transitivität:

$$xRy \wedge yRz \Rightarrow xRz.$$

Für $x \in M$ heißt $[x] := \{\, y \in M \mid yRx \,\}$ die Äquivalenzklasse *von x. Man nennt x den* Repräsentanten *der Äquivalenzklasse $[x]$. Die Menge aller Äquivalenzklassen $\{\, [x] \in \mathcal{P}(M) \mid x \in M \,\}$ wird mit M/R bezeichnet.*

Ein bekanntes Beispiel für eine Äquivalenzrelation wären wieder die reellen Zahlen mit $xRy :\Leftrightarrow x = y$. Die Äquivalenzklassen wären in dem Fall einfach $[x] = \{x\}$.

Ein weiteres Beispiel mit enormer Bedeutung für die elementare Zahlentheorie bilden die sog. *Restklassen*[2] . Hier betrachtet man für ein $n \in \mathbb{N} \setminus \{0\}$ auf $\mathbb{Z}$ die Relation

$$xRy :\Leftrightarrow \underset{k\in\mathbb{Z}}{\exists} : x - y = kn. \tag{3.1}$$

Die Äquivalenzklassen[3] sind dann genau die Zahlen, die nach Division durch n denselben Rest ergeben. Zum Beispiel gibt es für $n = 3$ die Restklassen

$$\begin{aligned}
[0] &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\
[1] &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\
[2] &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}.
\end{aligned}$$

Man beachte, dass bspw. $[2] = [5]$, denn 2 und 5 bilden nach Division durch 3 denselben Rest. Somit sind in unserem Beispiel 2 und 5 Repräsentanten derselben Äquivalenzklasse. Man muss daher, wenn man Operationen auf Äquivalenzklassen einführt, aufpassen, dass diese Repräsentanten-unabhängig sind. Wir werden später darauf zurückkommen.

Wir können an diesem Beispiel noch zwei weitere Dinge sehen. Erstens stellt man fest, dass durch die Vereingung aller Restklassen wieder die Ausgangsmenge entsteht, also dass $[0] \cup [1] \cup [2] = \mathbb{Z}$. Zweitens bilden die Äquivalenzklassen eine disjunkte Zerlegung der Menge $\mathbb{Z}$. Wir halten dies nun allgemein fest in dem

[2] Eine Einführung findet der interessierte Leser im Artikel über Zahlentheorie.
[3] Für die Menge der Restklassen hat sich die Bezeichnung $\mathbb{Z}/n\mathbb{Z}$ eingebürgert.

Satz 7: *Sei M eine Menge und R eine Äquivalenzrelation auf M. Dann gilt:*

(i) $[x] = [y] \Leftrightarrow xRy$

(ii) $M = \bigcup_{x \in M} [x]$

(iii) $[x] \cap [y] \neq \emptyset \Rightarrow [x] = [y]$.

BEWEIS:

(i) „$\Rightarrow$“: Sei $[x] = [y]$. Dann folgt aus xRx direkt $x \in [x] = [y]$, also xRy.
„$\Leftarrow$“: Es gelte nun xRy. Sei $z \in [x]$. Wegen zRx und xRy folgt zRy, also $z \in [y]$. Daraus folgt $[x] \subseteq [y]$. Analog erhält man $[y] \subseteq [x]$, also insgesamt $[x] = [y]$.

(ii) Wegen xRx gilt $x \in [x]$ für alle $x \in M$. Daher muss $\{x\} \subseteq [x]$ gelten. Wir erhalten damit die Inklusionskette

$$M = \bigcup_{x \in M} \{x\} \subseteq \bigcup_{x \in M} [x] \subseteq M,$$

woraus sofort die Gleichheit folgt. [4]

(iii) Sei $[x] \cap [y] \neq \emptyset$, d. h. es gibt ein $z \in [x] \cap [y]$. Daraus ergibt sich $z \in [x]$ und $z \in [y]$. Also gilt zRy und mit zRx auch xRz, woraus xRy, also $[x] = [y]$, folgt. □

Eine Zerlegung einer Menge mit den oben genannten Eigenschaften heißt eine Partition dieser Menge.

Definition 5 (Partition): *Eine Teilmenge $P \subseteq \mathcal{P}(M)$ heißt* Partition *von M, wenn für alle $N, O \in P$ gilt*

(i) $M = \bigcup_{N \in P} N$

(ii) $N \cap O \neq \emptyset \Rightarrow N = O$.

Obiger Satz zeigt, dass die Äquivalenzklassen einer Äquivalenzrelation auf einer Menge M eine Partition von M bilden. Umgekehrt liefert jede Partition P von M eine Äquivalenzrelation, wenn man zwei Elemente $x, y \in M$ für äquivalent erklärt, wenn sie in derselben Menge $N \in P$ liegen. Die Äquivalenzklassen sind dann gerade die Elemente von P.

[4] Die Bedeutung der Schreibweise $\bigcup_{x \in M} [x]$ bzw. $\bigcup_{x \in M} \{x\}$ sollte intuitiv klar sein; sie wird in Abschnitt 3.4 streng begründet.

3.2 Abbildungen

Durch Relationen werden Verbindungen zwischen Elementen verschiedener Mengen hergestellt. Von besonderer Bedeutung sind solche Relationen, bei denen einem Element einer Menge genau ein Element einer anderen Menge zugeordnet wird.

Definition 6 (Abbildung): *Seien M und N Mengen und R eine Relation zwischen M und N. Gibt es zu jedem $x \in M$ genau ein $y \in N$ mit xRy, so nennt man das Tripel $f := (M, N, R)$* Abbildung *von M nach N. Man nennt R den* Graphen *von f und schreibt $\mathrm{Gr} f := R$. Die Menge M heißt* Definitionsmenge*, die Menge N* Zielmenge*. Das $y \in N$ zu $x \in M$ mit xRy wird mit $f(x)$ bezeichnet*[5]*.Man schreibt dann*

$$f\colon M \longrightarrow N\colon x \longmapsto f(x).$$

oder übersichtlicher

$$\begin{array}{rccc} f: & M & \longrightarrow & N \\ & \cup & & \cup \\ & x & \longmapsto & f(x) \end{array}.$$

Man nennt $f(x)$ das Bild *des* Urbildes *x unter der Abbildung f. Ebenso definiert man für eine beliebige Teilmenge $O \subseteq M$ das Bild der Menge O unter f als*

$$f(O) := \{\, f(x) \mid x \in O \,\}.$$

Für eine Teilmenge $P \subseteq N$ nennt man die Menge

$$f^{-1}(P) := \{\, x \in M \mid f(x) \in P \,\}$$

das Urbild von P. Ist $P = \{y\}$ mit $y \in N$, so heißt die Menge

$$f^{-1}(y) := f^{-1}(\{y\})$$

Faser *über y.*

Zwei Abbildungen sind gemäß der Definition gleich, wenn Definitionsmenge, Zielmenge und Graph gleich sind, denn die Gleichheit der Abbildungen entspricht der Gleichheit der Tripel. Man beachte also, dass die Zuordnungsvorschift die Abbildung nicht eindeutig bestimmt!

Wir betrachten als Beispiel die Abbildung

$$f\colon \mathbb{Z} \longrightarrow \mathbb{Z}\colon x \longmapsto x^2.$$

Diese Abbildung ordnet jeder ganzen Zahl ihr Quadrat zu. Wie man an diesem Beispiel sieht, braucht nicht jedes Element der Zielmenge ein Urbild zu haben, denn es gibt kein $x \in \mathbb{Z}$ mit $f(x) = -1$. Ebenso kann ein Bild durchaus mehrere Urbilder haben, wie man an $(-1)^2 = 1^2 = 1$ sieht. Da diese beiden Eigenschaften aber durchaus wichtig sind, trifft man folgende

[5] Manchmal lässt man die Klammern auch weg und schreibt einfach fx.

Definition 7: *Seien M, N Mengen und $f\colon M \longrightarrow N$ eine Abbildung. Dann heißt f*

(i) surjektiv*, wenn es für jedes $y \in N$ ein $x \in M$ gibt mit $y = f(x)$*

(ii) injektiv*, wenn aus $x \neq y$ folgt $f(x) \neq f(y)$*

(iii) bijektiv*, wenn f surjektiv und injektiv ist.*

Die Abbildung f nennt man dann auch entsprechend Surjektion*,* Injektion *oder* Bijektion*.*

Für $f\colon M \to N$ heißt $f(M)$ auch *Wertemenge* von f. Die Abbildung f ist damit offenbar genau dann surjektiv, wenn $f(M) = N$ gilt, wenn also die Wertemenge gleich der Zielmenge ist. Zum Beweis der Injektivität wird in der Regel die Kontraposition $f(x) = f(y) \Rightarrow x = y$ verwendet.

Wir besprechen nun einige Beispiele. Für eine Menge N kann man die *leere Abbildung* $(\emptyset, N, \emptyset)$ definieren. Wie sieht es mit ihrer Injektivität und Surjektivität aus?

Die Abbildung

$$\mathrm{id}_M\colon M \longrightarrow M\colon x \longmapsto x$$

heißt *identische Abbildung* oder *Identität* auf M und bildet jedes Element aus M auf sich selbst ab. Sie ist klarerweise eine Bijektion.

Beim kartesischen Produkt $M \times N$ definiert man die *Projektionen*

$$\mathrm{pr}_1\colon M \times N \longrightarrow M\colon (x, y) \longmapsto x$$

und

$$\mathrm{pr}_2\colon M \times N \longrightarrow N\colon (x, y) \longmapsto y.$$

Sie ordnen jedem Paar die erste bzw. zweite Komponente zu. Oft werden auch die Bezeichnungen pr_M bzw. pr_N gewählt.

Ist auf einer Menge M eine Äquivalenzrelation R definiert, so heißt die Abbildung

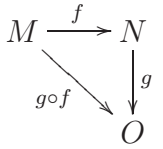
$$\pi\colon M \longrightarrow M/R\colon x \longmapsto [x]$$

kanonische Projektion oder *kanonische Surjektion*. Sie ordnet jedem Element aus M seine Äquivalenzklasse zu.

Man kann Abbildungen hintereinanderschalten (oder *verketten*). Sind etwa $f\colon M \to N$ und $g\colon N \to O$ zwei Abbildungen, so wird durch

$$g \circ f\colon M \longrightarrow O\colon x \longmapsto g(f(x))$$

das *Kompositum* von f und g definiert. Man verdeutlicht sich dies gern an einem *kommutativen Diagramm*[6]:



[6]Man hüte sich, ein solches Diagramm zu malen, falls es nicht kommutiert!

Es ist klar, dass i. A. $f \circ g \neq g \circ f$ gilt. Aus dem Diagramm geht sogar hervor, dass $f \circ g$ gar nicht zu existieren braucht, obwohl $g \circ f$ existiert. Die Komposition von Abbildungen ist also nicht kommutativ! Dafür gilt das Assoziativgesetz:

Satz 8: *Seien $f\colon M \to N$, $g\colon N \to O$ und $h\colon O \to P$ Abbildungen. Dann gilt $h \circ (g \circ f) = (h \circ g) \circ f$.*

BEWEIS: Für alle $x \in M$ gilt

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x). \qquad \square$$

Ist $M \subseteq N$ eine Teilmenge, so nennt man

$$i_M\colon M \longrightarrow N\colon x \longmapsto x$$

Inklusion oder *Einbettung* von M in N. Da sie offenbar injektiv ist, wird sie auch *kanonische Injektion* genannt. Hat man zusätzlich eine Abbildung $f\colon N \to O$, so heißt

$$f|_M := f \circ i_M$$

Einschränkung von f auf M.Entsprechend heißt für jede Menge $P \supseteq N$ eine Abbildung $g\colon P \to O$ *Fortsetzung* von f auf P, wenn $g|_N = f$ gilt.

Als letztes Beispiel führen wir die *Umkehrabbildung* oder *inverse Abbildung* ein. Diese ist nur dann definiert, wenn $f\colon M \to N$ bijektiv ist. Sie ordnet jedem $y \in N$ das eindeutig bestimmte Urbild $f^{-1}(y)$ unter f zu und wird mit f^{-1} bezeichnet:

$$f^{-1}\colon N \longrightarrow M\colon y \longmapsto f^{-1}(y).$$

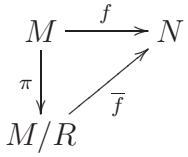
Offenbar ist $f \circ f^{-1} = \mathrm{id}_N$ und $f^{-1} \circ f = \mathrm{id}_M$. Die Umkehrabbildung ist daher nach Aufgabe 7 ebenfalls bijektiv.

Wir gehen nun noch etwas genauer auf das Zusammenspiel von Abbildungen und Äquivalenzrelationen ein. Wir beginnen mit der

Definition 8: *Seien M, N Mengen und R eine Äquivalenzrelation auf M. Eine Abbildung $f\colon M \to N$ heißt* verträglich *mit R, wenn für alle $x, y \in M$ mit xRy gilt $f(x) = f(y)$.*

Die Verträglichkeit der Abbildung f sagt also aus, dass Elemente der gleichen Äquivalenzklasse unter f dieselben Bilder haben. Für solche Abbildungen gilt der folgende

Satz 9: *Sei $f\colon M \to N$ eine mit der Äquivalenzrelation R auf M veträgliche Abbildung. Dann existiert eine eindeutig bestimmte Abbildung $\overline{f}\colon M/R \to N$, so dass*



kommutiert.

BEWEIS: Wir betrachten die durch $\overline{f}([x]) := f(x)$ gegebene Abbildung. Wir zeigen zunächst, dass sie wohldefiniert ist, d. h. dass ihr Wert unabhängig vom Repräsentanten x ist. Sei also $y \in [x]$, dann gilt xRy und wegen der Verträglichkeit von f auch $f(x) = f(y)$. Nun zeigen wir die Eindeutigkeit. Sei dazu $\overline{f}$ eine Abbilung mit der gewünschten Eigenschaft. Dann muss $f = \overline{f} \circ \pi$ gelten, also $f(x) = \overline{f}([x])$. Das ist aber genau unsere Definition von $\overline{f}$ gewesen. $\square$

3.3 Mächtigkeit von Mengen

Unter der *Mächtigkeit* oder *Kardinalität* einer endlichen Menge M versteht man die Anzahl der Elemente der Menge. Man schreibt $|M| = n$, $\#M = n$ oder auch $\operatorname{card} M = n$, wenn die Zahl der Elemente von M gleich n ist. So ist $|\{1, 2, 3\}| = 3$. Interessant wird der Mächtigkeitsbegriff aber erst, wenn man unendliche Mengen betrachtet. Doch wie kann man definieren, wann eine Menge unendlich ist?

Definition 9: *Eine Menge M heißt* unendlich*, wenn es eine Bijektion zwischen M und einer echten Teilmenge von M gibt.*

Wir betrachten als Beispiel den

Satz 10: *Die Menge der natürlichen Zahlen ist unendlich.*

BEWEIS: Als Beweis wählen wir die geraden Zahlen $\mathbb{G}$ als echte Teilmenge der natürlichen Zahlen und definieren eine Abbildung f durch

$$f\colon \mathbb{N} \longrightarrow \mathbb{G}\colon n \longmapsto 2n.$$

Man sieht leicht ein, dass f bijektiv ist. □

Klarerweise ist auch jede Obermenge einer unendlichen Menge unendlich.

Man nennt zwei endliche Mengen gleichmächtig, wenn sie die gleiche Anzahl von Elementen haben. Anders ausgedrückt können wir eine Bijektion zwischen den Elementen der einen und den Elementen der anderen Menge angeben. Dieses Prinzip lässt sich auch auf den Fall unendlicher Mengen übertragen.

Definition 10: *Zwei Mengen heißen* gleichmächtig*, wenn es eine Bijektion zwischen ihren Elementen gibt.*

Wir werden nun zeigen, dass die Potenzmenge einer Menge M echt größer als M selbst ist. Im Falle endlicher Mengen werden wir dies in Satz 104 erneut sehen, wenn wir die Mächtigkeit einer Menge aus n Elementen konkret berechnen können. Wir beweisen nun jedoch ein viel allgemeineres Resultat, das insbesondere für unendliche Mengen gilt:

Satz 11: *Es gibt keine Surjektion zwischen M und $\mathcal{P}(M)$.*

BEWEIS: Wir führen den Beweis durch Widerspruch, nehmen also an, eine solche Surjektion existiere. Dann ordnen wir jedem $x \in M$ eine Menge $N \in \mathcal{P}(M)$ so zu, dass die Zuordnung surjektiv ist. Es kann x in N enthalten sein oder auch nicht. Nun betrachten wir die Menge Ω aller $x \in M$, für die gilt: x ist nicht Element der ihm zugeordneten Menge N. Ω besteht aus Elementen von M, ist also eine Teilmenge von M und daher ein Element von $\mathcal{P}(M)$. Da die Zuordnung surjektiv ist, gibt es ein Element $o \in M$, dem Ω zugeordnet ist. Ist nun o ein Element von Ω? Falls ja, dann widerspricht das der Definition von Ω. Falls nein, so muss o laut Definition von Ω ein Element von Ω sein. So oder so ergibt sich ein Widerspruch. □

Es stellt sich nun natürlich die Frage, in welchem Sinne bspw. $\mathcal{P}(\mathbb{N})$ größer ist als $\mathbb{N}$. Kann man dies irgendwie anschaulich einsehen? Wir gehen dieser Frage auf den Grund, indem wir mehrere Abstufungen für unendliche Mengen einführen.

Definition 11: *Eine Menge heißt* abzählbar*, wenn sie gleichmächtig zu einer Teilmenge von* $\mathbb{N}$ *ist. Ansonsten heißt sie* überabzählbar*.*

Offensichtlich ist jede endliche Menge abzählbar. Die unendlichen Mengen, welche abzählbar sind, sind in gewissem Sinne die kleinsten unendlichen Mengen. Wie der Begriff schon andeutet bedeutet dies, dass man alle Elemente einer solchen Menge in einer (unendlichen) Liste aufschreiben kann. Wie wir bald sehen trifft dies verblüffenderweise noch lange nicht auf jede unendliche Menge zu. Für unser weiteres Vorgehen benutzen wir die Tatsache, dass das Kompositum bijektiver Abbildungen bijektiv ist (siehe Aufgabe 8). Wir schreiben nun $M \sim N$, falls M und N gleichmächtig sind. Aus den Eigenschaften bijektiver Abbildungen folgt dann sofort, dass durch $\sim$ eine Äquivalenzrelation definiert ist (auf der Menge, die alle betrachteten Mengen enthält).

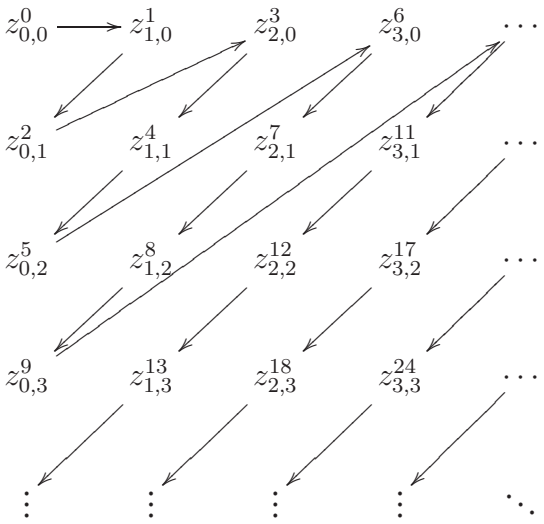
Satz 12: *Eine abzählbare Vereinigung abzählbarer Mengen und das kartesische Produkt zweier abzählbarer Mengen ist wieder abzählbar.*

BEWEIS: Da der Fall endlicher Mengen trivial ist, betrachten wir nur unendliche Mengen. Wir zeigen zunächst, dass die Vereinigung zweier abzählbarer Mengen M und N wieder abzählbar ist. Wir können ohne Einschränkung (o. E.) als Teilmenge von $\mathbb{N}$ die Menge $\mathbb{N}$ selbst nehmen. Dann gilt nach Voraussetzung $M \sim \mathbb{N}$ und $N \sim \mathbb{N}$. Da aber $\mathbb{N}$ auch gleichmächtig zu der Menge der geraden Zahlen $\mathbb{G}$ und der Menge der ungeraden Zahlen $\mathbb{U}$ ist, also $\mathbb{N} \sim \mathbb{G}$ und $\mathbb{N} \sim \mathbb{U}$ gilt, folgt nach obiger Bemerkung $M \sim \mathbb{G}$ und $N \sim \mathbb{U}$. Mit $M \cup N \sim \mathbb{G} \cup \mathbb{U} = \mathbb{N}$ folgt die Behauptung. Aus wiederholter Anwendung dieser Überlegung ergibt sich sofort, dass eine endliche Vereinigung abzählbarer Mengen abzählbar ist. Für eine unendliche abzählbare Vereinigung gehen wir wieder o. E. davon aus, dass alle Mengen unendlich sind und bezeichnen mit $z_{i,j}$ das $(i+1)$-te Element der $(j+1)$-ten Menge. Nun betrachten wir die Abbildung

$$f\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}\colon (i,j) \longmapsto \frac{(i+j)(i+j+1)}{2} + j.$$

Diese gibt an, wie man alle Elemente der Vereinigung durchzählen kann. Wir werden in Satz 96 sehen, dass diese Abbildung in der Tat eine Bijektion von $\mathbb{N} \times \mathbb{N}$ nach $\mathbb{N}$ ist. Fol-

gendes Schaubild soll dies verdeutlichen:



Dabei bedeutet der hochgestellte Index die durch f zugewiesene Stelle in der Vereinigung. Damit haben wir gleichzeitig bewiesen, dass das kartesische Produkt zweier abzählbarer Mengen abzählbar ist. Dazu braucht man nämlich nur die Paare (x_i, y_j) mit z_{ij} zu identifizieren. □

Damit ist natürlich die Menge der ganzen Zahlen $\mathbb{Z}$ abzählbar (als Vereinigung der Menge der natürlichen Zahlen einmal mit positivem und einmal mit negativem Vorzeichen). Da man jede rationale Zahl aus $\mathbb{Q}$ durch Zähler und Nenner darstellen kann, welche beide in $\mathbb{Z}$ liegen, gilt der

Satz 13: *Die Menge der rationalen Zahlen ist abzählbar.*

Andererseits wissen wir aber auch schon, dass $\mathcal{P}(\mathbb{N})$ überabzählbar ist. Es gibt aber auch noch eine allseits bekannte Menge, welche überabzählbar ist.

Satz 14: *Die Menge der reellen Zahlen ist überabzählbar.*

BEWEIS: Es reicht zu zeigen, dass die reellen Zahlen im Intervall $[0;1]$ überabzählbar sind. Angenommen, die reellen Zahlen in diesem Intervall wären abzählbar unendlich. Dann müsste folgende Liste alle enthalten:

$$\begin{aligned} r_1 &= 0{,}x_{1,1}x_{1,2}x_{1,3}x_{1,4}x_{1,5}\ldots \\ r_2 &= 0{,}x_{2,1}x_{2,2}x_{2,3}x_{2,4}x_{2,5}\ldots \\ r_3 &= 0{,}x_{3,1}x_{3,2}x_{3,3}x_{3,4}x_{3,5}\ldots \\ r_4 &= 0{,}x_{4,1}x_{4,2}x_{4,3}x_{4,4}x_{4,5}\ldots \\ \vdots &= \qquad\qquad \vdots \end{aligned}$$

Dabei stehen die Ziffern $x_{i,j}$ entweder für 0 oder 1; die Darstellung erfolgt also im Dualsystem. Es lässt sich aber nun folgendermaßen eine Zahl konstruieren, die in der Liste nicht vorkommt: Wir definieren die Abbildung

$$f\colon \{0,1\} \longrightarrow \{0,1\}\colon x \longmapsto \begin{cases} 1 & \text{falls } x = 0 \\ 0 & \text{falls } x = 1 \end{cases}$$

und stellen fest, dass die Zahl $0.y_1y_2y_3\ldots$, welche durch $y_n := f(x_{n,n})$ gegeben ist, mit r_1 in der 1. Nachkommastelle nicht übereinstimmt, mit r_2 nicht in der 2., und mit r_n nicht in der n-ten. Damit ist sie in der Liste nicht enthalten. Widerspruch! □

Die Menge der reellen Zahlen hat also eine größere Mächtigkeit als die Menge der natürlichen Zahlen. Man bezeichnet die Mächtigkeit der Menge der natürlichen Zahlen mit $\aleph_0$[7]. Die kleinste Mächtigkeit, welche echt größer als $\aleph_0$ ist, ist $\aleph_1$. Die *Kontinuumshypothese* besagt, dass zwischen der Mächtigkeit der reellen Zahlen und der der natürlichen Zahlen keine weitere Mächtigkeit liegt. Dann hätte die Menge der reellen Zahlen die Mächtigkeit $\aleph_1$. Es hat sich gezeigt, dass die Kontinuumshypothese unabhängig von den Axiomen der Mengenlehre ist, d. h. sie ist weder beweisbar noch widerlegbar und kann somit zu den Axiomen hinzugenommen werden oder auch nicht. Die *verallgemeinerte Kontinuumshyothese* besagt, dass es zwischen der Mächtigkeit einer unendlichen Menge und ihrer Potenzmenge keine weitere Mächtigkeit gibt. Damit wäre ebenfalls $\operatorname{card}\mathcal{P}(\mathbb{N}) = \aleph_1$. Die verallgemeinerte Kontinuumshypothese ist ebenfalls unentscheidbar.

3.4 Familien von Mengen

Wir haben im letzten Abschnitt die Elemente einer Menge durchnummeriert und sie zur Kennzeichnung mit einem Index versehen. Den mathematischen Hintergrund für dieses Vorgehen bildet die folgende

Definition 12 (Familie): *Seien I und M Mengen. Eine Abbildung $I \to M : i \mapsto x_i$ heißt durch I indizierte* Familie *von Elementen aus M, geschrieben als $(x_i)_{i\in I}$. Die Menge I heißt in diesem Zusammenhang auch* Indexmenge. *Die Menge aller durch I indizierten Familien von Elementen aus M, also die Menge aller Abbildungen von I nach M, wird mit M^I bezeichnet.*

In der Regel wird die Indexmenge die Menge der natürlichen Zahlen sein oder eine Teilmenge. Es sei jedoch betont, dass eine Indexmenge keineswegs abzählbar sein muss. Die Behauptung, man könne die reellen Zahlen nicht indizieren, ist also falsch. Es gibt lediglich keine abzählbare Indexmenge, die dies leisten könnte.

Die Vereinigung bzw. der Schnitt aller Bilder unter $i \mapsto x_i$ wird als

$$\bigcup_{i\in I} x_i \qquad \text{bzw.} \qquad \bigcap_{i\in I} x_i$$

geschrieben. Es gilt dann

$$x \in \bigcup_{i\in I} x_i \Leftrightarrow \bigvee_{i\in I} : x \in x_i \qquad \text{und} \qquad x \in \bigcap_{i\in I} x_i \Leftrightarrow \bigwedge_{i\in I} : x \in x_i.$$

Die Schreibweise in Satz 7 ist also durch die kanonische Projektion zu Stande gekommen. Ferner können wir das kartesische Produkt von Mengen verallgemeinern. Es ist

$$\prod_{i\in I} x_i$$

[7] Aleph, erster Buchstabe des hebräischen Alphabets

die Menge aller Familien $(y_i)_{i\in I}$ mit $y_i \in x_i$ für alle $i \in I$. Im Fall $x_i = x$ für alle $i \in I$ gilt

$$\prod_{i\in I} x_i = x^I.$$

Wir haben für geordnete Mengen N die Bezeichnungen $\max$, $\min$, $\sup$ und $\inf$ eingeführt. Indiziert J die Elemente von N, so ist klar, was

$$\max_{j\in J} x_j$$

und analog für $\min$, $\sup$ und $\inf$ bedeuten soll. Ist N von der Form $N = \{x_1, x_2, \ldots, x_n\}$, so schreiben wir auch

$$\max(x_1, x_2, \ldots, x_n) := \max\{x_1, x_2, \ldots, x_n\}$$

Diese Notation sagt natürlich nichts darüber aus, ob die so bezeichneten Objekte auch wirklich existieren!

Übungsaufgaben

Aufgabe 5: Zeige:

a) Für jede Menge M ist durch $xRy :\Leftrightarrow x \subseteq y$ auf $\mathcal{P}(M)$ eine Ordnungsrelation definiert. Ist diese Ordnung total?

b) Durch Gleichung 3.1 ist eine Äquivalenzrelation gegeben. Leite aus ihr formal die Äquivalenzklassen ab.

Aufgabe 6: Stelle das Ergebnis von Satz 8 mit Hilfe eines kommutativen Diagramms dar!

Aufgabe 7: Sei $f\colon M \to N$ eine Abbildung zwischen den Mengen M und N. Zeige:

a) f ist genau dann surjektiv, wenn es eine Abbildung $g\colon N \to M$ gibt mit $f \circ g = \mathrm{id}_N$.

b) f ist genau dann injektiv, wenn es eine Abbildung $g\colon N \to M$ gibt mit $g \circ f = \mathrm{id}_M$.

c) f ist genau dann bijektiv, wenn es eine Abbildung $g\colon N \to M$ gibt mit $f \circ g = \mathrm{id}_N$ und $g \circ f = \mathrm{id}_M$. Die Abbildung g ist eindeutig bestimmt.

Aufgabe 8: Seien $f\colon M \to N$ und $g\colon N \to O$ Abbildungen. Zeige:

a) Sind f und g injektiv, so ist auch $g \circ f$ injektiv.

b) Sind f und g surjektiv, so ist auch $g \circ f$ surjektiv.

c) Ist $g \circ f$ injektiv, so ist f injektiv.

d) Ist $g \circ f$ surjektiv, so ist g surjektiv.

Aufgabe 9: Seien M, N Mengen, $f\colon M \to N$ eine Abbildung und $O, P \subseteq M$ sowie $Q, R \subseteq N$ Teilmengen. Zeige:

$$O \subseteq P \Rightarrow f(O) \subseteq f(P), \quad Q \subseteq R \Rightarrow f^{-1}(Q) \subseteq f^{-1}(R), \quad \text{und} \quad f^{-1}\left(\complement Q\right) = \complement f^{-1}(Q).$$

Gib eine Abbilung f an, so dass weder $f\left(\complement O\right) \subseteq \complement f(O)$ noch $f\left(\complement O\right) \supseteq \complement f(O)$ gilt.

Aufgabe 10: Betrachte die Situation in Satz 9. Zeige:

a) Ist f surjektiv, so ist auch $\overline{f}$ surjektiv.

b) Durch $xRy :\Leftrightarrow f(x) = f(y)$ ist eine Äquivalenzrelation R gegeben. Für dieses R ist $\overline{f}$ injektiv.

Aufgabe 11: Es seien R_1 bzw. R_2 Äquivalenzrelationen auf M bzw. N. Eine Abbildung $f\colon M \to N$ heißt verträglich mit diesen Äquivalenzrelationen, wenn aus xR_1y folgt $f(x)R_2f(y)$. Zeige, dass es für jede verträgliche Abbildung eine eindeutig bestimmte Abbildung $\overline{f}$ gibt, so dass

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ M/R_1 & \xrightarrow{\overline{f}} & N/R_2 \end{array}$$

kommutiert.

Aufgabe 12: Seien M, N Mengen, I, J Indexmengen, $f\colon M \to N$ eine Abbildung und $(O_i)_{i\in I}$ sowie $(P_j)_{j\in J}$ Familien von Teilmengen $O_i \subseteq M$, $P_j \subseteq N$ für alle $i \in I, j \in J$. Zeige:

a) $f\left(\bigcup\limits_{i\in I} O_i\right) = \bigcup\limits_{i\in I} f(O_i)$

b) $f\left(\bigcap\limits_{i\in I} O_i\right) \subseteq \bigcap\limits_{i\in I} f(O_i)$

c) $f^{-1}\left(\bigcup\limits_{j\in J} P_j\right) = \bigcup\limits_{j\in J} f^{-1}(P_j)$

d) $f^{-1}\left(\bigcap\limits_{j\in J} P_j\right) = \bigcap\limits_{j\in J} f^{-1}(P_j)$

Zeige weiter, dass in b) Gleichheit gilt, wenn f injektiv ist.

4 Algebraische Strukturen

4.1 Halbgruppen und Monoide

Bisher haben wir uns über die Elemente der betrachteten Mengen kaum Gedanken gemacht. Dies wird sich nun ändern. Die einfachste Annahme, die man über diese Elemente machen kann, ist die Existenz einer Verknüpfung.

Definition 13 (Verknüpfung): *Seien M, N Mengen. Eine Abbildung*

(i) $+\colon M \times M \to M$ *heißt* innere Verknüpfung

(ii) $+\colon N \times M \to M$ *heißt* äußere Verknüpfung 1. Art

(iii) $+\colon M \times M \to N$ *heißt* äußere Verknüpfung 2. Art.

Man schreibt $x + y := +(x, y)$.

Da der Typ der Verknüpfung sich stets aus dem Zusammenhang ergibt, werden wir meist nur von Verknüpfungen oder *Operationen* sprechen. Die Elemente x und y heißen *Operanden*. Wir werden in nächster Zeit nur innere Verknüpfungen betrachten. Das Charakteristikum innerer Verknüpfungen ist, dass das Ergebnis der Verknüpfung wieder in der Ausgangsmenge liegt. Man sagt dann auch, dass die Menge unter dieser Verknüpfung *abgeschlossen* ist.

Ein Beispiel für eine Verknüpfung wäre die Differenzbildung $x-y$ auf der Menge der natürlichen Zahlen. Diese Verknüpfung ist jedoch nicht abgeschlossen, da die Differenz negativ ist, falls $x < y$ gilt. Betrachtet man dieselbe Verknüpfung auf der Menge der ganzen Zahlen, so ist sie abgeschlossen. Die Abgeschlossenheit unter Verknüpfungen wird eine wichtige Rolle bei der Erweiterung der Zahlbereiche in Kapitel 5 spielen.

Definition 14: *Eine Verknüpfung* $+\colon M \times M \to N$ *heißt*

(i) kommutativ, *wenn* $x + y = y + x$ *für alle* $x, y \in M$

(ii) assoziativ, *wenn* $x + (y + z) = (x + y) + z$ *für alle* $x, y, z \in M$

gilt. Im letzteren Fall kann man die Klammern auch weglassen.

Ein $e_l \in M$ *heißt* linksneutrales Element *bzgl. der Verknüpfung* $+$*, wenn für alle* $x \in M$ *gilt* $e_l + x = x$*. Analog ist* $e_r \in M$ rechtsneutral*, wenn stets* $x + e_r = x$ *gilt.*

Man bezeichnet $x'_l \in M$ *als ein zu* $x \in M$ linksinverses Element*, wenn* $x'_l + x = e_l$ *gilt. Entsprechend ist* $x'_r \in M$ *ein zu* $x \in M$ rechtsinverses Element*, wenn* $x + x'_r = e_r$ *gilt.*

In Satz 105 werden wir sehen, dass das Assoziativgesetz, wenn es für die Verknüpfung von drei Elementen gilt, auf die Verknüpfung von beliebig vielen Elementen übertragen werden kann.

Mengen, auf denen Verknüpfungen mit bestimmten Eigenschaften definiert sind, bekommen besondere Namen.

Definition 15 (Halbgruppe): *Sei $M \neq \emptyset$ eine Menge und $+$ eine innere Verknüpfung auf M. Ist $+$ assoziativ, so heißt das Paar $(M, +)$* Halbgruppe.

Um die Sprache (und die Notation) nicht unnötig sperrig zu machen, werden wir nicht zwischen der Menge M und der Halbgruppe $(M, +)$ unterscheiden, wenn klar ist, welche Verknüpfung auf M gemeint ist.

Satz 15: *Sei $(M, +)$ eine Halbgruppe mit linksneutralem bzw. rechtsneutralem Element. Ferner existiere für jedes $x \in M$ ein linksinverses bzw. rechtsinverses Element. Dann gilt:*

(i) Ein linksneutrales Element ist auch rechtsneutral und umgekehrt.

(ii) Ein zu $x \in M$ linksinverses Element ist zu x auch rechtsinvers und umgekehrt.

BEWEIS: Wegen der Symmetrie des Problems beweisen wir jeweils nur die erste Hälfte. Sei also $e_l \in M$ ein linksinverses Element, $x \in M$ beliebig, $x'_l \in M$ ein zu x linksinverses Element und $x''_l \in M$ ein linksinverses Element zu x'_l. Wir zeigen zunächst, dass dann auch $x+x'_l = e_l$ gilt, und folgern daraus, dass e_l auch rechtsneutral ist. Damit ist x'_l auch rechtsinvers zu x.

Wir rechnen

$$\begin{aligned} x + x'_l &= (e_l + x) + x'_l = ((x''_l + x'_l) + x) + x'_l = (x''_l + (x'_l + x)) + x'_l \\ &= (x''_l + e_l) + x'_l = x''_l + (e_l + x'_l) = x''_l + x'_l = e_l \end{aligned}$$

und

$$x + e_l = x + (x'_l + x) = (x + x'_l) + x = e_l + x = x.$$

Da $x \in M$ beliebig war, ist e_l ein rechtsneutrales Element, und wegen $x + x'_l = e_l$ ist x'_l auch rechtsinvers zu x. □

Dieses Ergebnis führt uns zu der

Definition 16: *Ein $e \in M$ heißt* neutrales Element*, wenn e links- und rechtsneutral ist. Weiter heißt $x' \in M$ zu $x \in M$* inverses Element*, wenn x' zu x links- und rechtsinvers ist.*

Aus Satz 15 folgt nun, dass in einer Halbgruppe mit den geforderten Eigenschaften jedes links- bzw. rechtsneutrale Element automatisch neutral ist, und eine analoge Aussage gilt für die inversen Elemente. Darüberhinaus gilt der

Satz 16: *Sei $(M, +)$ eine Halbgruppe. Dann gilt:*

(i) Existiert ein bzgl. $+$ neutrales Element in M, so ist dieses eindeutig bestimmt.

(ii) Existiert zu $x \in M$ ein inverses Element $x' \in M$ bzgl. $+$, so ist dieses eindeutig bestimmt.

(iii) Ist x' zu x invers, so ist auch x zu x' invers.

(iv) Es ist $(x')' = x$.

(v) Sind x' invers zu x und y' invers zu y, dann ist $y' + x'$ invers zu $x + y$.

BEWEIS:

(i) Sei $\widetilde{e}$ ein weiteres neutrales Element. Dann gilt $e = e + \widetilde{e} = \widetilde{e}$.

(ii) Sei $\widetilde{x'}$ ein weiteres zu x inverses Element. Dann folgt

$$x' = x' + e = x' + (x + \widetilde{x'}) = (x' + x) + \widetilde{x'} = e + \widetilde{x'} = \widetilde{x'}.$$

(iii) Nach Definition des inversen Elements gilt $x + x' = x' + x = e$. Liest man diese Gleichung von rechts nach links, so folgt die Behauptung.

(iv) Betrachte die Gleichungskette

$$(x')' = (x')' + e = (x')' + (x' + x) = ((x')' + x') + x = e + x = x.$$

(v) Es gilt

$$(y' + x') + (x + y) = ((y' + x') + x) + y = (y' + (x' + x)) + y = (y' + e) + y = y' + y = e.$$

Analog folgt $(x + y) + (y' + x') = e$. □

Definition 17 (Monoid): *Eine Halbgruppe mit neutralem Element heißt* Monoid.

Wir werden in diesem Kapitel auch Verküpfungen zwischen Mengen über ihre Elemente definieren. Sind etwa M, N Mengen und $+$ ein Verknüpfung auf $M \times N$, so definiert man

$$M + N := \{\, m + n \mid m \in M, n \in N \,\}$$

oder für ein $m \in M$

$$m + N := \{\, m + n \mid n \in N \,\}.$$

Beim Rechnen mit diesen Mengen muss man sehr vorsichtig sein, wie schon das einfache Beispiel $\mathbb{Z} + \mathbb{Z} = \mathbb{Z} \neq 2\mathbb{Z}$ zeigt!

4.2 Gruppen

4.2.1 Elementare Eigenschaften

Wir haben nun die absoluten Grundlagen im Umgang mit Verknüpfungen auf Mengen kennengelernt. Sehr viel wichtiger als die bisherigen Strukturen ist die

Definition 18 (Gruppe): *Ein Monoid, in dem jedes Element ein Inverses hat, heißt* Gruppe. *Ist die Verknüpfung zusätzlich kommutativ, so heißt die Gruppe* abelsch.

Mit Gruppen werden wir uns nun recht ausführlich befassen. Im Prinzip hatten wir schon in Satz 15 mit Gruppen zu tun, wir konnten es dort jedoch noch nicht wissen. Wie sich gezeigt hat, ist die Assoziativität einer Verknüpfung viel wichtiger als die Kommutativität, denn letztere haben wir bis jetzt noch gar nicht benutzt. In der Gruppentheorie ist es üblich, nur für eine kommutative Verknüpfung das Symbol $+$ zu verwenden. Das zu x Inverse bezeichnet man dann mit $-x$ und das neutrale Element mit 0. Außerdem setzt man $x - y := x + (-y)$. Man spricht in dem Fall auch von der *additiven* Schreibweise. Es sei jedoch betont, dass diese Bezeichnungen rein symbolisch zu verstehen sind und man nicht glauben sollte, Gruppen müssten immer mit Zahlen zu tun haben. Wir werden gleich ein Beispiel kennenlernen. Ist die Gruppe nicht abelsch, so schreibt man für die Verknüpfung $\cdot$ oder lässt das Verknüpfungszeichen gleich weg. Das zu x Inverse ist dann x^{-1} und das neutrale Element 1. Dies ist die *multiplikative* Schreibweise. Man definiert für $n \in \mathbb{N}$ und $x \in G$ je nach Schreibweise rekursiv

$$\begin{array}{lll} 0\,x := 0, & nx := x + (n-1)x, & (-n)x := -(nx), \\ x^0 := 1, & x^n := x \cdot x^{n-1}, & x^{-n} := (x^n)^{-1}. \end{array}$$

In Gruppen gelten die folgenden Rechenregeln:

Satz 17: *Seien $(G, \cdot)$ eine Gruppe und $g, h, k \in G$. Dann gilt:*

(i) Kürzungsregeln: $gh = gk \Rightarrow h = k$ und $hg = kg \Rightarrow h = k$.

(ii) Es gibt genau ein $x \in G$ mit $gx = h$ und ein (im Allgemeinen von x verschiedenes) $y \in G$ mit $yg = h$.

BEWEIS:

(i) Betrachte die Implikationen

$$gh = gk \Rightarrow g^{-1}(gh) = g^{-1}(gk) \Rightarrow (g^{-1}g)h = (g^{-1}g)k \Rightarrow 1h = 1k \Rightarrow h = k.$$

Die zweite Aussage erhält man analog.

(ii) Existenz: Setze $x := g^{-1}h$. Dann gilt:

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

Eindeutigkeit:

$$h = gx \Rightarrow g^{-1}h = g^{-1}(gx) = (g^{-1}g)x = 1x = x.$$

Analog für y $(= hg^{-1})$. □

Wenn man auf einer Gruppe eine Ordnungsrelation einführen will, so ist es wünschenswert, dass die Ordnung die Gruppenverknüpfung respektiert. Man kommt so zu der

Definition 19 (Geordnete Gruppe): *Eine abelsche Gruppe G heißt* geordnet, *wenn auf G eine Ordnungsrelation $\leq$ definiert ist, so dass für alle $g, h, k \in G$ gilt $g \leq h \Rightarrow g+k \leq h+k$.*

Wir werden das folgende Beispiel recht ausführlich diskutieren. Für eine beliebige Menge M kann man die Menge $\mathrm{Bij}(M) := \{ f \in M^M \mid f \text{ ist bijektiv} \}$ aller Bijektionen von M nach M betrachten. Dann folgt aus den Eigenschaften bijektiver Abbildungen, dass $\mathcal{S} := (\mathrm{Bij}(M), \circ)$ eine Gruppe ist mit neutralem Element id und dem zu f inversen Element f^{-1}. Diese Gruppe heißt *symmetrische Gruppe* und ist in der Gruppentheorie von großer Bedeutung. Hat M eine endliche Mächtigkeit n, so heißt $\mathcal{S}_n$ symmetrische Gruppe n-ten Grades. Die Elemente von $\mathrm{Bij}(M)$ heißen dann *Permutationen*.

Wir betrachten den Spezialfall $M = \{1, 2, 3\}$. Die Permutation

$$f\colon 1 \longmapsto f(1), 2 \longmapsto f(2), 3 \longmapsto f(3)$$

schreibt man kompakter als

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

Wir können die Gruppe $\mathcal{S}_3$ geometrisch interpretieren. Dazu stellen wir uns ein gleichseitiges Dreieck vor und benennen die Ecken mit 1, 2 und 3. Die Permutationen entsprechen dann genau den Spiegelungen und Drehungen, die das Dreieck in sich selbst überführen. Betrachten wir die Elemente von $\mathcal{S}_3$ einmal in Detail:

$$D_{0^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad D_{120^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad D_{240^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$S_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad S_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad S_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Wir erkennen die Drehungen um 0°, 120°, 240° und die Spiegelungen an der Seitenhalbierenden durch Punkt 1, 2 und 3. Damit haben wir gezeigt, dass die Hintereinanderschaltung der Drehungen und Spiegelungen, die ein gleichseitiges Dreieck in sich selbst überführen, eine Gruppe bildet!

Es ist interessant, sich die inversen Elemente zu einer vorgegebenen Abbildung anzuschauen. Das macht man am besten mit einer *Verknüpfungstabelle* wie in Tabelle 4.1. Man kann dann ebenfalls direkt sehen, dass diese Gruppe nicht abelsch ist. Es folgt übrigens aus Satz 17, dass in der Tabelle in jeder Zeile und jeder Spalte jedes Element genau einmal vorkommt.

Wir können die Elemente von $\mathcal{S}_n$ auch noch anders aufschreiben. Wir beginnen mit der 1 und notieren weiter $f(1)$, $f(f(1))$ usw. bis sich die Teilpermutation schließt. Wir setzen die Teilpermutation in Klammern und machen mit der nächsten Zahl weiter, die noch in keiner Teilpermutation aufgetaucht ist. So ergeben sich die Schreibweisen

$$D_{0^\circ} = (1)(2)(3) \qquad D_{120^\circ} = (1,2,3) \qquad D_{240^\circ} = (1,3,2)$$
$$S_1 = (1)(2,3) \qquad S_2 = (1,3)(2) \qquad S_3 = (1,2)(3).$$

$\circ$	D_{0°	D_{120°	D_{240°	S_1	S_2	S_3
D_{0°	D_{0°	D_{120°	D_{240°	S_1	S_2	S_3
D_{120°	D_{120°	D_{240°	D_{0°	S_2	S_3	S_1
D_{240°	D_{240°	D_{0°	D_{120°	S_3	S_1	S_2
S_1	S_1	S_3	S_2	D_{0°	D_{240°	D_{120°
S_2	S_2	S_1	S_3	D_{120°	D_{0°	D_{240°
S_3	S_3	S_2	S_1	D_{240°	D_{120°	D_{0°

Tabelle 4.1: Verknüpfungtabelle für $\mathcal{S}_3$.

Definition 20: *Eine Permutation $f \in \mathcal{S}_n$ heißt* Zyklus *der Länge k oder k-Zyklus, wenn paarweise verschiedene Elemente $x_1, \ldots, x_k \in \{1, \ldots, n\}$ existieren mit $f(x_1) = x_2$, $\ldots$, $f(x_{k-1}) = x_k$, $f(x_k) = x_1$ und $f(x) = x$ sonst. Man schreibt dann $f = (x_1, \ldots, x_k)$. Ein Zyklus der Länge 2 heißt* Transposition. *Zwei Zyklen $(x_1, \ldots, x_k)$ und $(y_1, \ldots, y_l)$ heißen* disjunkt, *wenn $\{x_1, \ldots, x_k\} \cap \{y_1, \ldots, y_l\} = \emptyset$ gilt.*

Wir haben gerade gesehen, dass man jede Permutation aus $\mathcal{S}_3$ in disjunkte Zyklen zerlegen kann. Dies gilt natürlich allgemein in $\mathcal{S}_n$. Weiter gilt der

Satz 18: *Jede Permutation aus $\mathcal{S}_n$ ist ein Kompositum von Transpositionen.*

BEWEIS: Schreibe jeden Zyklus als $(x_1, \ldots, x_k) = (x_1, x_k)(x_1, x_{k-1}) \cdots (x_1, x_2)$. □

Man kann also jede beliebige Permutation durch wiederholtes Vertauschen von je zwei Elementen erhalten. Dabei ist die Zerlegung in Transpositionen natürlich nicht eindeutig.

4.2.2 Untergruppen

Es kommt sehr häufig vor, dass Teilmengen einer Gruppe wieder eine Gruppe bilden. Deshalb definiert man:

Definition 21 (Untergruppe): *Sei $(G, \cdot)$ eine Gruppe und $\emptyset \neq U \subseteq G$ eine Teilmenge. U heißt* Untergruppe *von G (geschrieben $U < G$) genau dann, wenn gilt:*

(i) $g, h \in U \Rightarrow gh \in U$

(ii) $g \in U \Rightarrow g^{-1} \in U$.

Es ist trivial, dass dann U mit der Einschränkung der Gruppenoperation von G auf U wieder eine Gruppe bildet. Jede Gruppe G hat stets $\{1\}$ und G selbst als Untergruppe.

An Tabelle 4.1 liest man ab, dass $\mathcal{S}_3$ die Untergruppen

$$\{D_{0^\circ}\}, \{D_{0^\circ}, S_1\}, \{D_{0^\circ}, S_2\}, \{D_{0^\circ}, S_3\}, \{D_{0^\circ}, D_{120^\circ}, D_{230^\circ}\}, S_3$$

hat.

Man kann die zwei Aussagen aus der Definition der Untergruppe zusammenfassen zu einer einzigen zu überprüfenden Aussage. Es gilt nämlich der folgende

Satz 19: *Für $\emptyset \neq U \subseteq G$ sind äquivalent:*

(i) $U < G$

(ii) $g, h \in U \Rightarrow gh^{-1} \in U$.

BEWEIS:
„⇒“: Es sei $U < G$. Aus $h \in U$ folgt $h^{-1} \in U$ und $gh^{-1} \in U$.
„⇐“: (ii) gelte für alle $g, h \in U$. Mit $g := 1$ folgt $h^{-1} \in U$. Da $(h^{-1})^{-1} = h$folgt mit $k := h^{-1}$ sofort $gk^{-1} = g(h^{-1})^{-1} = gh \in U$, also 1). □

Definition 22: *Sei G ein Gruppe und $M \subseteq G$ eine Teilmenge. Man bezeichnet mit $\langle M \rangle$ die kleinste Untergruppe von G, die M enthält. Ist $M = \{g_1, \ldots, g_n\}$, so schreibt man $\langle g_1, \ldots, g_n \rangle := \langle \{g_1, \ldots, g_n\} \rangle$.*

Die Gruppe $\langle M \rangle$ besteht aus dem neutralen Element in G, allen Elementen von M, ihren Verknüpfungen untereinander und deren Inversen. Deshalb sagt man, dass $\langle M \rangle$ von M *erzeugt* wird.

Auf unser Beispiel übertragen ergibt das

$$\{D_{0^\circ}\} = \langle D_{0^\circ} \rangle, \{D_{0^\circ}, S_1\} = \langle S_1 \rangle, \{D_{0^\circ}, S_2\} = \langle S_2 \rangle, \{D_{0^\circ}, S_3\} = \langle S_3 \rangle,$$

$$\{D_{0^\circ}, D_{120^\circ}, D_{230^\circ}\} = \langle D_{120^\circ} \rangle = \langle D_{240^\circ} \rangle, S_3 = \langle S_1, S_3 \rangle = \langle S_1, D_{120^\circ} \rangle = \cdots.$$

Weiter ist $(\mathbb{Z}, +) = \langle 1 \rangle$ und $(\mathbb{Q} \setminus \{0\}, \cdot) = \langle \mathbb{Z} \setminus \{0\} \rangle$.

Definition 23 (Zyklische Gruppe): *Eine Gruppe G heißt* zyklisch*, wenn es ein $g \in G$ gibt, so dass $\langle g \rangle = G$ ist.*

Jede zyklische Gruppe ist von der Form $\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$. Daher folgt:

Satz 20: *Jede zyklische Gruppe ist abelsch.*

BEWEIS: Sind $h, l \in G$, so existieren $m, n \in \mathbb{Z}$, so dass $h = g^m$ und $l = g^n$ gilt. Somit folgt $hl = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = lh$. □

Ein Beispiel für eine zyklische Gruppe kennen wir schon, nämlich $(\mathbb{Z}, +) = \langle 1 \rangle$. Diese Gruppe ist unendlich. Wir gehen nun näher auf die endlichen zyklischen Gruppen ein.

Definition 24 (Ordnung): *Sei G eine Gruppe und $g \in G$. Hat G endlich viele Elemente k, so heißt k die* Ordnung *der Gruppe G. Man schreibt dafür auch $\mathrm{Ord}(G) := |G|$. Die kleinste Zahl $n \in \mathbb{N} \setminus \{0\}$ mit $g^n = 1$ nennt man die* Ordnung *von g.*

Man zeigt nun zunächst:

Satz 21: *Die Ordnung von g ist gleich der Ordnung von $\langle g \rangle$.*

BEWEIS: Sei g von der Ordnung n. Es gelte o. E. $n > 1$, d. h. $g \neq 1$. Die Behauptung folgt, wenn die Menge $\{ g^n \mid n \in \mathbb{Z} \}$ genau n Elemente enthält, d. h. genauer wenn die Elemente g^k mit $0 \leq k < n$ paarweise verschieden sind. Nehmen wir dazu das Gegenteil an, also es gäbe $k, m \in \mathbb{N}$ mit $0 \leq k < m < n$ und $g^k = g^m$. Dann wäre $g^{m-k} = 1$, was wegen $0 < m - k < n$ ein Widerspruch zur Minimalität von n ist. Damit hat $\langle g \rangle$ gerade n Elemente, da für jedes $k \in \mathbb{Z}$ stets $g^{k+n} = g^k$ gilt. □

Damit folgt nun unmittelbar der

Satz 22: *Ist G eine Gruppe der Ordnung n, so ist $g \in G$ genau dann erzeugendes Element der Gruppe, d. h. $\langle g \rangle = G$, wenn g von der Ordnung n ist.*

Da die Elemente der Gruppe eine Struktur haben, kann man nun über diese Struktur weitere Operationen auf Mengen einführen.

Definition 25 (Nebenklassen und Normalteiler): *Seien G ein Gruppe und $M, N \subseteq G$ Teilmengen. Man setzt*

$$M \cdot N := \{ m \cdot n \in G \mid m \in M \wedge n \in N \} \quad \textit{und} \quad M^{-1} := \{ m^{-1} \in G \mid m \in M \}.$$

Für $g \in G$ schreibt man weiter

$$g \cdot M := \{ g \cdot m \in G \mid m \in M \}$$

sowie analoge Ausdrücke für $M \cdot g$ und $g \cdot M \cdot g^{-1}$. Die entsprechenden additiven Ausdrücke sind klar.

Ist $U < G$, so nennt man die Menge gU die Linksnebenklasse *von g bzgl. U. Entsprechend ist Ug die* Rechtsnebenklasse. *Die Menge gUg^{-1} heißt* Normalteiler *von G (geschrieben $U \lhd G$), wenn gilt $gUg^{-1} = U$ für alle $g \in G$, d. h. wenn $gU = Ug$ ist.*

Wegen Aufgabe 16 a) ist noch folgende Definition sinnvoll:

Definition 26 (Index): *Die Anzahl der Links- bzw. Rechtsnebenklassen wird* Index *von U in G genannt und $[G : U]$ geschrieben.*

Wir steuern nun auf einen wichtigen Satz der elementaren Gruppentheorie zu, den Satz von Lagrange. Vorher machen wir noch ein paar Vorarbeiten.

Satz 23: *Sei G eine Gruppe und $U < G$ eine Untergruppe. Die Relation R, die durch $gRh :\Leftrightarrow gh^{-1} \in U$ definiert ist, ist eine Äquivalenzrelation, und es ist $[g] = Ug$.*

BEWEIS: Reflexivität: Es ist $gRg \Leftrightarrow gg^{-1} = 1 \in U$, was klar ist. Symmetrie: Sei gRh, also $gh^{-1} \in U$. Da U Untergruppe ist, ist auch $(gh^{-1})^{-1} = hg^{-1} \in U$, also hRg. Transitivität: Sei gRh und hRk bzw. $gh^{-1} \in U$ und $hk^{-1} \in U$. Dann ist auch $(gh^{-1})(hk^{-1}) = gk^{-1} \in U$, also gilt gRk. Die Äquivalenzklasse ergibt sich aus[1]

$$[g] = \{ x \in G \mid xRg \} = \{ x \in G \mid xg^{-1} \in U \} = \{ x \in G \mid x \in Ug \} = Ug. \qquad \square$$

[1] Die Äquivalenz $xg^{-1} \in U \Leftrightarrow x \in Ug$ schreibt sich etwas ausführlicher

$$xg^{-1} \in U \Leftrightarrow \exists_{u \in U} : xg^{-1} = u \Leftrightarrow \exists_{u \in U} : x = ug \Leftrightarrow x \in Ug.$$

Alle Äquivalenzklassen sind also gerade die Rechtsnebenklassen. Der folgende Satz besagt, dass alle Rechtsnebenklassen gleich groß sind.

Satz 24: *Für alle $g \in G$ ist $\mathrm{Ord}(Ug) = \mathrm{Ord}(U)$.*

BEWEIS: Wir zeigen, dass die Abbildung $f\colon U \to Ug\colon u \mapsto ug$ eine Bijektion ist. Dass sie surjektiv ist, ist klar. Wir zeigen nun die Injektivität. Sei dazu $f(u) = f(v)$, dann folgt $ug = vg$ und damit $u = v$. □

Satz 25 (Satz von Lagrange): *Sei G eine endliche Gruppe und $U < G$ eine Untergruppe, dann ist $\mathrm{Ord}(U)$ ein Teiler von $\mathrm{Ord}(G)$. Genauer gilt $\mathrm{Ord}(G) = \mathrm{Ord}(U) \cdot [G : U]$.*

BEWEIS: Nach Satz 7 und Satz 23 ist $G = U \cup Ug_1 \cup \cdots \cup Ug_n$ mit geeignet gewählten $g_i \in G$ eine disjunkte Vereinigung. Mit Satz 24 folgt die Behauptung. □

Der Satz von Lagrange ist nur ein erstes Beispiel für die mannigfachen Verknüpfungen zwischen Algebra und Zahlentheorie. Aus ihm folgt z. B. ein interessanter Zusammenhang zwischen Primzahlen und zyklischen Gruppen.

Satz 26: *Jede Gruppe, deren Ordnung eine Primzahl ist, ist zyklisch.*

BEWEIS: Sei $\mathrm{Ord}(G) = p \in \mathbb{P}$ und $1 \neq g \in G$. Die Untergruppe $\langle g \rangle$ hat mehr als ein Element. Da nach Satz 25 $\mathrm{Ord}(\langle g \rangle)$ ein Teiler von p sein muss, folgt $\mathrm{Ord}(\langle g \rangle) = p$. Damit muss $\langle g \rangle = G$ gelten. □

Satz 27: *Sei G eine Gruppe mit $\mathrm{Ord}(G) = n$ und $g \in G$. Dann gilt $g^n = 1$.*

BEWEIS: Die Ordnung von g ist gleich der Ordnung von $\langle g \rangle$ (Satz 21). Da $\langle g \rangle < G$ ist $\mathrm{Ord}(\langle g \rangle)$ Teiler von $\mathrm{Ord}(G) = n$ nach Satz 25. Somit existiert ein $k \in \mathbb{N}$, so dass $n = \mathrm{Ord}(\langle g \rangle) \cdot k$ und folglich $g^n = g^{\mathrm{Ord}(\langle g \rangle) \cdot k} = 1^k = 1$ ist. □

Der Satz von Lagrange sagt nur etwas über die Größe von möglichen Untergruppen, aber nichts über ihre Existenz aus. Es ist weder klar, ob jeder Teiler der Gruppenordnung als Untergruppenordnung vorkommt, noch wieviele Untergruppen derselben Ordnung es gibt. Eine teilweise Umkehrung des Satzes von Lagrange liefern die Sylow-Sätze, auf die wir hier nicht eingehen.

4.2.3 Homomorphismen

Wir untersuchen nun Abbildungen zwischen Gruppen. Dabei ist es natürlich sinnvoll, solche Abbildungen zu untersuchen, welche die Gruppenstruktur respektieren. Dies sind die sogenannten Gruppenhomomorphismen. Wenn es klar ist, welche algebraische Struktur gemeint ist, werden wir kurz von Homomorphismen sprechen. Es sei darauf hingewiesen, dass von Homomorphismen zwischen anderen algebraischen Strukturen als Gruppen (z. B. Körperhomomorphismen oder Vektorraumhomomorphismen) zusätzliche Eigenschaften als die folgenden verlangt werden!

Definition 27 (Gruppenhomomorphismus): *Seien G und H Gruppen, $f\colon G \to H$ eine Abbildung. f heißt* Homomorphismus *genau dann, wenn gilt: $f(gh) = f(g)f(h)$ für alle $g, h \in G$. Für Homomorphismen mit bestimmten Eigenschaften werden weitere Bezeichnungen eingeführt. Diese sind im Einzelnen:*

(i) Ein injektiver Homomorphismus heißt Monomorphismus*.*

(ii) Ein surjektiver Homomorphismus heißt Epimorphismus*.*

(iii) Ein bijektiver Homomorphismus heißt Isomorphismus*.*

(iv) Ein Homomorphismus $f\colon G \to G$ heißt Endomorphismus*.*

(v) Ein bijektiver Endomorphismus heißt Automorphismus*.*

Wir stellen zunächst fest, dass das neutrale Element von G unter einem Homomorphismus immer auf das neutrale Element von H abgebildet wird. (Die Umkehrung gilt nicht, d. h. das Urbild des neutralen Elements von H muss nicht nur das neutrale Element von G sein.) Um Konfusionen zu vermeiden, bezeichnen wir das neutrale Element von G mit 1_G und das neutrale Element von H mit 1_H. Außerdem ist das Inverse des Bildes eines Elements das Bild des Inversen des Urbildes.

Satz 28: *Seien G, H Gruppen und $f\colon G \to H$ ein Homomorphismus. Dann gilt:*

(i) Es ist $f(1_G) = 1_H$.

(ii) Es gilt $f(g^{-1}) = f(g)^{-1}$.

BEWEIS:

(i) Aus $f(1_G) = f(1_G 1_G) = f(1_G)f(1_G)$ folgt

$$1_H = (f(1_G)f(1_G))f(1_G)^{-1} = f(1_G)(f(1_G)f(1_G)^{-1}) = f(1_G)1_H = f(1_G).$$

(ii) Es ist $1_H = f(1_G) = f(gg^{-1}) = f(g)f(g^{-1})$, also $f(g^{-1}) = 1_H f(g)^{-1} = f(g)^{-1}$. □

Aus verschiedenen Gründen ist es interessant zu wissen, welche Elemente aus G auf das neutrale Element von H abgebildet werden. Daher trifft man die

Definition 28 (Bild und Kern): *Man bezeichnet die Menge $f(G) = \{\, f(g) \in H \mid g \in G \,\}$ als das* Bild *von f, geschrieben* $\operatorname{Bild} f$*. Die Faser $f^{-1}(1_H) = \{\, g \in G \mid f(g) = 1_H \,\}$ heißt* Kern *von f und wird mit* $\operatorname{Kern} f$ *bezeichnet.*

Diese beiden Objekte, vor allem aber der Kern, sind in der Algebra von großer Bedeutung. Dies liegt daran, dass diese zunächst mengentheoretische Konstruktion algebraische Eigenschaften hat, wie der folgende Satz zeigt. Wir verwenden daher die Bezeichung $\operatorname{Kern} f$ bzw. $\operatorname{Bild} f$ für das algebraische Objekt, und $f^{-1}(1_H)$ bzw. $f(G)$, wenn wir nur die Menge meinen.

Satz 29: *Seien G, H Gruppen und $f\colon G \to H$ ein Homomorphismus. Dann gilt*

(i) $\operatorname{Kern} f < G$

(ii) $\operatorname{Bild} f < H$.

BEWEIS:

(i) Seien $g_1, g_2 \in \operatorname{Kern} f$. Dann gilt $f(g_1) = 1_H$ und $f(g_2) = 1_H$, d. h. $f(g_1) = f(g_2)$ und $1_H = f(g_1)f(g_2)^{-1} = f(g_1)f(g_2^{-1}) = f(g_1 g_2^{-1})$, also $g_1 g_2^{-1} \in \operatorname{Kern} f$.

(ii) Seien $h_1, h_2 \in \operatorname{Bild} f$, d. h es gibt $g_1, g_2 \in G$ mit $f(g_1) = h_1$ und $f(g_2) = h_2$. Daraus folgt $h_1^{-1} = f(g_1)^{-1} = f(g_1^{-1})$, also $h_1^{-1} \in \operatorname{Bild} f$. Außerdem ist $h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2)$, also $h_1 h_2 \in \operatorname{Bild} f$. □

Erstaunlicherweise reicht es schon zu wissen, dass nur das neutrale Element von G auf das neutrale Element von H abgebildet wird, damit f injektiv ist.

Satz 30: *Es ist f ein Monomorphismus genau dann, wenn $\operatorname{Kern} f = \{1_G\}$ gilt.*

BEWEIS:
„⇒“: Klar!
„⇐“: Sei $f(g_1) = f(g_2)$. Dann folgt $1_H = f(g_1)f(g_2)^{-1} = f(g_1)f(g_2^{-1}) = f(g_1 g_2^{-1})$ und somit $g_1 g_2^{-1} \in \operatorname{Kern} f$. Da $\operatorname{Kern} f = \{1_G\}$ folgt $g_1 = g_2$, also ist f injektiv. □

Wir erweitern nun Satz 29 und zeigen: Es gilt sogar $\operatorname{Kern} f \lhd G$.

Satz 31: *Der Kern eines Homomorphismus $f : G \to H$ ist ein Normalteiler von G.*

BEWEIS: Definitionsgemäß ist $g(\operatorname{Kern} f)g^{-1} = \{\, gug^{-1} \mid u \in \operatorname{Kern} f \,\}$. Es gilt jedoch $f(gug^{-1}) = f(g)f(u)f(g^{-1}) = f(g)1_H f(g)^{-1} = 1_H$, also $gug^{-1} \in \operatorname{Kern} f$. □

Wir werden unsere Einführung in die Gruppentheorie mit einigen Überlegungen zur Isomorphie von Gruppen abschließen. Zwei Gruppen G und H heißen *isomorph* (geschrieben $G \simeq H$), wenn es einen Isomorphismus zwischen ihnen gibt. Die Isomorphie bedeutet anschaulich, dass es keine Rolle spielt, ob man ein Ergebnis in der einen oder in der anderen Gruppe erziehlt, da dieses problemlos auf die andere Gruppe übetragen werden kann. Man kann daher grundsätzlich Eindeutigkeitsaussagen nur „bis auf Isomorphie“ machen.

Definition 29 (Faktorgruppe): *Sei G eine Gruppe und $N \lhd G$ ein Normalteiler. Die Menge G/N aller Nebenklassen wird als* Faktorgruppe *von G nach N bezeichnet.*

Der Name Faktorgruppe legt schon den folgenden Satz nahe:

Satz 32: *Die Faktorgruppe bildet bzgl. der in Defintion 25 eingeführten Verknüpfung von Mengen eine Gruppe.*

BEWEIS: Da $1 \in G$ ist $1N = N \in G/N$ und somit $G/N \neq \emptyset$. Abgeschlossenheit: Seien $g, h \in G$. Dann gilt $(gN)(hN) = g(Nh)N = g(hN)N = ghN$. Die Assoziativität wird direkt von der Assoziativität der Verknüpfung in G geerbt. Ebenfalls ergibt sich, dass N neutrales Element und $g^{-1}N$ das zu gN inverse Element sind. □

Bei diesem Beweis ist absolut wesentlich, dass N ein Normalteiler und nicht nur eine Untergruppe ist. Faktorisiert man nach einer Untergruppe, so muss der Quotient keine Gruppe mehr sein. Darin liegt die eigentliche Bedeutung der Normalteiler.

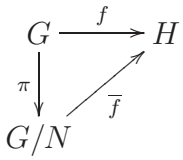
Es findet sich nun ein interessanter Zusammenhang zu Satz 31. Dieser besagte, dass jeder Kern eines Homomorphismus ein Normalteiler ist. Umgekehrt ist aber nun auch jeder Normalteiler Kern eines Homomorphismus, und zwar des *kanonischen Epimorphismus*

$$\pi\colon G \longrightarrow G/N\colon g \longmapsto gN,$$

denn

$$g \in \operatorname{Kern}\pi \Leftrightarrow gN = N \Leftrightarrow g \in N.$$

Satz 33 (Homomorphiesatz für Gruppen): *Sei $f\colon G \to H$ ein Epimorphismus und $N := \operatorname{Kern} f$. Dann ist die Abbildung $\overline{f}\colon G/N \to H\colon gN \mapsto f(g)$ ein Isomorphismus, also $G/N \simeq H$ und*



kommutiert.

BEWEIS: Wir müssen wieder zunächst die Wohldefiniertheit von $\overline{f}$ zeigen. Seien dazu $g, h \in G$ mit $gN = hN$. Dann folgt $gh^{-1} \in N = \operatorname{Kern} f$ und somit

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

Wir überprüfen als nächstes, dass $\overline{f}$ tatsächlich ein Homomorphismus ist. Es gilt

$$\overline{f}(gNhN) = \overline{f}(ghN) = f(gh) = f(g)f(h) = \overline{f}(gN)\overline{f}(hN),$$

da f ein Homomorphismus ist. Nun rechnen wir die Bijektivität von $\overline{f}$ nach. Die Surjektivität ist klar. Zur Injektivität liest man an der Äquivalenz

$$gN \in \operatorname{Kern}\overline{f} \Leftrightarrow 1_H = \overline{f}(gN) = f(g) \Leftrightarrow g \in \operatorname{Kern} f = N$$

ab, dass $\operatorname{Kern}\overline{f} = \{N\}$ gilt. Aus Satz 30 folgt die Behauptung. □

Satz 34: *Sei G eine Gruppe, $U < G$ eine Untergruppe und $N \lhd G$ ein Normalteiler. Dann gilt:*

(i) $U \cap N \lhd U$

(ii) $N \subseteq U \Rightarrow N \lhd U$

(iii) $U \cdot N < G$ *und* $N \lhd U \cdot N$

(iv) $N \subseteq U \wedge U \lhd G \Rightarrow U/N \lhd G/N.$

BEWEIS:

(i) Sei $\pi\colon G \to G/N$ der kanonische Epimorphismus, so ist die Einschränkung von π auf U ein Homomorphismus, und $\pi|_U : U \to G/N$ hat $\operatorname{Kern}\ \pi|_U = U \cap N$.

(ii) Klar.

(iii) Seien $u_1, u_2 \in U$, $n_1, n_2 \in N$. Dann sind $u_1 n_1, u_2 n_2 \in U \cdot N$. Da N Normalteiler ist ergibt sich

$$u_1 n_1 (u_2 n_2)^{-1} = u_1 n_1 n_2^{-1} u_2^{-1} = u_1 n_1 u_2^{-1} \underbrace{(u_2 n_2^{-1} u_2^{-1})}_{:= n_3 \in N} = u_1 u_2^{-1} \underbrace{(u_2 n_1 u_2^{-1})}_{:= n_4 \in N} n_3,$$

also $u_1 u_2^{-1} n_4 n_3 \in U \cdot N$. Daraus folgt $U \cdot N < G$. Zur zweiten Aussage betrachtet man

$$u_1 n_1 n (u_1 n_1)^{-1} = u_1 (n_1 n n_1^{-1}) u_1^{-1} \in N$$

für alle $n \in N$.

(iv) Zunächst ist

$$U/N = \{\, uN \mid u \in U \,\} \subseteq \{\, gN \mid g \in G \,\} = G/N.$$

Man berechnet weiter mit Satz 32 $u_1 N \cdot u_2 N = u_1 u_2 N \in U/N$ und $(u_1 N)^{-1} = u_1^{-1} N \in U/N$, also ist $U/N < G/N$. Aus $gNuN(gN)^{-1} = gug^{-1}N$ folgt wegen $gug^{-1} \in U$ die Behauptung. □

Satz 35 (Erster Isomorphiesatz für Gruppen): *Sei G eine Gruppe, $U < G$ eine Untergruppe und $N \lhd G$ ein Normalteiler. Dann gilt $(UN)/N \simeq U/(U \cap N)$.*

BEWEIS: Betrachte den Epimorphismus $f\colon U \to (UN)/N\colon u \mapsto uN$. Offenbar ist $\operatorname{Kern} f = U \cap N$. Die Isomorphie erhält man direkt aus Satz 33. □

Satz 36 (Zweiter Isomorphiesatz für Gruppen): *Seien $U, N \lhd G$ Normalteiler mit $N < U$, so gilt $(G/N)/(U/N) \simeq G/U$.*

BEWEIS: Der Epimorphismus $f\colon G \to (G/N)/(U/N)\colon g \mapsto (gN)U/N$ hat $\operatorname{Kern} f = U$. Mit Satz 33 folgt die Behauptung. □

Wir kommen nun zum Hauptergebnis dieses Abschnitts, dem Klassifikationssatz für zyklische Gruppen. Wir werden feststellen, dass jede zyklische Gruppe isomorph zu $(\mathbb{Z}, +)$ oder zu $(\mathbb{Z}/n\mathbb{Z}, +)$ ist[2]. Vorher brauchen wir noch den

Satz 37: *Jede Untergruppe von $(\mathbb{Z}, +)$ hat die Form $n \cdot \mathbb{Z}$ mit $n \in \mathbb{N}$.*

[2] Zur Wohldefiniertheit der Restklassenaddition siehe den bereits erwähnten Artikel zur Zahlentheorie.

BEWEIS: Betrachte den Homomorphismus $f\colon \mathbb{Z} \to \mathbb{Z}\colon m \mapsto n \cdot m$. Es ist $\operatorname{Bild} f = n\mathbb{Z}$, also ist wegen Satz 29 $n\mathbb{Z} < \mathbb{Z}$. Sei nun $U < \mathbb{Z}$ eine beliebige Untergruppe. Ist $U = \{0\}$, so folgt $U = 0\mathbb{Z}$, und wir sind fertig. Andernfalls existiert ein $u \in U \setminus \{0\}$. Da U Untergruppe ist, ist auch $-u \in U$. Da stets $u \in \mathbb{N}$ oder $-u \in \mathbb{N}$ gilt, ist $U \cap \mathbb{N} \neq \emptyset$. In Satz 90 werden wir sehen, dass jede nicht-leere Teilmenge von $\mathbb{N}$ ein kleinstes Element besitzt. Wir können daher $n := \min(U \cap \mathbb{N})$ wählen. Da U Untergruppe ist, ist mit n auch $mn = \underbrace{n + \cdots + n}_{m \text{ mal}}$ in U, und zwar für alle $m \in \mathbb{N}$. Ebenfalls ist $-mn \in U$. Daraus folgt $n\mathbb{Z} \subseteq U$. Für die Inklusion in die andere Richtung wähle man ein $u \in U$ und dividiere durch n mit Rest. Es ist dann $u = qn + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < n$. Wegen $n\mathbb{Z} \subseteq U$ ist insbesondere $qn \in U$ und somit auch $r = u - qn$. Dann kann nur $r = 0$ gelten, da $n = \min(U \cap \mathbb{N})$. Damit folgt $u \in n\mathbb{Z}$, woraus sich $n\mathbb{Z} \supseteq U$ und insgesamt $n\mathbb{Z} = U$ ergibt. □

Wir sind nun bereit für den

Satz 38 (Klassifikationssatz für zyklische Gruppen): *Sei $(G, \cdot)$ eine zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$ gewählt. Dann gilt:*

(i) Ist $\operatorname{Ord}(G) = \infty$, so ist $G \simeq \mathbb{Z}$, $G = \{\, g^n \mid n \in \mathbb{Z} \,\}$ und $g^k \neq g^l$ für $k \neq l$.

(ii) Ist $\operatorname{Ord}(G) = n$, so ist $G \simeq \mathbb{Z}/n\mathbb{Z}$, $G = \{1, g, \ldots, g^{n-1}\}$ und $g^k = g^l \Leftrightarrow k - l = mn$ mit $m \in \mathbb{Z}$.

BEWEIS: Wie schon weiter oben bemerkt gilt $G = \langle g \rangle = \{\, g^n \mid n \in \mathbb{Z} \,\}$. Wir betrachten die Abbildung $f\colon \mathbb{Z} \to G\colon m \mapsto g^m$. Wegen $g^{m+n} = g^m g^n$ ist f ein Epimorphismus. Wir unterscheiden nun zwei Fälle. Ist f zusätzlich injektiv, so ist $G \simeq \mathbb{Z}$ und insbesondere $\operatorname{Ord}(G) = \infty$ und $g^k \neq g^l$ für $k \neq l$. Ist f nicht injektiv, so ist gibt es ein $n \in \mathbb{N}$ mit $\operatorname{Kern} f = n\mathbb{Z}$ aufgrund von Satz 37. Wegen Satz 33 ist dann aber

$$\overline{f}\colon \mathbb{Z}/n\mathbb{Z} \longrightarrow G\colon m + n\mathbb{Z} \longmapsto g^m$$

ein Isomorphismus und somit $G \simeq \mathbb{Z}/n\mathbb{Z}$. Da

$$\mathbb{Z}/n\mathbb{Z} = \{\, 0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z} \,\}$$

ist $\operatorname{Ord}(\mathbb{Z}/n\mathbb{Z}) = n$. Dies liefert $G = \{1, g, \ldots, g^{n-1}\}$, $\operatorname{Ord}(G) = n$ sowie $g^k = g^l \Leftrightarrow k - l = mn$ für ein $m \in \mathbb{Z}$. □

Wir zeigen nun zum Abschluss unserer Untersuchungen von zyklischen Gruppen den

Satz 39: *Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer gilt: Ist $G = \langle g \rangle$, so sind die Untergruppen von G genau die Gruppen der Form $\langle g^n \rangle$ mit $n \geq 0$.*

BEWEIS: Sei $U < G$ eine beliebige Untergruppe. Der Fall $U = \{1\}$ ist klar. Ist $U \neq \{1\}$, so gibt es ein $1 \neq g^m \in U$ mit $m \in \mathbb{Z}$. Da U Untergruppe ist, ist auch $g^{-m} \in U$, so dass wir $m > 0$ annehmen können. Sei nun $n \in \mathbb{N} \setminus \{0\}$ die kleinste natürliche Zahl mit $g^n \in U$. Natürlich ist dann $\langle g^n \rangle \subseteq U$. Sei nun $g^m \in U$. Wir dividieren m durch n mit Rest und erhalten $m = qn + r$ mit $0 \leq r < n$. Daraus folgt $a^m = (a^n)^q \cdot a^r$, also $a^r = (a^n)^{-q} \cdot a^m \in U$. Aus der Minimalität von n folgt $r = 0$ und damit $m = qn$ sowie $a^m = (a^n)^q \in \langle a^n \rangle$. Also haben wir die Inklusion $U \subseteq \langle a^n \rangle$ und insgesamt $U = \langle a^n \rangle$. □

4.2.4 Grothendieck-Gruppen

Wir werden nun sehen, wie man aus einer Halbgruppe eine Gruppe konstruieren kann. Dabei besteht der Trick darin, diese Konstruktion gerade so anzulegen, dass man die ursprüngliche Halbgruppe in der neuen Gruppe wiederfinden kann. Wir werden dieses Verfahren in Kapitel 5 benutzen, um aus den natürlichen die ganzen Zahlen zu gewinnen.

Satz 40: *Sei $(M,\cdot)$ eine Halbgruppe mit einer kommutativen Verknüpfung $\cdot$. Dann wird durch*

$$(x_1,y_1)R(x_2,y_2) :\Leftrightarrow \exists_{z\in M} : x_1y_2z = x_2y_1z$$

auf $M\times M$ ein Äquivalenzrelation eingeführt.

BEWEIS: Reflexivität: Ist erfüllt, da $x_1y_1z = x_1y_1z$ für alle $x_1,y_1,z\in M$ gilt. Symmetrie: Sei $(x_1,y_1)R(x_2,y_2)$. Dann ist $x_1y_2z = x_2y_1z$ mit einem $z\in M$ und auch $(x_2,y_2)R(x_1,y_1)$. Transitivität: Seien (x_1,y_1), (x_2,y_2) und (x_3,y_3) mit $(x_1,y_1)R(x_2,y_2)$ und $(x_2,y_2)R(x_3,y_3)$. Es gibt $z,\widetilde{z}\in M$ mit $x_1y_2z = x_2y_1z$ und $x_2y_3\widetilde{z} = x_3y_2\widetilde{z}$. Daraus folgt

$$\begin{aligned}(x_1y_3)(y_2z\widetilde{z}) &= (x_1y_2z)(y_3\widetilde{z}) = (x_2y_1z)(y_3\widetilde{z})\\ &= (y_1z)(x_2y_3\widetilde{z}) = (y_1z)(x_3y_2\widetilde{z}) = (x_3y_1)(y_2z\widetilde{z}),\end{aligned}$$

also $(x_1,y_1)R(x_3,y_3)$. □

Man schreibt für die Äquivalenzklassen abkürzend $[x,y] := [(x,y)]$.

Satz 41: *Die Menge der Äquivalenzklassen wird durch die Verknüpfung*

$$[x_1,y_1]\cdot[x_2,y_2] := [x_1\cdot x_2, y_1\cdot y_2]$$

zu einer abelschen Gruppe, der Grothendieck-Gruppe.

BEWEIS: Wohldefiniertheit: Für $[x_1,y_1] = [\widetilde{x_1},\widetilde{y_1}]$ ergibt sich $x_1\widetilde{y_1}z = \widetilde{x_1}y_1z$ mit einem $z\in M$. Daraus folgt $x_1x_2\widetilde{y_1}y_2z = \widetilde{x_1}x_2y_1y_2z$, also $[x_1x_2,y_1y_2] = [\widetilde{x_1}x_2,\widetilde{y_1}y_2]$. Genauso ist für $[x_2,y_2] = [\widetilde{x_2},\widetilde{y_2}]$ die Gleichheit $[x_1\widetilde{x_2},y_1\widetilde{y_2}] = [x_1\widetilde{x_2},y_1\widetilde{y_2}]$ gegeben. Assoziativität:

$$\begin{aligned}([x_1,y_1][x_2,y_2])[x_3,y_3] &= [x_1x_2,y_1y_2][x_3y_3] = [(x_1x_2)x_3,(y_1y_2)y_3] = [x_1(x_2x_3),y_1(y_2y_3)]\\ &= [x_1,y_1][x_2x_3,y_2y_3] = [x_1,y_1]([x_2,y_2][x_3,y_3]).\end{aligned}$$

Kommutativität:

$$[x_1,y_1][x_2,y_2] = [x_1x_2,y_1y_2] = [x_2x_1,y_2y_1] = [x_2,y_2][x_1,y_1].$$

Neutrales Element ist die Äquivalenzklasse $[x,x]$:

$$[x,x][x_1,y_1] = [xx_1,xy_1] = [x_1,y_1],$$

da $xx_1y_1z = x_1xy_1z$. Inverses Element ist $[x_1,y_1]^{-1} := [y_1,x_1]$:

$$[x_1,y_1][y_1x_1] = [x_1y_1,y_1x_1] = [x_1y_1,x_1y_1].$$ □

Wie werden nun sehen, wie wir die Halbgruppe in die Gruppe einbetten können.

Satz 42: *Sei M eine Halbgruppe und G die zugehörige Grothendieck-Gruppe. Dann ist die Abbildung $f\colon M \to G\colon x \mapsto [x^2, x]$ ein Halbgruppenhomomorphismus, d. h. es gilt $f(xy) = f(x)f(y)$ für alle $x, y \in M$. Es ist f genau dann injektiv, wenn für alle $x, y, z \in M$ gilt $xz = yz \Leftrightarrow x = y$.*

BEWEIS: Es gilt

$$f(xy) = [(xy)^2, xy] = [x^2y^2, xy] = [x^2, x][y^2, y] = f(x)f(y).$$

Sei nun f injektiv und $x, y, z \in M$ mit $xz = yz$. Dann folgt

$$f(x) = [x^2, x] = [x^2z, xz] = [xz, z] = [yz, z] = [y^2z, yz] = f(y)$$

und damit $x = y$. Gilt umgekehrt für alle $x, y, z \in M$ die Äquivalenz $xz = yz \Leftrightarrow x = y$, so folgt aus $f(x) = f(y)$, also $[x^2, x] = [y^2, y]$, direkt $x^2yz = y^2xz$. Mit $\widetilde{z} := xyz$ folgt mit der Voraussetzung die Behauptung. □

Ist f nun injektiv, so kann man M mit $f(M)$ identifizieren, da $M \simeq f(M)$. Wir werden bei der Konstruktion der ganzen Zahlen sehen, dass dies in unserem Fall erfüllt ist.

4.3 Ringe

4.3.1 Elementare Eigenschaften

Wir haben nun einen guten Überblick über die einfachsten Eigenschaften von Gruppen gewonnen. Ist auf einer Gruppe noch eine zweite Verknüpfung gegeben, welche sich mit der anderen verträgt, so hat man einen Ring vorliegen. Genauer gilt:

Definition 30 (Ring): *Seien R eine Menge und $+, \cdot$ innere Verknüpfungen auf R. Das Tripel $(R, +, \cdot)$ heißt* Ring*, wenn gilt:*

(i) $(R, +)$ *ist eine abelsche Gruppe.*

(ii) $(R, \cdot)$ *ist ein Monoid*[3]*.*

(iii) Für alle $r, s, t \in R$ gelten die Distributivgesetze

$$r \cdot (s + t) = r \cdot s + r \cdot t, \qquad (r + s) \cdot t = r \cdot t + s \cdot t.$$

Der Ring heißt kommutativ*, wenn $\cdot$ kommutativ ist.*

[3]Manchmal wir nur verlangt, dass $(R, \cdot)$ eine Halbgruppe ist. Der hier definierte Ring heißt dann „Ring mit 1“.

Man bezeichnet nun das neutrale Element bzgl. $+$ mit 0 und nennt es das *Nullelement*. Entsprechend ist das neutrale Element bzgl. $\cdot$ die 1 und heißt *Einselement*. Es sei ausdrücklich darauf hingewiesen, dass trotz der verschiedenen Bezeichnungen in Ringen $0 = 1$ gelten kann wie im Ring $(\{0\}, +, \cdot)$[4]. Weiter gilt die Regel, dass $\cdot$ stärker bindet als $+$. Wir haben dies bereits in der Definition benutzt. Wir müssen nun wieder zunächst die wichtigsten Rechenregeln herausarbeiten.

Satz 43: *Sei R ein Ring. Dann gilt für alle $r, s \in R$:*

(i) $0 \cdot r = r \cdot 0 = 0$

(ii) $-(r \cdot s) = (-r) \cdot s = r \cdot (-s)$

(iii) $(-r) \cdot (-s) = r \cdot s$.

BEWEIS:

(i) Aus $0 = 0 + 0$ folgt $0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$. Addition von $-(0 \cdot r)$ ergibt

$$0 = (0 \cdot r + 0 \cdot r) - 0 \cdot r = 0 \cdot r + (0 \cdot r - 0 \cdot r) = 0 \cdot r + 0 = 0 \cdot r.$$

Analog für $r \cdot 0 = 0$.

(ii) Es ist $0 = r \cdot 0 = r \cdot (s - s) = r \cdot s + r \cdot (-s)$. Addition von $-(r \cdot s)$ führt auf

$$-(r \cdot s) = -(r \cdot s) + (r \cdot s + r \cdot (-s)) = (-(r \cdot s) + r \cdot s) + r \cdot (-s) = 0 + r \cdot (-s) = r \cdot (-s).$$

Entsprechend für $-(r \cdot s) = (-r) \cdot s$.

(iii) Es gilt $(-r) \cdot (-s) = -(r \cdot (-s)) = -(-(r \cdot s)) = r \cdot s$. □

Ähnlich wie bei den Gruppen trifft man die

Definition 31 (Unterring): *Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$ eine Teilmenge. Man nennt S einen* Unterring *von R, wenn S mit der Einschränkung von $+$ und $\cdot$ auf S ein Ring ist.*

Wir betrachten dazu ein Beispiel. Wir führen auf $\mathbb{Z} \times \mathbb{Z}$ die komponentenweise Addition und Multiplikation durch $(r_1, r_2) + (s_1, s_2) := (r_1 + s_1, r_2 + s_2)$ und $(r_1, r_2) \cdot (s_1, s_2) := (r_1 \cdot s_1, r_2 \cdot s_2)$ ein. Man überlegt sich dann leicht, dass $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ ein Ring ist mit Nullelement $(0, 0)$, dem zu (r_1, r_2) inversen Element $-(r_1, r_2) := (-r_1, -r_2)$, sowie dem Einselement $(1, 1)$. Es ist offenbar $\mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z}$ bzgl. der eingschränkten Verknüpfungen ein Ring. Es ist jedoch das Einselement $(1, 0) \neq (1, 1)$! Da man häufig das Einselement beibehalten will, legt man fest:

Definition 32 (Unitärer Unterring): *Eine Teilmenge $S \subseteq R$ eines Ringes R heißt* unitärer Unterring*, wenn gilt:*

(i) $0, 1 \in S$

[4] In der Tat ist jeder Ring mit $0 = 1$ der Nullring, denn aus $r \in R$ folgt $r = 1r = 0r = 0$.

(ii) $r, s \in S \Rightarrow r - s, r \cdot s \in S$.

Es gibt noch eine weitere wichtige Teilmenge von Ringen, welche besonders bei den Teilbarkeitsuntersuchungen in Abschnitt 4.3.3 eine Rolle spielen wird.

Definition 33 (Ideal): *Sei R ein Ring und $I \subseteq R$ eine Teilmenge. Man nennt I ein* Ideal, *wenn gilt:*

(i) $(I, +)$ *ist eine Untergruppe von* $(R, +)$.

(ii) Für alle $r \in R$ *und alle* $s \in I$ *ist* $rs \in I$ *und* $sr \in I$.

Analog wie bei Gruppen will man auch für Ringe sicherstellen, dass eine Ordnungsrelation die beiden Verknüpfungen respektiert.

Definition 34 (Geordneter Ring): *Ein kommutativer Ring* $(R, +, \cdot)$ *heißt* geordnet, *wenn auf* R *eine Ordnungsrelation definiert ist, so dass* $(R, +)$ *eine geordnete Gruppe ist, und dass für alle* $r, s, t \in R$ *gilt* $r \leq s \wedge t \geq 0 \Rightarrow rt \leq ts$.

Für geordnete Ringe gilt der folgende

Satz 44: *Sei R ein geordneter Ring mit $r, s, t \in R$. Dann gilt:*

(i) $r \leq s \Leftrightarrow r + t \leq s + t$

(ii) $r < s \Leftrightarrow r + t < s + t$

(iii) $r \leq s \Leftrightarrow -s \leq -r$

(iv) $r \leq s \wedge t \leq 0 \Rightarrow rt \geq st$

(v) $r \geq 0 \wedge s \geq 0 \Rightarrow r + s \geq 0, rs \geq 0$.

BEWEIS:

(i) Die Hinrichtung ergibt sich daraus, dass $(R, +)$ eine geordnete Gruppe ist. Die Rückrichtung erhält man wegen $r = r + t + (-t) \leq s + t + (-t) = s$.

(ii) Bekommt man aus (i) durch Ausschluss des Falls $r = s$.

(iii) Die Hinrichtung folgt aus $-s = r + (-r) + (-s) \leq s + (-r) + (-s) = -r$. Die Rückrichtung folgt mit $-(-r) = r$.

(iv) Nach (iii) ist $-t \geq 0$ und weiter $-rt = r(-t) \leq s(-t) = -st$ sowie $st \leq rt$.

(v) Es ist $r + s \geq 0 + s = s \geq 0$ und $rs \geq 0s = 0$. □

4.3.2 Homomorphismen

Wir werden nun kurz die wichtigsten Ergebnisse des letzten Abschnitts über Gruppen auf Ringe übertragen. Wir beginnen mit der

Definition 35 (Ringhomomorphismus): *Seien R und S Ringe, $f\colon R \to S$ eine Abbildung. f heißt* Homomorphismus *genau dann, wenn gilt:*

(i) $f(r+s) = f(r) + f(s)$

(ii) $f(r \cdot s) = f(r) \cdot f(s)$

für alle $r, s \in R$.

Es folgt nun wie bei Gruppen, dass $f(0_R) = 0_S$ ist. Es muss jedoch nicht $f(1_R) = 1_S$ sein. Beim Beweis von Satz 28.(i) wurde nämlich die Existenz von inversen Elementen benutzt, welche bei Ringen bzgl. $\cdot$ nicht gegeben sein muss. Gilt trotzdem $f(1_R) = 1_S$ so heißt der Homomorphismus *unitär*.

Satz 45: *Sei $f\colon R \to S$ ein Homomorphismus und $M \subseteq R$ sowie $N \subseteq S$ eine Teilmenge. Dann gilt:*

(i) Ist M Unterring von R, so ist $f(M)$ Unterring von S.

(ii) Ist N Unterring von S, so ist $f^{-1}(N)$ Unterring von R.

(iii) Ist N ein Ideal von S, so ist $f^{-1}(N)$ ein Ideal von R.

(iv) $\operatorname{Kern} f$ ist ein Ideal von R.

(v) Ist f surjektiv und M ein Ideal von R, so ist $f(M)$ ein Ideal von S.

BEWEIS:

(i) Seien $f(r), f(s) \in f(M)$ mit $r, s \in M$. Es folgt $f(r) - f(s) = f(r-s) \in f(M)$, da $r - s \in M$. Weiter ist $f(r)f(s) = f(rs) \in f(M)$, weil $rs \in M$.

(ii) Seien $r, s \in f^{-1}(N)$. Dann folgt $f(r) - f(s) = f(r-s) \in N$, also $r - s \in f^{-1}(N)$. Ebenso ist $f(r)f(s) = f(rs) \in N$, und somit $rs \in f^{-1}(N)$.

(iii) Der erste Teil ist analog zu (ii). Sei nun $s \in f^{-1}(N)$ und $r \in R$ beliebig. Es gilt $f(rs) = f(r)f(s) \in N$, also $rs \in f^{-1}(N)$. Genauso folgt $f(sr) \in f^{-1}(N)$.

(iv) Folgt direkt mit (iii), denn $\{0\}$ ist ein Ideal von S.

(v) Sei $s \in S$ und $r \in M$. Da f surjektiv ist, existiert ein $t \in R$ mit $f(t) = s$. Daraus ergibt sich $sf(r) = f(t)f(r) = f(tr) \in f(M)$. Entsprechend für $f(rt) \in f(M)$. □

Wir betrachten nun den Homomorphismus $f\colon \mathbb{Z} \to R\colon m \mapsto m{\cdot}1$, wobei die Multiplikation eines Ringelements mit einer ganzen Zahl wie bei Gruppen definiert ist. Sein Kern ist eine Untergruppe von $(\mathbb{Z}, +)$, hat also nach Satz 37 die Form $n\mathbb{Z}$ mit $n \in \mathbb{N}$. Man nennt n die *Charakteristik* von R und schreibt $\operatorname{Char} R := n$. Offenbar ist $\operatorname{Char}\mathbb{Z} = \operatorname{Char}\mathbb{Q} = \operatorname{Char}\mathbb{R} = 0$.

Definition 36 (Restklasse): *Sei R ein Ring und I ein Ideal von R. Dann nennt man die Menge $r + I$* Restklasse von r modulo I. *Die Menge aller Restklassen wird mit R/I bezeichnet.*

Natürlich gilt der

Satz 46: *Die Menge aller Restklassen wird bzgl. der üblichen Mengenverknüpfungen zum Ring, dem* Restklassenring.

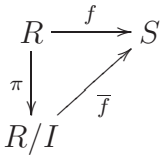
BEWEIS: Das Nullelement ist die Restklasse $0+I = I$, das Einselement ist $1+I$. Das Übrige ist klar. □

Man führt nun wieder einen *kanonischen Epimorphismus* $\pi\colon R \to R/I\colon r \mapsto r + I$ ein. Es ist erneut nicht nur jeder Kern ein Ideal, sondern umgekehrt definiert jedes Ideal einen Homomorphismus, dessen Kern es ist. Dies sieht man an der Äquivalenz

$$r \in \operatorname{Kern}\pi \Leftrightarrow r + I = I \Leftrightarrow r \in I.$$

In Abschnitt 4.6 werden wir eine interessante Anwendung von Restklassenringen kennenlernen. Wir wenden uns nun wieder Isomorphieüberlegungen zu und beginnen mit dem

Satz 47 (Homomorphiesatz für Ringe): *Sei $f\colon R \to S$ ein Epimorphismus mit $I := \operatorname{Kern} f$. Dann ist die Abbildung $\overline{f}\colon R/I \to S\colon r + I \mapsto f(r)$ ein Isomorphismus, also $R/I \simeq S$ und*



kommutiert.

BEWEIS: Da f bzgl. $+$ ein Gruppenhomomorphismus ist, ist nach Satz 33 $\overline{f}$ ein Gruppenisomorphismus. Wir müssen nun nur noch die Verträglichkeit mit $\cdot$ prüfen. Diese ist wegen

$$\overline{f}((r + I)(s + I)) = \overline{f}(rs + I) = f(rs) = f(r)f(s) = \overline{f}(r + I)\overline{f}(s + I)$$

gegeben. □

Satz 48 (Erster Isomorphiesatz für Ringe): *Sei R ein Ring, S ein Unterring von R und I ein Ideal von R. Dann gilt $(S + I)/I \simeq S/(S \cap I)$.*

BEWEIS: Betrachte den Epimorphismus $f\colon S \to (S + I)/I\colon s \mapsto s + I$. Offenbar ist $\operatorname{Kern} f = S \cap I$. Die Isomorphie erhält man direkt aus Satz 47. □

Satz 49 (Zweiter Isomorphiesatz für Ringe): *Seien R ein Ring und I, J Ideale von R mit $J \subseteq I$. Dann ist I/J ein Ideal von R/J und $(R/J)/(I/J) \simeq R/I$.*

BEWEIS: Da $R \to R/J : r \mapsto r + J$ surjektiv ist, folgt mit Satz 45.(v), dass I/J ein Ideal von R/J ist. Betrachtet man nun den Epimorphismus $f : R/J \to R/I : r + J \mapsto r + I$, so gilt $\operatorname{Kern} f = I/J$ und mit Satz 47 die Behauptung. □

4.3.3 Teilbarkeit

Wir können leider in dieser Einführung die Teilbarkeitstheorie in Ringen nicht erschöpfend behandeln. Es soll aber versucht werden, einen kleinen Überblick über die Methoden und Begriffe zu geben, die mit diesem Thema verbunden sind. Die Teilbarkeit in Ringen ist eng mit den Idealen verknüpft. Wir entwickeln deshalb beide Theorien parallel. Dabei beschränken wir uns hauptsächlich auf kommutative Ringe.

Nimmt man zu der Addition noch die gewöhnliche Multiplikation hinzu, so wird aus der Untergruppe $(n\mathbb{Z}, +)$ von $(\mathbb{Z}, +, \cdot)$ ein Ideal. Das erste Problem wird offensichtlich, wenn wir als Beispiel den Restklassenring $\mathbb{Z}/6\mathbb{Z}$ betrachten[5]. Es ist nämlich $(2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 6 + 6\mathbb{Z} = 6\mathbb{Z}$, aber $2 + 6\mathbb{Z} \neq 6\mathbb{Z}$ und $3 + 6\mathbb{Z} \neq 6\mathbb{Z}$. Dies führt uns zu der

Definition 37 (Nullteiler): *Ein Element $r \in R$ heißt* Nullteiler*, wenn ein $s \in R\backslash\{0\}$ existiert mit $rs = 0$ oder $sr = 0$.*

In unserem Beispiel ist sowohl $2 + 6\mathbb{Z}$ als auch $3 + 6\mathbb{Z}$ ein Nullteiler. Außer im Fall $R = \{0\}$ ist 0 immer ein Nullteiler. Häufig ist es wichtig zu wissen, dass außer 0 keine weiteren Nullteiler existieren. Man trifft daher die

Definition 38 (Integritätsring): *Sei $\{0\} \neq R$ ein Ring. Es heißt R* nullteilerfrei*, wenn 0 der einzige Nullteiler in R ist. R heißt* Integritätsring*, wenn R nullteilerfrei und kommutativ ist.*

Da für einen Ring $(R, +, \cdot)$ nur bekannt ist, dass $(R, \cdot)$ ein Monoid ist, existieren nicht für alle $r \in R$ Inverse bzgl. $\cdot$.

Definition 39 (Einheit): *Ein Element $r \in R$ heißt* Einheit*, wenn ein $r^{-1} \in R$ existiert mit $rr^{-1} = r^{-1}r = 1$. Die Menge R^* aller Einheiten von R wird* Einheitengruppe *von R genannt.*

Offensichtlich gilt also der

Satz 50: *Die Einheitengruppe R^* eines Ringes R bildet bzgl. $\cdot$ eine Gruppe.*

BEWEIS: Wegen $1 \in R^*$ ist $R^* \neq \emptyset$. Die Assoziativität und die Existenz des neutralen Elements sind damit klar. Per Definition existiert auch für jedes Element von R^* ein Inverses. Wir müssen nur noch die Abgeschlossenheit zeigen. Seien dazu $r, s \in R^*$. Es ist zu zeigen, dass rs ein Inverses in R^* besitzt. Wir wählen dazu $(rs)^{-1} := s^{-1}r^{-1}$. Es folgt $(rs)(rs)^{-1} = rss^{-1}r^{-1} = 1$ und $(rs)^{-1}(rs) = s^{-1}r^{-1}rs = 1$, also $s^{-1}r^{-1} \in R^*$. □

[5] Es sei darauf hingewiesen, dass $6\mathbb{Z}$ kein Ring ist, da das Einselement fehlt!

Im Ring $(\mathbb{Z}, +, \cdot)$ sind 1 und -1 die einzigen Einheiten. Im Ring $(\mathbb{R}, +, \cdot)$ ist dagegen ganz $\mathbb{R} \setminus \{0\}$ die Einheitengruppe.

Satz 51: *Die Elemente der Einheitengruppe sind keine Nullteiler.*

BEWEIS: Sei $r \in R^*$ und $s \in R$. Angenommen $rs = 0$. Dann folgt

$$s = 1s = (r^{-1}r)s = r^{-1}(rs) = r^{-1}0 = 0. \qquad \square$$

Wie schon angekündigt müssen wir uns nun näher mit Idealen beschäftigen. Wir beginnen mit der

Definition 40 (Hauptideal): *Sei R ein kommutativer Ring und $a \in R$. Dann heißt $(a) := \{ ra \in R \mid a \in R \}$ das von a erzeugte* Hauptideal.

Natürlich gilt der

Satz 52: *Jedes Hauptideal ist ein Ideal.*

BEWEIS: Seien $r, s \in R$. Dann folgt $ra - sa = (r - s)a \in (a)$. Weiter ist $s(ra) = (sr)a \in (a)$. $\square$

Wir können nun mit unserem eigentlichen Thema, also der Teilbarkeit in Ringen, anfangen. Wir beginnen mit der

Definition 41 (Teiler): *Sei R ein Integritätsring. Sind $a, b \in R$, so schreibt man $a|b$, wenn ein $c \in R$ existiert mit $ac = b$. Man sagt a ist ein* Teiler *von b. Es heißen a und b* assoziiert*, geschrieben $a \sim b$, wenn eine Einheit $e \in R^*$ existiert mit $ae = b$.*

Satz 53: *Sei R ein Integritätsring. Dann gilt:*

(i) *$\sim$ ist eine Äquivalenzrelation auf R.*

(ii) *$a \sim b \Leftrightarrow a|b \wedge b|a$.*

(iii) *Aus $a_1 \sim a_2$ und $b_1 \sim b_2$ folgt $a_1|b_1 \Leftrightarrow a_2|b_2$.*

BEWEIS:

(i) Reflexivität ist klar ($e = 1$). Symmetrie: Sei $a \sim b$, also $ae = b$ mit $e \in R^*$. Daraus folgt $a = be^{-1}$ und somit $b \sim a$. Transitivität: Sei $a \sim b$ und $b \sim c$, d. h. $ae = b$ und $bf = c$ mit $e, f \in R^*$. Dann folgt $c = bf = (ae)f = a(ef)$, also $a \sim c$.

(ii) „$\Rightarrow$“: Folgt aus Symmetrie von $\sim$, siehe (i).
„$\Leftarrow$“: Sei $ac = b$ und $bd = a$ mit $c, d \in R$. Daraus ergibt sich $bdc = ac = b$, also $b(dc - 1) = 0$. Da R Integritätsring ist, folgt $b = 0$ oder $dc - 1 = 0$ bzw. $dc = 1$. Ist $b = 0$, so ist auch $a = bd = 0$, also $a \sim b$. Ist $dc = 1$, so ist c Einheit und erneut $a \sim b$.

(iii) Sei $a_1 \sim a_2$ und $b_1 \sim b_2$.
„$\Rightarrow$“: Es gelte $a_1|b_1$, d. h. $a_1 c = b_1$ mit $c \in R$. Nach Voraussetzung gilt $a_1 = a_2 e$ und $b_1 f = b_2$ mit $e, f \in R^*$. Dann folgt $b_2 = b_1 f = a_1 cf = a_2 ecf$, also $a_2|b_2$.
„$\Leftarrow$“: Analog. □

Der Zusammenhang zu den Hauptidealen wird hergestellt durch den

Satz 54: *Sei R ein Integritätsring mit $a, b \in R$. Dann sind äquivalent:*

(i) $a|b$

(ii) $(b) \subseteq (a)$.

BEWEIS:
„(i) $\Rightarrow$ (ii)“: Sei $c \in R$ mit $ac = b$. Dann folgt $(b) = bR = acR \subseteq aR = (a)$.
„(ii) $\Rightarrow$ (i)“: Sei nun $(b) \subseteq (a)$. Dann ist insbesondere $b \in (a)$ und damit $b = ra$ für ein $r \in R$. □

Daraus folgt sofort der

Satz 55: *Sei R ein Integritätsring und $a, b \in R$. Es sind äquivalent:*

(i) $a \sim b$

(ii) $(a) = (b)$.

BEWEIS: Ist $a \sim b$, so gilt nach Satz 53.(ii) $a|b$ und $b|a$. Daraus folgt nach Satz 54 $(b) \subseteq (a)$ und $(a) \subseteq (b)$, also $(a) = (b)$. Gilt umgekehrt $(a) = (b)$, so folgt $a|b$ und $b|a$ und somit $a \sim b$. □

Wir stellen nun die wichtigsten Rechenregeln zusammen.

Satz 56: *Sei R ein Integritätsring. Dann gilt für alle $a, b, c, d \in R$ und $e \in R^*$:*

(i) $a|a$, $e|a$.

(ii) $a|e \Leftrightarrow a \in R^*$, $0|a \Rightarrow a = 0$.

(iii) *Aus* $a|b$ *und* $b|c$ *folgt* $a|c$.

(iv) *Aus* $a|b$ *und* $c|d$ *folgt* $ac|bd$.

(v) *Aus* $a|b$ *folgt* $a|(bc)$.

(vi) *Aus* $a|b$ *und* $a|c$ *folgt* $a|(b + c)$.

BEWEIS:
(i) $a = 1a \Rightarrow a|a$. Es existiert ein $f \in R$ mit $ef = 1$. Daraus folgt $(ef)a = 1a = a$, also $e|a$.

(ii) „⇒“: Es existieren $f, g \in R$ mit $ef = 1$ und $ag = e$. Also folgt $a(gf) = (ag)f = ef = 1$, also $a \in R^*$.
„⇐“: Satz 50.
Es gelte nun $0|a$. Dann gibt es ein $f \in R$ mit $0f = a = 0$.

(iii) Es existieren $f, g \in R$ mit $af = b$ und $bg = c$. Dann folgt $c = bg = (af)g = a(fg)$, also $a|c$.

(iv) Es gibt $f, g \in R$ mit $af = b$ und $cg = d$. Daraus ergibt sich $bd = (af)(cg) = (ac)(fg)$, also $ac|bd$.

(v) Es gibt $f \in R$ mit $af = b$. Dann gilt $afc = bc$, also $a|bc$.

(vi) Es existieren $f, g \in R$ mit $af = b$ und $ag = c$. Daraus folgt $b+c = af+ag = a(f+g)$, also $a|(b + c)$. □

Wir kommen nun wieder zurück zu den Idealen.

Definition 42 (Primideal): *Sei R ein kommutativer Ring. Ein Ideal $P \subseteq R$ heißt* Primideal, *wenn für alle $r, s \in R$ gilt: $rs \in P \Rightarrow r \in P \vee s \in P$.*

Für Primideale gilt der

Satz 57: *Sei R ein kommutativer Ring und $P \subseteq R$ ein Ideal. Dann sind äquivalent:*

(i) R/P ist Integritätsring.

(ii) P ist Primideal.

BEWEIS:
„(i) ⇒ (ii)“: Seien $r, s \in R$ mit $rs \in P$. Es gilt $(r + P)(s + P) = rs + P = P$. Da R/P Integritätsring ist folgt $r + P = P$ oder $s + P = P$ und damit $r \in P$ oder $s \in P$.
„(ii) ⇒ (i)“: Seien $r + P, s + P \in R/P$ mit $P = (r + P)(s + P) = rs + P$. Dann folgt $rs \in P$, und da P Primideal ist $r \in P$ oder $s \in P$. Also ist $r + P = P$ oder $s + P = P$ und damit R/P Integritätsring. □

Wegen $R \simeq R/(0)$ und Aufgabe 24 folgt nun sofort, dass R genau dann Integritätsring ist, wenn (0) Primideal ist.

Das wichtigste Ziel der Teilbarkeitslehre ist es, jedes Element des Rings so weit es geht zu faktorisieren. Wir beginnen dazu mit der

Definition 43: *Sei R ein Integritätsring. Ein Element $p \in R$ heißt* Primelement *oder* prim, *wenn $p \neq 0$, $p \notin R^*$ und $p|ab \Rightarrow p|a \vee p|b$. Ein Element $q \in R$ heißt* irreduzibel, *wenn $q \neq 0$, $q \notin R^*$ und $q = ab \Rightarrow a \in R^* \vee b \in R^*$.*

Im Gegensatz zur bekannten Situation in $\mathbb{Z}$ ist in einem beliebigen Integritätsring nicht jedes irreduzible Element auch prim. Es gilt aber der

Satz 58: *Ist $p \in R$ prim, so ist p auch irreduzibel.*

BEWEIS: Sei $p \in R$ prim mit $p = ab$. Dann folgt insbesondere $p|ab$ und somit $p|a$ oder $p|b$. Wir können o. E. annehmen $p|a$. Dann existiert ein $c \in R$ mit $pc = a$. Daraus ergibt sich $pcb = ab = p$, also $p(cb - 1) = 0$. Da R Integritätsring ist, folgt $cb - 1 = 0$, also $cb = 1$ und $b \in R^*$. □

Einen Zusammenhang zwischen den irreduziblen Elementen und Primidealen gibt der

Satz 59: *Sei R ein Integritätsring und $p \in R$ mit $p \neq 0$, $p \notin R^*$. Ist (p) ein Primideal, so ist p irreduzibel.*

BEWEIS: Sei $p = ab$. Dann folgt $ab \in (p)$, und da (p) Primideal ist $a \in (p)$ oder $b \in (p)$. Sei o. E. $a \in (p)$. Dann existiert ein $r \in R$ mit $a = pr = abr$. Daraus folgt $a(br - 1) = 0$. Da $p \neq 0$ ist auch $a \neq 0$, und weil R Integritätsring ist ergibt sich $br = 1$. Also gilt $b \in R^*$. □

Zum Abschluss geben wir noch die

Definition 44: *Ein Integritätsring R heißt* Gauß'scher Ring, faktorieller Ring *oder* ZPE-Ring[6]*, wenn jedes Element $a \in R$ eine Darstellung der Form $a = p_1 \cdots p_n$ mit p_i prim besitzt. Diese Darstellung heißt* Primfaktorzerlegung.

Leider können wir hier nicht der Frage nachgehen, unter welchen Umständen ein vorgegebener Ring faktoriell ist. Wir werden aber in Satz 107 sehen, dass eine Primfaktorzerlegung, wenn sie existiert, stets eindeutig ist (bis auf Assoziiertheit).

4.4 Moduln

Wir begegnen nun unserer erster algebraischen Struktur mit einer äußeren Verknüpfung. Gewissermaßen ist ein Modul die Vorstufe eines Vektorraums. Da Moduln für uns relativ uninteressant sind, werden wir nur einen ganz kurzen Blick auf sie werfen.

Definition 45 (Modul): *Sei $(R, +, \cdot)$ ein kommutativer Ring, $(G, +)$ eine abelsche Gruppe und $\cdot : R \times G \to G$ eine äußere Verknüpfung. Das Tripel $((R, +, \cdot), (G, +), \cdot)$ heißt* R-Modul *oder Modul über R, wenn für alle $r, s \in R$ und $g, h \in G$ gilt*

(i) $(r + s)g = rg + sg$

(ii) $r(g + h) = rg + rh$

(iii) $(rs)g = r(sg)$

(iv) $1g = g$.

[6] Zerlegung in Primelemente eindeutig

Es sei darauf hingewiesen, dass wir nur der Übersichtlichkeit halber die Symbole $+$ in R und G sowie die innere Verknüpfung $\cdot$ in R und die äußere Verknüpfung $\cdot$ nicht unterscheiden. Grundsätzlich sind dies natürlich verschiedene Abbildungen!

Ein triviales Beispiel für Moduln sind Ringe, denn jeder Ring ist Modul über sich selbst. Weiter haben wir schon oft benutzt, dass man für jede Gruppe eine Verknüpfung mit Elementen aus $\mathbb{Z}$ definieren kann. In unserer neuen Sprechweise wird damit jede abelsche Gruppe zu einem $\mathbb{Z}$-Modul. Tatsächlich ist dies auch die einzige mit den Axiomen verträgliche Art, eine abelsche Gruppe zu einem $\mathbb{Z}$-Modul zu machen. Umgekehrt kann man jeden $\mathbb{Z}$-Modul als abelsche Gruppe auffassen.

4.5 Schiefkörper

Ebenfalls nur ganz kurz werden wir auf Schiefkörper eingehen.

Definition 46 (Schiefkörper): *Ein Ring $(R, +, \cdot)$ heißt* Schiefkörper*, wenn er aus mindestens zwei Elementen besteht und für alle $r \in R \setminus \{0\}$ ein inverses Element bzgl. $\cdot$ existiert.*

Demnach ist R genau dann ein Schiefkörper, wenn $(R, +)$ eine abelsche Gruppe ist und $(R \setminus \{0\}, \cdot)$ eine Gruppe. Die wichtigsten Rechenregeln für Schiefkörper liefert der

Satz 60: *Sei R ein Schiefkörper mit $r, s \in R$. Dann gilt*

(i) $0 \neq 1$.

(ii) $rs = 0 \Leftrightarrow r = 0 \vee s = 0$.

BEWEIS:

(i) Sei $0 = 1$ und $r \in R$. Dann folgt $r = 1r = 0r = 0$, also $R = \{0\}$. Widerspruch.

(ii) „$\Rightarrow$“: Es gelte $rs = 0$ und $r \neq 0$. Dann existiert $r^{-1} \in R$ mit

$$0 = r^{-1}0 = r^{-1}(rs) = (r^{-1}r)s = 1s = s.$$

„$\Leftarrow$“: Satz 43.(i). □

Wegen (ii) ist jeder Schiefköper nullteilerfrei. Die Umkehrung gilt nur bedingt. Es ist z. B. $\mathbb{Z}$ ein nullteilerfreier Ring, der kein Schiefkörper ist. Es gilt aber der

Satz 61: *Jeder endliche nullteilerfreie Ring $R \neq \{0\}$ ist ein Schiefkörper.*

BEWEIS: Betrachte die Abbildung $f_a \colon R \to R \colon r \mapsto ar$ mit $a \in R \setminus \{0\}$. Wir zeigen, dass sie injektiv ist. Sei dazu $f_a(r) = f_a(s)$, also $ar = as$. Daraus folgt $a(r - s) = 0$, und da R nullteilerfrei ist folgt $r = s$. Da R endlich ist, ist f_a dann auch surjektiv. Da schon $f_a(0) = 0$ ist folgt $f_a(R \setminus \{0\}) = R \setminus \{0\}$. Insbesondere gibt es ein $a^{-1} \in R \setminus \{0\}$ mit $aa^{-1} = 1$. Da a in der Definition von f_a frei gewählt war, gibt es zu jedem $a \in R \setminus \{0\}$ ein $a^{-1} \in R \setminus \{0\}$ mit $aa^{-1} = 1$. Damit ist $R \setminus \{0\}$ eine Gruppe und R ein Schiefkörper. □

4.6 Körper

4.6.1 Elementare Eigenschaften

Auf Körper gehen wir nun wieder ausführlich ein.

Definition 47 (Körper): *Ein Schiefkörper $(K, +, \cdot)$ heißt* Körper*, wenn $\cdot$ kommutativ ist.*

Es ist ein äußerst faszinierendes Ergebnis der Algebra, dass ein Schiefkörper mit endlich vielen Elementen automatisch ein Körper ist. Wir können diese Aussage leider in diesem Rahmen nicht beweisen, halten das Ergebnis aber trotzdem fest im

Satz 62 (Satz von Wedderburn): *Jeder endliche Schiefkörper ist ein Körper.*

Ausschließlich für Körper (und hier auch nicht für alle) hat sich die Schreibweise

$$\frac{x}{y} := xy^{-1}$$

eingebürgert. Aus Platzgründen werden wir aber weitgehend auf die Bruchschreibweise verzichten. Wie immer gibt es nun zunächst ein paar Rechenregeln.

Satz 63: *Sei K ein Körper mit $x, y, u, v \in K$. Dann gilt:*

(i) $\frac{x}{1} = x$.

(ii) $\frac{x}{x} = 1$ *für* $x \neq 0$.

(iii) $\frac{x}{y} \cdot \frac{u}{v} = \frac{x \cdot u}{y \cdot v}$ *für* $y, v \neq 0$.

(iv) $\frac{x}{y} = x\frac{1}{y}$ *für* $y \neq 0$.

(v) $\frac{xy}{xv} = \frac{y}{v}$ *für* $x, v \neq 0$.

(vi) $\frac{-x}{y} = \frac{x}{-y} = -\frac{x}{y}$ *für* $y \neq 0$.

(vii) $\frac{x}{y} \pm \frac{u}{v} = \frac{xv \pm yu}{yv}$ *für* $y, v \neq 0$.

(viii) $\frac{0}{x} = 0$ *für* $x \neq 0$.

(ix) $\left(\frac{x}{y}\right)^{-1} = \frac{y}{x}$ *für* $x, y \neq 0$.

BEWEIS:

(i) Klar, da $1 = 1^{-1}$.

(ii) Auch klar.

(iii) Es ist

$$(yv)\left(\frac{x}{y}\frac{u}{v}\right) = \left(y\frac{x}{y}\right)\left(v\frac{u}{v}\right) = (yy^{-1}x)(vv^{-1}u) = xu.$$

Multiplikation mit $(yv)^{-1}$ ergibt

$$\frac{x}{y}\frac{u}{v} = (yv)^{-1}(xu) = \frac{xu}{yv}.$$

(iv) Folgt aus

$$x\frac{1}{y} = x(1y^{-1}) = xy^{-1} = \frac{x}{y}.$$

(v) Wegen

$$\frac{xy}{xv} = \frac{x}{x}\frac{y}{v} = 1\frac{y}{v} = \frac{y}{v}.$$

(vi) Ergibt sich aus

$$\frac{-x}{y} = \frac{(-1)x}{1y} = \frac{-1}{1}\frac{x}{y} = (-1)\frac{x}{y} = -\frac{x}{y}$$

und

$$\frac{x}{-y} = \frac{1x}{(-1)y} = \frac{1}{-1}\frac{x}{y} = \frac{(-1)}{(-1)(-1)}\frac{x}{y} = \frac{-1}{1}\frac{x}{y} = -\frac{x}{y}.$$

(vii) Es ist

$$\frac{x}{y} \pm \frac{u}{v} = \frac{xv}{yv} \pm \frac{yu}{yv} = (xv)\frac{1}{yu} \pm (yu)\frac{1}{yv} = (xv \pm yu)\frac{1}{yv} = \frac{xv \pm yu}{yv}.$$

(viii) Klar.

(ix) Wegen

$$\frac{x}{y}\frac{y}{x} = \frac{xy}{yx} = \frac{xy}{xy} = 1.$$

□

Natürlich werden wir auch hier wieder Homomorphismen betrachten. Diese sind jedoch wie bei Ringen definiert.

Definition 48 (Körperhomomorphismus): *Ein Ringhomomorphismus zwischen zwei Körpern heißt* Körperhomomorphismus*.*

Wir wissen von Körperhomomorphismen f nur $f(0) = 0$. Ist aber f injektiv, so kann man in $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ das Element $f(1) \neq 0$ kürzen und erhält auch noch $f(1) = 1$.

Wir erweitern nun das Konzept des geordneten Rings auf Körper. Dabei müssen wir jedoch keine weiteren Forderungen stellen.

Definition 49 (Geordneter Körper): *Ein Körper heißt* geordnet*, wenn er ein geordneter Ring ist.*

Wir können nun Satz 44 etwas erweitern.

Satz 64: *Sei K ein geordneter Körper mit $x, y, z \in K$ und $z > 0$. Dann gilt:*

(i) $x \leq y \Leftrightarrow xz \leq yz$

(ii) $x < y \Leftrightarrow xz < yz$.

BEWEIS:

(i) Es ist $x = xzz^{-1} \leq yzz^{-1} = y$.

(ii) Folgt aus (i) wegen $x \neq y$. □

Einen Zusammenhang zwischen Idealen und Körpern liefert der folgende

Satz 65: *Sei R ein kommutativer Ring, in dem (0) und R die einzigen Ideale sind. Dann ist R ein Körper.*

BEWEIS: Sei $a \in R$ mit $a \neq 0$. Dann folgt $(0) \neq (a)$ und somit $(a) = R$. Also ist insbesondere $1 \in (a)$. Dann existiert ein $r \in R$ mit $1 = ra = ar$ und a ist invertierbar. □

4.6.2 Quotientenkörper

Wir werden uns nun damit beschäftigen, wie man einen Ring zu einem Körper erweitern kann. Dieses Verfahren wird uns in Kapitel 5 nützlich sein, wenn wir aus den ganzen die rationalen Zahlen konstruieren.

Definition 50 (Nennermenge): *Sei R ein kommutativer Ring. Eine Teilmenge $\emptyset \neq S \subseteq R$ heißt* Nennermenge*, wenn gilt:*

(i) Für alle $r \in R$ und $s \in S$ ist die Implikation $rs = 0 \Rightarrow r = 0$ erfüllt.

(ii) S ist bzgl. $\cdot$ abgeschlossen.

Wir führen nun ähnlich wie bei den Grothendieck-Gruppen eine Äquivalenzrelation ein.

Satz 66: *Sei R ein kommutativer Ring und S eine Nennermenge von R. Dann wird durch*

$$(r_1, s_1) \sim (r_2, s_2) :\Leftrightarrow r_1 s_2 = r_2 s_1$$

auf $R \times S$ eine Äquivalenzrelation definiert.

BEWEIS: Reflexivität ist klar, Symmetrie folgt aus der Kommutativität. Transitivität: Es gelte $(r_1, s_1) \sim (r_2, s_2)$ und $(r_2, s_2) \sim (r_3, s_3)$, also $r_1 s_2 = r_2 s_1$ und $r_2 s_3 = r_3 s_2$. Daraus ergibt sich

$$r_1 s_2 s_3 = r_2 s_1 s_3 = r_2 s_3 s_1 = r_3 s_2 s_1$$

und somit $s_2(r_1 s_3 - r_3 s_1) = 0$. Da $s_2 \in S$ muss dann $r_1 s_3 - r_3 s_1 = 0$ sein und folglich $r_1 s_3 = r_3 s_1$, also $(r_1, s_1) \sim (r_3, s_3)$. □

Wir schreiben die Äquivalenzklassen nun als

$$\frac{r}{s} := (r, s).$$

Es gilt damit offenbar die Kürzungsregel

$$\frac{r}{s} = \frac{rt}{st}.$$

Satz 67: *Die Menge der Äquivalenzklassen wird durch die Verknüpfungen*

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

zu einem kommutativem Ring. Die Einbettung

$$i\colon R \longrightarrow (R \times S)/\sim\colon r \longmapsto \frac{rs}{s}$$

für ein $s \in S$ ist ein Monomorphismus.

BEWEIS: Wir müssen natürlich zunächst die Wohldefiniertheit von Addition und Multiplikation zeigen. Sei dazu $r_1/s_1 = \widetilde{r_1}/\widetilde{s_1}$ und $r_2/s_2 = \widetilde{r_2}/\widetilde{s_2}$, also $r_1\widetilde{s_1} = \widetilde{r_1}s_1$ und $r_2\widetilde{s_2} = \widetilde{r_2}s_2$. Dann folgt

$$(r_1 s_2 + r_2 s_1)\widetilde{s_1}\widetilde{s_2} = r_1 s_2 \widetilde{s_1}\widetilde{s_2} + r_2 s_1 \widetilde{s_1}\widetilde{s_2} = \widetilde{r_1} s_1 s_2 \widetilde{s_2} + \widetilde{r_2} s_2 s_1 \widetilde{s_1} = s_1 s_2 (\widetilde{r_1}\widetilde{s_2} + \widetilde{r_2}\widetilde{s_1}),$$

also

$$\frac{r_1 s_2 + r_2 s_1}{s_1 s_2} = \frac{\widetilde{r_1}\widetilde{s_2} + \widetilde{r_2}\widetilde{s_1}}{\widetilde{s_1}\widetilde{s_2}}.$$

Ebenso erhält man $r_1 r_2 \widetilde{s_1}\widetilde{s_2} = \widetilde{r_1} s_1 \widetilde{r_2} s_2$ und somit

$$\frac{r_1 r_2}{s_1 s_2} = \frac{\widetilde{r_1}\widetilde{r_2}}{\widetilde{s_1}\widetilde{s_2}}.$$

Die Abgeschlossenheit ist klar. Die Assoziativität und Kommutativität von $+$ und $\cdot$ vererbt sich von R. Nullelement ist $0/s$, Einselement ist s/s. Das zu r/s bzgl. $+$ Inverse ist $(-r)/s$. Wegen der Kürzungsregel ist i unabhängig von der Wahl von s. Ferner gilt

$$i(r_1 + r_2) = \frac{(r_1 + r_2)s}{s} = \frac{r_1}{s} + \frac{r_2}{s} = i(r_1) + i(r_2)$$

und

$$i(r_1 r_2) = \frac{(r_1 r_2)s}{s} = \frac{r_1 r_2 ss}{ss} = \frac{r_1}{s}\frac{r_2}{s} = i(r_1) i(r_2).$$

Injektivität: Sei $i(r) = 0$. Daraus folgt $(rs)/s = 0/s$ bzw. $rss = 0s = 0$. Da $s \in S$ muss also $r = 0$ gelten. Daraus folgt $\operatorname{Kern} i = \{0\}$ und somit die Behauptung. □

Aufgrund er Injektivität von i können wir R mit $i(R)$ identifizieren. Der Ring R wird damit in natürlicher Weise unitärer Unterring des Äquivalenzklassenrings. Sind die Elemente von S invertierbar, so gilt sogar $R \simeq i(R)$, da i wegen

$$\frac{r}{s} = \frac{rs^{-1}s}{s} = i(rs^{-1})$$

surjektiv ist.

Satz 68: *Ist R ein Integritätsring, so ist $S := R \setminus \{0\}$ eine Nennermenge und $Q(R) := (R \times S)/\sim$ ein Körper, der* Quotientenkörper *von R.*

BEWEIS: Die erste Aussage ist klar. Zur zweiten Aussage: Wir wissen schon (Satz 67), dass $(R \times S)/\sim$ ein kommutativer Ring ist. Wir müssen nur noch zeigen, dass es multiplikativ inverse Elemente gibt. Sei also $r/s \neq 0/s$. Dann folgt $r \neq 0$, also $r \in S$. Damit ergibt sich $(r/s)^{-1} = s/r$. □

Also haben wir erhalten, dass jeder Integritätsring unitärer Unterring eines Körpers ist. Die Umkehrung, dass jeder unitäre Unterring eines Körpers Integritätsring ist, ist nach Satz 60.(ii) trivial. Die Einbettung des Integritätsrings in den Quotientenkörper wird im nächsten Satz genauer untersucht.

Satz 69: *Seien R_1, R_2 Integritätsringe, $Q(R_1), Q(R_2)$ die entsprechenden Quotientenkörper und $f\colon R_1 \to R_2$ ein Isomorphismus. Dann gibt es einen Isomorphismus $\overline{f}\colon Q(R_1) \to Q(R_2)$ mit $\overline{f}(r) = f(r)$ für alle $r \in R_1$, der f auf $Q(R_1)$ fortsetzt, d. h.*

$$\begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ {\scriptstyle i_1}\downarrow & & \downarrow{\scriptstyle i_2} \\ Q(R_1) & \xrightarrow[\overline{f}]{} & Q(R_2) \end{array}$$

komnmutiert.

BEWEIS: Man wähle ein $0 \neq s \in R_1$. Wegen $\operatorname{Kern} f = \{0\}$ ist ebenfalls $f(s) \neq 0$. Wir betrachten nun die Abbildung $\overline{f}(r/s) := f(r)/f(s)$. Wir zeigen zunächst, dass sie wohldefiniert ist. Sei also $r/s = \widetilde{r}/\widetilde{s}$, d. h. $r\widetilde{s} = \widetilde{r}s$. Dann gilt weiter $f(r\widetilde{s}) = f(\widetilde{r}s)$ bzw. $f(r)f(\widetilde{s}) = f(\widetilde{r})f(s)$. Daraus ergibt sich sofort $f(r)/f(s) = f(\widetilde{r})/f(\widetilde{s})$. Injektivität: Sei $\overline{f}(r_1/s_1) = \overline{f}(r_2/s_2)$. Dann ergibt sich $f(r_1)/f(s_1) = f(r_2)/f(s_2)$ und weiter $f(r_1)f(s_2) = f(r_2)f(s_1)$. Somit ist $f(r_1s_2) = f(r_2s_1)$ und wegen der Injektivität von f auch $r_1s_2 = r_2s_1$ sowie $r_1/s_1 = r_2/s_2$. Surjektivität: Sei $u/v \in Q(R_2)$. Da f surjektiv ist, gibt es $r, s \in R_1$ mit $f(r) = u$ und $f(s) = v$. Damit ist $\overline{f}(r/s) = f(r)/f(s) = u/v$, also $\overline{f}$ surjektiv. Nun bleibt nur noch die Verträglichkeit mit $+$ und $\cdot$. Diese ergibt sich aus

$$\begin{aligned} \overline{f}\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) &= \overline{f}\left(\frac{r_1s_2 + r_2s_1}{s_1s_2}\right) = \frac{f(r_1s_2 + r_2s_1)}{f(s_1s_2)} = \frac{f(r_1s_2) + f(r_2s_1)}{f(s_1s_2)} \\ &= \frac{f(r_1s_2)}{f(s_1s_2)} + \frac{f(r_2s_1)}{f(s_1s_2)} = \overline{f}\left(\frac{r_1s_2}{s_1s_2}\right) + \overline{f}\left(\frac{r_2s_1}{s_1s_2}\right) = \overline{f}\left(\frac{r_1}{s_1}\right) + \overline{f}\left(\frac{r_2}{s_2}\right) \end{aligned}$$

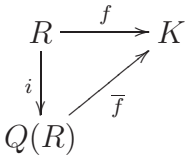
und

$$\overline{f}\left(\frac{r_1}{s_1}\frac{r_2}{s_2}\right) = \overline{f}\left(\frac{r_1 r_2}{s_1 s_2}\right) = \frac{f(r_1 r_2)}{f(s_1 s_2)} = \frac{f(r_1)f(r_2)}{f(s_1)f(s_2)} = \frac{f(r_1)}{f(s_1)}\frac{f(r_2)}{f(s_2)} = \overline{f}\left(\frac{r_1}{s_1}\right)\overline{f}\left(\frac{r_2}{s_2}\right).$$

□

Insbesondere ergibt sich für $R_1 = R_2$ bzw. $f = \mathrm{id}$, dass Quotientenkörper über demselben Ring stets isomorph sind. Ist R_2 schon ein Körper und f lediglich injektiv, so existiert eine eindeutig bestimmte Fortsetzung von f auf $Q(R_1)$.

Satz 70: *Sei R ein Integritätsring, K ein Körper und $f\colon R \to K$ ein Monomorphismus. Dann existiert ein eindeutig bestimmter Monomorphismus $\overline{f}\colon Q(R) \to K$ mit $\overline{f}(r) = f(r)$ für alle $r \in R$, d. h.*



kommutiert.

BEWEIS: Existenz: Definiere $\overline{f}(r/s) := f(r)/f(s)$. Die Wohldefiniertheit haben wir schon in Satz 69 nachgerechnet. Ebenfalls wissen wir schon, dass diese Abbildung ein Monomorphismus ist. Eindeutigkeit: Sei $\overline{f}$ eine Fortsetung von f auf $Q(R)$. Dann muss für alle $r, s \in R$ gelten

$$\overline{f}\left(\frac{r}{s}\right) = \overline{f}(rs^{-1}) = \overline{f}(r)\overline{f}(s)^{-1} = f(r)f(s)^{-1} = \frac{f(r)}{f(s)}.$$

□

4.6.3 Polynomringe

Der Polynomring gehört mit Sicherheit zu den wichtigsten Ringen in der ganzen Mathematik. Wir werden uns deshalb ausführlich mit ihm befassen.

Definition 51 (Polynom): *Sei R ein Ring. Man nennt einen Ausdruck der Form*

$$p = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \tag{4.1}$$

mit $a_k \in R$ ein Polynom *in der* Unbestimmten X *über R. Die a_k heißen* Koeffizienten*, das größte k mit $a_k \neq 0$ heißt* Grad *von p. Ist n der Grad von p, so schreibt man $\operatorname{Grad} p := n$. Der Koeffizient a_n heißt dann* Leitkoeffizient*. Ist der Leitkoeffizient gleich 1, so nennt man das Polynom* normiert*. Außerdem setzt man $\operatorname{Grad} 0 := -\infty$. Die einzelnen Summanden $a_k X^k$ heißen* Glieder*. Die Menge aller Polynome mit Koeffizienten aus R in der Unbestimmten X wird mit $R[X]$ bezeichnet.*

Diese Definition der Polynome ist nicht unproblematisch. Wir halten zunächst fest, dass man Polynome nicht mit Polynomabbildungen verwechseln darf. Ein Polynom ist ein Ausdruck, der die oben angegebene Form hat. Eine Polynomabbildung ist eine Abbildung, deren Definitionsgleichung ein Polynom ist. Das Problem mit der Identifikation von Polynom und Polynomabbildung ist, dass dieselbe Polynomabbildung durch verschiedene Polynome dargestellt werden kann. Es sind z. B. über $\mathbb{Z}/2\mathbb{Z}$ die Polynomabbildungen $X \mapsto X^2 + X$ und $X \mapsto 0$ identisch, ebenso die Abbildungen $X \mapsto X$ und $X \mapsto X^2$, nicht aber die Polynome. Es ist schade, dass man in der Algebra nicht zwei verschiedene Notationen für das Polynom p und den Wert $p(X)$ der Polynomabbildung an der Stelle X hat, denn beide werden mit 4.1 bezeichnet.

Zur sauberen Definition setzen wir

$$R[X] := \{\, p\colon \mathbb{N} \longrightarrow R \mid p(k) \neq 0 \text{ nur für endlich viele } k \in \mathbb{N} \,\}.$$

Ein solches $p \in R[X]$ wird durch die Folge $(p(k))_{k\in\mathbb{N}}$ eindeutig bestimmt. Jedes Polynom der Form (4.1) identifizieren wir nun mit dieser Folge $(a_0, a_1, \ldots, a_n, 0, \ldots)$. Natürlich sind alle Folgenglieder nach dem Leitkoeffizient gleich 0. Das Polynom ist dann eindeutig festgelegt durch die Koeffizienten. Insbesondere sind zwei Polynome genau dann gleich, wenn ihre Koeffizienten gleich sind, wie gewünscht. Zur expliziten Konstruktion des Polynomrings sei auf Anhang B verwiesen.

Da die Einbettung $i\colon R \to R[X]\colon r \mapsto (r, 0, 0, \ldots)$ ein Monomorphismus ist, kann man die Elemente von R mit den konstanten Polynomen in $R[X]$ identifizieren. Damit wird R zu einem unitären Unterring von $R[X]$. Insbesondere sind dann die Koeffizienten eines Polynoms wieder Polynome, so dass wir keine äußere Verknüpfung $R \times R[X] \to R[X]$ brauchen.

Wir werden die Verknüpfungen in $R[X]$ so definieren, dass für jeden kommutativen Ring R die Abbildung $R[X] \to R\colon p \mapsto p(r)$ bei festem r ein Homomorphismus ist, der sogenannte *Einsetzungshomomorphismus* .

Satz 71: *Sei R ein kommutativer Ring. Definiert man auf $R[X]$ die Verknüpfungen*

$$\begin{aligned}(a_0, a_1, \ldots) + (b_0, b_1, \ldots) &:= (a_0 + b_0, a_1 + b_1, \ldots)\\ (a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) &:= (c_0, c_1, \ldots)\end{aligned}$$

mit

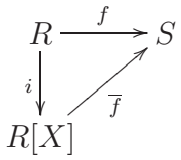
$$c_k := a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0,$$

so wird $(R[X], +, \cdot)$ zu einem kommutativem Ring, dem Polynomring.

BEWEIS: Die Verknüpfung $+$ in $R[X]$ ist assoziativ und kommutativ, weil $+$ in R assoziativ und kommutativ ist. Das Nullelement ist $(0, 0, \ldots)$, das zu $(a_1, a_2, \ldots)$ bzgl. $+$ Inverse ist $(-a_0, -a_1, \ldots)$. Das Einselement ist $(1, 0, \ldots)$. Den Rest rechnet man leicht nach. □

Viele algebraischen Objekte lassen sich durch sog. universelle Eigenschaften charakterisieren. Diese lassen sich am übersichtlichsten durch das Kommutieren von Diagrammen formulieren.

Satz 72 (Universelle Eigenschaft des Polynomrings): *Seien R, S kommutative Ringe, $i\colon R \to R[X]$ die kanonische Injektion, $f\colon R \to S$ ein Homomorphismus und $s \in S$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\overline{f}\colon R[X] \to S$ mit $\overline{f}(X) = s$, so dass*



kommutiert.

BEWEIS: Existenz: Setze

$$\overline{f}(a_n X^n + \cdots + a_1 X + a_0) := f(a_n)s^n + \cdots + f(a_1)s + f(a_0).$$

Offensichtlich ist dann $\overline{f}$ ein Homomorphismus mit der gewünschten Eigenschaft. Eindeutigkeit: Sei nun $\overline{f}$ ein Homomorphismus, der das Geforderte erfüllt. Dann muss $f = \overline{f} \circ i$ gelten. Oder etwas ausführlicher:

$$\begin{aligned}\overline{f}(a_n X^n + \cdots + a_1 X + a_0) &= \overline{f}(i(a_n))\overline{f}(X)^n + \cdots + \overline{f}(i(a_1))\overline{f}(X) + \overline{f}(i(a_0)) \\ &= f(a_n)s^n + \cdots + f(a_1)s + f(a_0).\end{aligned}$$ □

Dass $\operatorname{Grad}(p+q) \leq \max(\operatorname{Grad} p, \operatorname{Grad} q)$ gilt ist klar[7]. Über $\operatorname{Grad}(pq)$ kann man jedoch mehr aussagen.

Satz 73: *Seien R ein kommutativer Ring und $p, q \in R[X]$. Dann gilt*

$$\operatorname{Grad}(pq) \leq \operatorname{Grad} p + \operatorname{Grad} q.$$

Ist R ein Integritätsring, so gilt sogar Gleichheit.

BEWEIS: Sei zunächst $p = 0$ oder $q = 0$. Dann ist auch $pq = 0$ und die Gleichung erfüllt. Es gelte nun $p, q \neq 0$. Nach Definition ist mit

$$p = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

und

$$q = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$$

dann

$$pq = c_{n+m} X^{n+m} + c_{n+m-1} X^{n+m-1} + \cdots + c_1 X + c_0,$$

wobei a_n und b_m jeweils die Leitkoeffizienten sind und c_k die Summe der Koeffizienten a_i, b_j ist, deren Indexsumme gerade k ergibt. Damit ist dann $c_{n+m} = a_n b_m \neq 0$, falls R Integritätsring ist. □

[7] Man setzt $-\infty + n := -\infty$ und $-\infty + (-\infty) := -\infty$.

Ist K ein Körper, so ist die Einheitengruppe $K^* = K \setminus \{0\}$. Betrachtet man nun den Polynomring $K[X]$, so stellt man fest, dass die Einheiten identisch sind.

Satz 74: *Für jeden Körper K gilt $K^* = K[X]^*$.*

BEWEIS:
„$\subseteq$“: Klar.
„$\supseteq$“: Sei $p \in K[X]^*$. Dann gibt es ein $q \in K[X]$ mit $pq = 1$. Wegen Satz 73 muss dann $\operatorname{Grad} p = 0$ gelten, denn K ist Integritätsring. Also ist p ein konstantes Polynom ungleich 0, somit ein Element von $K \setminus \{0\}$ und damit eine Einheit in K. □

Wir werden nun die Teilbarkeitslehre in Ringen auf den Polynomring anwenden. Wir müssen dazu noch ein paar Begriffe einführen. Teilt ein $r \in R$ die Elemente $r_1, \ldots, r_n \in R$, so heißt r *gemeinsamer Teiler* von $r_1, \ldots, r_n$. Sind die einzigen gemeinsamen Teiler dieser Elemente Einheiten, so heißen die $r_1, \ldots, r_n$ *teilerfremd*. Ein gemeinsamer Teiler der $r_1, \ldots, r_n$ heißt *größter gemeinsamer Teiler* ggT, wenn alle anderen gemeinsamen Teiler von $r_1, \ldots, r_n$ den ggT teilen[8].

Definition 52: *Sei R ein Integritätsring und $0 \neq f \in R[X]$. Es heißt f* primitiv*, falls die Koeffizienten von f teilerfremd sind.*

Man stellt nun fest, dass sich jedes Polynom als Produkt aus einem primitiven Polynom und einem Körperelement des Quotientenkörpers schreiben lässt. Diese Schreibweise ist bis auf die Multiplikation mit einer Einheit eindeutig.

Satz 75: *Sei R ein faktorieller Ring. Dann gibt es zu jedem $0 \neq f \in Q(R)[X]$ ein $x \in Q(R)$ und ein primitives Polynom $g \in R[X]$ mit $f = xg$. Ist umgekehrt ein $y \in Q(R)$ und ein primitives Polynom $h \in R[X]$ mit $f = yh$ gegeben, so gibt es ein $e \in R^*$ mit $h = eg$ und $y = xe^{-1}$.*

BEWEIS: Sei

$$f = \frac{r_n}{s_n} X^n + \frac{r_{n-1}}{s_{n-1}} X^{n-1} + \cdots + \frac{r_1}{s_1} X + \frac{r_0}{s_0}$$

gegeben. Betrachte für $s := s_0 \cdots s_n$ das Polynom

$$sf = t_n X^n + t_{n-1} X^{n-1} + \cdots + t_1 X + t_0.$$

Ist a der ggT der $t_0, \ldots, t_n$, so sind $t_0/a, \ldots, t_n/a \in R$ teilerfremd. Damit ist $g := s/af$ primitiv und $f = xg$ mit $x := a/s$. Sei nun $f = yh$ mit $y \in Q(R)$ und $h \in R[X]$ primitiv. Wir können $y = r/t$ schreiben mit $r, t \in R$. Aus $fs = ag$ und $ft = rh$ folgt $rsh = atg$. Folglich ist at gemeinsamer Teiler der Koeffizienten von rsh. Es ist aber h primitiv, also muss $at | rs$ gelten. Umgekehrt folgt $rs | at$ und nach Satz 53.(ii) gilt $at \sim rs$. Demnach existiert ein $e \in R^*$ mit $at = rse$. Also folgt $x = a/s = r/te = ye$ und $h = 1/yf = e/xf = eg$. □

[8] Es gibt verschiedene Verfahren, um den ggT zu bestimmen, wovon das einfachste der *Euklidische Algorithmus* ist, worauf wir hier aber nicht eingehen können.

Über das Produkt zweier primitiver Polynome sagt der folgende Satz etwas aus.

Satz 76 (Satz von Gauß): *Sei R ein faktorieller Ring. Dann sind $f, g \in R[X]$ genau dann primitv, wenn fg primitiv ist.*

BEWEIS:
„⇒“: Angenommen, fg wäre nicht primitiv. Da R faktoriell ist, existiert ein Primelement $p \in R$, das alle Koeffizienten von fg teilt. Diese sind Elemente des Primideals (p) (siehe Aufgabe 25), also im Kern des kanonischen Epimorphismus $\pi\colon R \to R/(p)$. Wir untersuchen nun die Abbildung

$$\psi\colon R[X] \longrightarrow (R/(p))[X]\colon a_nX^n + \cdots + a_1X + a_0 \longmapsto \pi(a_n)X^n + \cdots + \pi(a_1)X + \pi(a_0).$$

Man sieht leicht, dass ψ ein Epimorphismus ist, und insbesondere gilt $0 = \psi(fg) = \psi(f)\psi(g)$. Da nach Satz 57 $R/(p)$ ein Integritätsring ist, ist auch $R/(p)[X]$ ein Integritätsring, und es muss $\psi(f) = 0$ oder $\psi(g) = 0$ gelten. Sei o. E. $\psi(f) = 0$. Also sind alle Koeffizienten von f Elemente von $\operatorname{Kern}\pi$ und damit durch p teilbar und nicht primitiv.
„⇐“: Angenommen, f wäre nicht primitiv. Dann existiert ein Primelement $p \in R$, das alle Koeffizienten von f teilt. Folglich gibt es ein $h \in R[X]$, so dass $f = ph$. Aber dann ist $fg = phg$ nicht primitiv. □

Wir betrachten nun die irreduziblen Elemente in $R[X]$.

Satz 77: *Sei R ein faktorieller Ring und $f \in R[X]$. Dann sind äquivalent:*

(i) Es ist f irreduzibel in $R[X]$.

(ii) Entweder ist f irreduzibel in R oder f ist primitiv in $R[X]$ und irreduzibel in $Q(R)[x]$.

BEWEIS:
‘(i) ⇒ (ii)“: Sei f irreduzibel in $R[X]$. Dann gilt $f \neq 0$ und $f \notin R[X]^* = R^*$ (siehe Aufgabe 26). Ist $\operatorname{Grad} f = 0$, so muss $f \in R\setminus R^*$ gelten. Schreibt man $f = ab$ mit $a, b \in R \subseteq R[X]$, so folgt nach Voraussetzung $a \in R[X]^* = R^*$ oder $b \in R[X]^* = R^*$. Dann ist f auch irreduzibel über R. Sei nun $\operatorname{Grad} f > 0$. Dann gilt $f \notin Q(R)[X]^* = Q(R)^*$. Außerdem ist f primitiv in $R[X]$, denn sonst ließe sich f schreiben als $f = pg$ mit $p \in R$ prim und $g \in R[X]$, was mit $p \notin R^* = R[X]^*$ sowie $g \notin R^* = R[X]^*$ zum Widerspruch zur Irreduzibilität von f führen würde. Sei nun $f = hk$ mit $h, k \in Q(R)[X]$. Nach Satz 75 existieren $x, y \in Q(R)$ und $\widetilde{h}, \widetilde{k} \in R[X]$ mit $h = x\widetilde{h}$ und $k = y\widetilde{k}$. Folglich ist $f = 1f = (xy)(\widetilde{h}\widetilde{k})$ mit $xy \in Q(R)$ und $\widetilde{h}\widetilde{k}$ primitiv nach Satz 76. Erneut nach Satz 75 folgt dann für die Zerlegungen $e\widetilde{h}\widetilde{k} = f$ und $xye^{-1} = 1$ mit einem $e \in R^*$. Da f irreduzibel in $R[X]$ ist, ist damit $\widetilde{h} \in R[X]^* = R^*$ oder $\widetilde{k} \in R[X]^* = R^*$ und weiter $h \in Q(R)[X]^* = Q(R)^*$ oder $k \in Q(R)[X]^* = Q(R)^*$. Somit ist f in $Q(R)$ irreduzibel.
„(ii) ⇒ (i)“: Sei zunächst f irreduzibel in R. Dann ist $0 \neq f \notin R^* = R[X]^*$. Sei $f = gh$ mit $g, h \in R[X]$, dann folgt $0 = \operatorname{Grad} f = \operatorname{Grad} g + \operatorname{Grad} h$ nach Satz 73, also $0 = \operatorname{Grad} g = \operatorname{Grad} h$. Damit ist $g, h \in R$. Da f irreduzibel in R ist folgt $g \in R^* = R[X]^*$ oder $h \in R^* = R[X]^*$, also ist f irreduzibel in $R[X]$. Sei nun f primitiv in $R[X]$ und irreduzibel in $Q(R)[X]$. Dann ist $0 \neq f \notin Q(R)[X]^* = Q(R)^*$. Daraus folgt $\operatorname{Grad} f > 0$ sowie

$f \notin R[X]^* = R^*$. Sei $f = gh$ mit $g, h \in R[X]$, so folgt $g \in Q(R)[X]^* = Q(R)^*$ oder $h \in Q(R)[X]^* = Q(R)^*$. Sei o. E. $g \in Q(R)^*$, also $g \in R[X] \cap Q(R)^* = R \setminus \{0\}$. Dann teilt g alle Koeffizienten von f, und weil f primitiv ist ergibt sich $g \in R^*$. □

Eines der Hauptergebnisse dieses Abschnitts ist der

Satz 78: *Ist R ein faktorieller Ring, so auch $R[X]$.*

BEWEIS: Sei $0 \neq f \in R[X] \setminus R[X]^*$. Falls $f \in R$ sind wir fertig. Sei also $\operatorname{Grad} f > 0$ und a der ggT der Koeffizienten von f. Dann lässt sich f schreiben als $f = ag$ mit $g \in R[X]$ primitiv. Betrachtet man jedoch f über $Q(R)$, so lässt sich schreiben $f = f_1 \cdots f_n$ mit $f_i \in Q(R)[X]$ irreduzibel. Für jedes $i \in \{1, \ldots, n\}$ existiert nach Satz 75 ein $a_i \in Q(R)$ und ein primitives Polynom $g_i \in R[X]$ mit $f_i = a_i g_i$. Dann sind die g_i auch irreduzibel in $R[X]$. Betrachte also das Produkt $f = a_1 \cdots a_n g_1 \cdots g_n$. Laut Satz 76 ist aber $g_1 \cdots g_n$ primitiv, und es gibt erneut nach Satz 75 ein $e \in R^*$ mit $a_1 \cdots a_n = ae$ sowie $g = eg_1 \cdots g_n$. Daraus folgt nun $f = aeg_1 \cdots g_n$. Falls $a \in R^*$ ist nichts mehr zu zeigen. Ansonsten können wir a in irreduzible Elemente zerlegen. Schließlich ist f vollständig faktorisiert und die Existenz der Zerlegung gesichert. □

Wir untersuchen nun noch kurz den Zusammenhang zwischen den Nullstellen von Polynomen und der Faktorisierbarkeit.

Satz 79: *Sei R ein kommutativer Ring, $f \in R[X]$, $r \in R$ und $f(r) = 0$. Dann ist $f = (X - a)g$ für ein $g \in R[X]$.*

BEWEIS: Schreibe

$$\begin{aligned} f &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \\ &= a_n (X - r + r)^n + a_{n-1} (X - r + r)^{n-1} + \cdots + a_1 (X - r + r) + a_0 \\ &= b_n (X - r)^n + b_{n-1} (X - r)^{n-1} + \cdots + b_1 (X - r) + b_0 \end{aligned}$$

mit $b_0, \ldots, b_n$ geeignet gewählt. Da $0 = f(r) = b_0$ ergibt sich

$$f = (X - r)(b_n (X - r)^{n-1} + b_{n-1} (X - r)^{n-2} + \cdots + b_1).$$ □

Man kann natürlich nicht nur Polynome in einer Unbestimmten betrachten, sondern Polynome in beliebig vielen Unbestimmten. Man erhält z. B. den Ring der Polynome in den Unbestimmten X und Y über $R[X, Y] := (R[X])[Y]$.

Ist K ein Körper, so erhält man übrigens mit $Q(K[X])$ den Körper der *rationalen Funktionen* über K in der Unbestimmten X.

4.6.4 Primkörper

Definition 53 (Unter- und Erweiterungskörper): *Sei L ein Körper und $K \subseteq L$ ein unitärer Unterring. Es heißt K* Unterkörper *von L, wenn für alle $x \in K$ und $y \in K\backslash\{0\}$ gilt $xy^{-1} \in K$. Dann heißt L* Erweiterungskörper *von K, und man schreibt $L|K$.*

Analog zu Aufgabe 14 zeigt man, dass der Schnitt von Unterkörpern wieder ein Unterkörper ist. Der Schnitt aller Unterkörper von L heißt *Primkörper* von L. Er hat keinen echten Unterkörper.

Satz 80: *Die Charakteristik eines nullteilerfreien Rings ist entweder 0 oder eine Primzahl.*

BEWEIS: Betrachte die Abbildung $f\colon \mathbb{Z} \to R\colon m \mapsto m \cdot 1$. Angenommen $\operatorname{Char} R > 0$. Sei $\operatorname{Char} R = ab$ mit $a, b \in \mathbb{N}$. Dann gilt $0 < a, b \leq \operatorname{Char} R$. Weiter ist $f(a)f(b) = f(ab) = f(\operatorname{Char} R) = 0$. Da R nullteilerfrei ist folgt $f(a) = 0$ oder $f(b) = 0$. Sei o. E. $f(a) = 0$. Dann ist wegen der Ungleichung $a = \operatorname{Char} R$ und $b = 1$. Folglich ist $\operatorname{Char} R \in \mathbb{P}$. □

Insbesondere gilt dieser Satz natürlich für Körper. Wir wissen also, dass die Charakteristik jedes Körpers 0 oder prim ist. Umgekehrt ist der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ für $p \in \mathbb{P}$ ein Körper. Der Beweis wird in Anhang B geführt.

Satz 81: *Sei K ein Körper und $P \subseteq K$ sein Primkörper. Dann gilt:*

(i) Ist $\operatorname{Char} K = 0$, so ist $P \simeq \mathbb{Q}$.

(ii) Ist $\operatorname{Char} K = p \neq 0$, so ist $P \simeq \mathbb{Z}/p\mathbb{Z}$.

BEWEIS: Betrachte den Ringhomomorphismus $f\colon \mathbb{Z} \to K\colon m \mapsto m \cdot 1$.

(i) Ist $\operatorname{Char} K = 0$, so ist f injektiv. Nach Satz 70 existiert die Fortsetzung $\overline{f}\colon \mathbb{Q} \to K$[9]. Nun ist $\overline{f}$ aber ein Körpermonomorphismus, d. h. insbesondere ist $\overline{f}(\mathbb{Q})$ ein Unterkörper von K. Da P ein Primkörper ist folgt $P \subseteq \overline{f}(\mathbb{Q})$. Für die umgekehrte Inklusion schreibe

$$\overline{f}(\mathbb{Q}) = \{\, \overline{f}(r) \in K \mid r \in \mathbb{Q} \,\} = \left\{ \frac{\overline{f}(m)}{\overline{f}(n)} \in K \,\middle|\, m, n \in \mathbb{Z} \wedge n \neq 0 \right\}.$$

Da $\overline{f}(1) = 1 \in P$ folgt weiter für $m \in \mathbb{N}$

$$\overline{f}(m) = \overline{f}(\underbrace{1 + \cdots + 1}_{m\,\text{mal}}) = \underbrace{\overline{f}(1) + \cdots + \overline{f}(1)}_{m\,\text{mal}} = \underbrace{1 + \cdots + 1}_{m\,\text{mal}} = m \in P.$$

Schließlich ist für $n \neq 0$ auch $\overline{f}(m/n) = \overline{f}(m)/\overline{f}(n) \in P$, also $\overline{f}(\mathbb{Q}) \subseteq P$ und insgesamt $\overline{f}(\mathbb{Q}) = P$ bzw. $\mathbb{Q} \simeq P$.

(ii) Ist $\operatorname{Char} K = p \neq 0$, so ist $\operatorname{Kern} f = p\mathbb{Z}$, also $f(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ ist ein Unterkörper von K. Wieder ist $P \subseteq f(\mathbb{Z})$. Andersrum ist erneut $1 \in P, \ldots, m \in P$ für alle $m \in \mathbb{N}$, d. h. $f(\mathbb{Z}) \subseteq P$. Also ist $P = f(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$. □

[9] Wir haben hier $Q(\mathbb{Z}) = \mathbb{Q}$ benutzt, was wir in der Tat in Kapitel 5 so einführen werden.

Mit diesem schönen Ergebnis, das beispielhaft die Mächtigkeit einfacher Isomorphieüberlegungen zeigt, erhalten wir einen tieferen Einblick in die Struktur von Körpern. Primkörper spielen übrigens bei der Klassifikation der endlichen Körper eine entscheidende Rolle. Zum Abschluss unserer Beschäftigung mit der Algebra sprechen wir noch kurz den Vektorraumbegriff an.

4.7 Vektorräume und Algebren

Vektorräume gehören zu den absolut fundamentalen algebraischen Strukturen in der Mathematik. Viele Objekte in der Mathematik lassen sich als Vektorräume auffassen, und man kann dann direkt die Theorie der Vektorräume, die in der *linearen Algebra* entwickelt wird, auf sie anwenden.

Definition 54 (Vektorraum): *Sei K ein Körper, V eine abelsche Gruppe und $\cdot\colon K \times V \to V$ eine äußere Verknüpfung. Das Tripel $((K,+,\cdot),(V,+),\cdot)$ heißt* Vektorraum *oder* linearer Raum*, wenn gilt*

(i) $(\lambda+\mu)\cdot v = \lambda\cdot v + \mu\cdot v$

(ii) $\lambda\cdot(v+w) = \lambda\cdot v + \lambda\cdot w$

(iii) $(\lambda\cdot\mu)\cdot v = \lambda\cdot(\mu\cdot v)$

(iv) $1\cdot v = v$

für alle $\lambda,\mu \in K$ und $v,w \in V$. Die Elemente von V heißen Vektoren*, die Elemente von K* Skalare*, K heißt der* Skalarenkörper*. Die Verknüpfung $\cdot$ heißt* skalare Multiplikation*.*

Man beachte, dass wir hier erneut die Verknüpfungen auf den verschiedenen Mengen symbolisch nicht unterscheiden. Gelten die obigen Axiome, so nennt man auch abkürzend V einen K-Vektorraum oder Vektorraum über K.

Wir geben hier nur ganz kurz ein Beispiel für einen Vektorraum an. Dieses Beispiel kommt aus der Analysis. Und zwar betrachten wir die Menge M der Funktionen $\mathbb{R} \to \mathbb{R}$. Definieren wir die Summe zweier Funktionen über $(f+g)(x) = f(x)+g(x)$, so ist M sicher eine abelsche Gruppe. Außerdem können wir jede reelle Funktion mit einer reellen Zahl multiplizieren gemäß $(\lambda f)(x) = \lambda f(x)$ und erhalten wieder eine reelle Funktion. Dieser wichtige Vektorraum heißt *Funktionenraum*. In unserem Beispiel gilt aber sogar noch mehr. Wir können nämlich auch zwei reelle Funktionen über $(fg)(x) = f(x)g(x)$ miteinander multiplizieren und erhalten wieder eine reelle Funktion. Man spricht deshalb von der *Funktionenalgebra*.

Definition 55 (Algebra): *Sei K ein Körper und V ein K-Vektorraum. Man nennt V eine K-*Algebra *oder* Algebra über K*, wenn eine Verknüpfung $\cdot\colon V \times V \to V$ definiert ist, für die gilt*

(i) $(\lambda u + \mu v)\cdot w = \lambda(u\cdot w) + \mu(v\cdot w)$

(ii) $u(\lambda v + \mu w) = \lambda(u\cdot v) + \mu(u\cdot w)$

für alle $\lambda, \mu \in K$ und $u, v, w \in V$. Eine Algebra heißt assoziativ *bzw.* kommutativ*, wenn $\cdot$ assoziativ bzw. kommutativ ist. Eine Algebra heißt* unitär*, wenn ein Einselement bzgl. $\cdot$ existiert.*

Die Funktionenalgebra M ist somit eine unitäre, assoziative und kommutative $\mathbb{R}$-Algebra. Funktionenräume und Funktionenalgebren spielen in der modernen Analysis, aber besonders in der *Funktionalanalysis*, eine wichtige Rolle.

Wir haben übrigens nicht ohne Grund den Polynomring so intensiv untersucht. Es lässt sich nämlich zeigen, dass für jeden Körper K und jedes irreduzible Polynom f über K ein Erweiterungskörper von K existiert, über dem f in Linearfaktoren zerfällt. Der kleinste Erweiterungskörper mit dieser Eigenschaft heißt *Zerfällungskörper* von f über K[10]. Dieses Ergebnis wird in der linearen Algebra oft benutzt. Wir können den Beweis hier leider nicht geben, da er nicht-triviale Resultate aus der linearen Algebra benutzt, die wir hier nicht besprechen können. Wir verlassen vielmehr nun unseren algebraischen Kompaktkurs und wenden uns der Konstruktion der Zahlbereiche zu.

Übungsaufgaben

Aufgabe 13: Überführe

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

in Zyklen-Schreibweise.

Aufgabe 14: Sei G eine Gruppe und $(U_i)_{i \in I}$ eine Familie von Untergruppen von G. Zeige: Dann ist $\bigcap_{i \in I} U_i$ ebenfalls eine Untergruppe von G. Was ist mit $\bigcup_{i \in I} U_i$?

Aufgabe 15: Seien G eine Gruppe und $U, V \subseteq G$ Teilmengen. Zeige:

a) Es ist U genau dann eine Untergruppe von G, wenn $U \cdot U \subseteq U$ und $U^{-1} \subseteq U$ gilt. Gilt auch Gleichheit?

b) Das Mengenprodukt $U \cdot V$ ist genau dann Untergruppe von G, wenn $U \cdot V = V \cdot U$ gilt.

Aufgabe 16: Zeige:

a) Es gibt genauso viele Links- wie Rechtsnebenklassen.

b) In einer abelschen Gruppe ist jede Untergruppe Normalteiler.

Aufgabe 17: Seien G eine Gruppe und $U, V < G$ Untergruppen. Dann gilt $[G : U] = [G : V] \cdot [V : U]$.

Aufgabe 18: Sei f ein Endomorphismus auf einer Gruppe. Zeige: Dann sind äquivalent:

[10] Man kann den Zerfällungskörper sogar explizit konstruieren.

a) f ist injektiv

b) f ist surjektiv

c) f ist bijektiv.

Aufgabe 19: Seien G und H Gruppen, $f\colon G \to H$ ein Epimorphismus und $U \lhd G$. Zeige: $f(U) \lhd H$.

Aufgabe 20: Zeige: Hat jedes Element einer Gruppe außer dem neutralen Ordnung 2, so ist die Gruppe abelsch.

Aufgabe 21: Zeige, dass in jeder Gruppe die Ordnungen von gh und hg gleich sind.

Aufgabe 22: Seien G, H Gruppen und $f\colon G \to H$ ein Homomorphismus.

a) Sei $g \in G$ mit Ordnung k. Was folgt daraus für die Ordnung von $f(g)$?

b) Nun seien G, H endliche Gruppen, deren Ordnungen teilerfremd seien. Zeige, dass $f(g) = 1$ für alle $g \in G$ ist.

Aufgabe 23: Sei M eine beliebige Menge. Wir definieren auf $\mathcal{P}(M)$ die Verknüpfung

$$N \triangle O := (N \setminus O) \cup (O \setminus N),$$

welche *symmetrische Differenz* genannt wird. Zeige, dass damit $(\mathcal{P}(M), \triangle, \cap)$ ein Ring ist, der sogenannnte *Potenzmengenring*. Welche Charakteristik hat er?

Aufgabe 24: Seien R, S Ringe mit $R \simeq S$. Zeige: Ist R nullteilerfrei, so auch S.

Aufgabe 25: Sei R ein Integritätsring und $0 \neq p \in R$. Zeige: Es ist p genau dann Primelement, wenn (p) Primideal ist.

Aufgabe 26: Zeige: Für jeden Integritätsring R gilt $R^* = R[X]^*$.

Aufgabe 27: Sei K ein total geordneter Körper mit $x, y \in K$. Zeige: Dann gilt:

a) $0 < 1$.

b) Es ist $xy \geq 0$ genau dann, wenn $x, y \geq 0$ oder $x, y \leq 0$.

c) Gilt $x > 0$, dann ist $xy > 0$ genau dann, wenn $y > 0$ ist.

d) Falls $x < y$ gilt, so existiert ein $z \in K$ mit $x < z < y$.

e) K ist unendlich.

Aufgabe 28: Seien V ein K-Vektorraum und 0_V bzw. 0_K die Nullelemente von V bzw. K. Zeige:

a) $0_K \cdot v = 0_V$

b) $\lambda \cdot 0_V = 0_V$

c) $(-\lambda) \cdot v = \lambda \cdot (-v) = -(\lambda \cdot v)$

d) $\lambda \cdot v = 0_V \Rightarrow \lambda = 0_K \vee v = 0_V$

für alle $v \in V, \lambda \in K$. Welche Rechenregeln gelten auch für Moduln?

5 Die Konstruktion der Zahlbereiche

5.1 Natürliche Zahlen

5.1.1 Das Prinzip der vollständigen Induktion

Der am Anfang unserer Überlegungen stehende Zahlbereich ist die Menge der natürlichen Zahlen. Um sie zu konstruieren bleibt uns nichts anderes übrig, als direkt die Axiome der Mengenlehre zu verwenden. Wir erinnern insbesondere an das Unendlichkeitsaxiom: „Es gibt eine Menge, die $\emptyset$ und mit jedem Element M auch die Menge enthält, die aus M und den Elementen von M besteht." Wir schreiben nun $A(x)$, wenn die Menge x das Unendlichkeitsaxiom erfüllt.

Sei N eine Menge mit $A(N)$. Dann muss $\emptyset \in N$ gelten, $\{\emptyset\} \in N$, $\{\emptyset, \{\emptyset\}\} \in N$ usw. Eine Menge, die genau aus diesen Elementen bestünde, wäre in gewisser Weise die „kleinste" Menge, die das Unendlichkeitsaxiom erfüllt. Wir werden nun zeigen, dass es eine solche kleinste Menge in der Tat gibt.

Satz 82: *Es gibt eine Menge $\mathbb{N}$ mit $A(\mathbb{N})$, so dass für jede andere Menge N mit $A(N)$ stets $\mathbb{N} \subseteq N$ gilt.*

BEWEIS: Sei N mit $A(N)$ gegeben. Definiere

$$M := \{x \in \mathcal{P}(N) \mid A(x)\}.$$

Wegen $N \in M$ ist $M \neq \emptyset$. Nun setze

$$\mathbb{N} := \bigcap_{x \in M} x.$$

Wir zeigen nun, dass $A(\mathbb{N})$ gilt. Zunächst ist $\emptyset \in \mathbb{N}$, da $\emptyset \in x$ für alle $x \in M$. Sei nun $n \in \mathbb{N}$. Da $n \in x$ für alle $x \in M$ ist auch $n \cup \{n\} \in x$ für alle $x \in M$ und somit $n \cup \{n\} \in \mathbb{N}$.

Sei nun O eine beliebige Menge mit $A(O)$. Dann gilt auch $A(N \cap O)$. Nun ist aber $N \cap O \in \mathcal{P}(N)$ und daher $N \cap O \in M$ und weiter $\mathbb{N} \subseteq N \cap O \subseteq O$. □

Definition 56 (Menge der natürlichen Zahlen): *Die Menge $\mathbb{N}$ heißt* Menge der natürlichen Zahlen. *Wir führen für ihre Elemente induktiv die Bezeichnungen $0 := \emptyset$ und $n+1 := n \cup \{n\}$ ein.*

Damit erhalten wir also

$$0 = \emptyset, \quad 1 = 0 \cup \{0\} = \{\emptyset\}, \quad 2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\}, \quad \ldots$$

Man beachte, dass stets $n = \{0, 1, \ldots, n-1\}$ gilt. Dies ist intuitiv klar und wird im nächsten Abschnitt bewiesen. Wir werden diese Tatsache dann u. a. nutzen, um auf $\mathbb{N}$ eine Ordnung einzuführen.

Untrennbar mit der Struktur der natürlichen Zahlen verknüpft ist das Beweisprinzip der vollständigen Induktion. Es ist in der Mathematik absolut unverzichtbar und wird uns nun näher beschäftigen.

Satz 83 (Prinzip der vollständigen Induktion): *Sei $A(x)$ eine Aussageform. Ist $A(0)$ und für alle $n \in \mathbb{N}$ die Implikation $A(n) \Rightarrow A(n+1)$ wahr, so gilt $A(n)$ für alle $n \in \mathbb{N}$.*

BEWEIS: Setze $M := \{\, n \in \mathbb{N} \mid A(n) \,\}$. Nach Voraussetzung ist $0 \in M$. Ebenso gilt $n \in M \Rightarrow n+1 \in M$. Damit erfüllt aber M das Unendlichkeitsaxiom und nach Satz 82 gilt $\mathbb{N} \subseteq M \subseteq \mathbb{N}$, d. h. $M = \mathbb{N}$ und $A(n)$ gilt für alle $n \in \mathbb{N}$. □

Das Prinzip der vollständigen Induktion gilt in dieser Formulierung nur für Aussagen, die für alle natürlichen Zahlen gelten. Es gibt aber viele Aussagen, die erst ab einer bestimmten Zahl gelten. Deshalb wird man wünschen, dass man den *Induktionsanfang* 0 durch eine beliebige Zahl $m \in \mathbb{N}$ ersetzen kann[1].

Satz 84: *Sei $A(x)$ eine Aussageform und $m \in \mathbb{N}$. Ist $A(m)$ und für alle $n \in \mathbb{N}$ mit $n \geq m$ die Implikation $A(n) \Rightarrow A(n+1)$ wahr, so gilt $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq m$.*

BEWEIS: Wir wenden Satz 83 mit der Aussageform

$$B(x) \colon x \in \mathbb{N} \wedge x \geq m \Rightarrow A(x)$$

an. Dann gilt $B(0)$, denn falls $m = 0$ ist nichts zu zeigen, und falls $m > 0$ ist die Voraussetzung immer falsch, die Implikation also wahr. Wir nehmen nun an, dass $B(n)$ gilt und zeigen, dass dann auch $B(n+1)$ gilt. Da $n+1 \geq m$ reicht es zu zeigen, dass $A(n+1)$ gilt. Im Fall $n+1 = m$ ist dies nach Voraussetzung erfüllt. Im Fall $n+1 > m$ folgt $n \geq m$ und mit $B(n)$ folgt $A(n)$. Dann folgt aber automatisch $A(n+1)$. □

Als nächstes werden wir die *Induktionsvoraussetzung* $A(n)$ und damit verbunden den *Induktionsschluss* $A(n) \Rightarrow A(n+1)$ modifizieren.

Satz 85 (Verallgemeinertes Prinzip der vollständigen Induktion): *Sei $A(x)$ eine Aussageform und $m \in \mathbb{N}$. Gilt für alle $n \in \mathbb{N}$ mit $n \geq m$ die Implikation*

$$\left(\bigwedge_{l \in \mathbb{N}} : m \leq l < n \Rightarrow A(l) \right) \Rightarrow A(n),$$

so gilt $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq m$.

Der Beweis erfolgt genau analog zum vorigen Beweis; wir werden uns damit nicht aufhalten. Der mit Induktionsbeweisen nicht vertraute Leser sollte zunächst Abschnitt 5.1.7 besuchen, denn die dort gelieferten Induktionsbeweise sind elementarer als die folgenden.

[1] Die folgenden Sätze und Beweise benutzen die Ordnung auf $\mathbb{N}$ sowie einige elementare Eigenschaften natürlicher Zahlen, die im folgenden Abschnitt behandelt werden. Sie sind der Übersichtlichkeit wegen vorgezogen worden und können zunächst übersprungen und dann nachgeholt werden.

5.1.2 Die Ordnung auf $\mathbb{N}$

Wir müssen zunächst die anschauliche Vorstellung von der mengentheoretischen Darstellung der natürlichen Zahlen mathematisch streng machen.

Satz 86: *Für alle $n \in \mathbb{N}$ gilt:*

(i) Aus $x \in n$ folgt $x \in \mathbb{N}$ und $x \subseteq n$.

(ii) Aus $x \in \mathbb{N}$ und $x \subseteq n$ und $x \neq n$ folgt $x \in n$.

(iii) Es gilt $n \notin n$ und insbesondere $n \neq n + 1$.

BEWEIS: Wir beweisen die Aussagen durch Induktion nach n.

(i) Da $x \in 0 = \emptyset$ immer falsch ist, ist die Implikation und damit der Induktionsanfang wahr. Nehmen wir nun an, die Behauptung gelte für ein beliebiges n. Per Konstruktion ist $n + 1 \in \mathbb{N}$. Aus $x \in n + 1 = n \cup \{n\}$ folgt sofort $x \in n$ oder $x = n$. Im ersten Fall folgt aus der Induktionsannahme $x \in \mathbb{N}$ und $x \subseteq n \subseteq n + 1$. Im zweiten Fall ist $x = n \in \mathbb{N}$ und $x = n \subseteq n + 1$. Damit folgt die Behauptung für $n + 1$.

(ii) Die Aussage lautet formal

$$A(n)\colon \bigvee_{x \in \mathbb{N}} : (x \subseteq n \wedge x \neq n \Rightarrow x \in n).$$

Es ist wieder $A(0)$ trivialerweise wahr. Gilt nun $A(n)$ für ein n, so betrachte $x \in \mathbb{N}$ mit $x \subseteq n + 1$ und $x \neq n + 1$. Es gilt $n \notin x$, denn aus $n \in x$ würde mit (i) direkt $n \subseteq x$ und somit

$$n + 1 = n \cup \{n\} \subseteq x \cup \{n\} \subseteq x \subseteq n + 1$$

folgen, was $x \neq n + 1$ widerspricht. Aus $x \subseteq n + 1 = n \cup \{n\}$ und $n \notin x$ folgt somit $x \subseteq n$. Im Fall $x = n$ ist $x \subseteq n + 1$ klar. Gilt stattdessen $x \neq n$, so folgt aus der Induktionsannahme $x \in n \subseteq n + 1$.

(iii) Die letzte Aussage ist $A(n)\colon n \notin n$. Natürlich ist $A(0)$ wahr. Die Aussage gelte nun für ein n. Wir müssen nun $n + 1 \notin n + 1$ zeigen. Angenommen, es gelte $n + 1 \in n + 1 = n \cup \{n\}$. Daraus folgt $n + 1 \in n$ oder $n + 1 = n \cup \{n\} \in \{n\}$, d. h. $n \cup \{n\} = n$. Im ersten Fall folgt aus (i) $n + 1 = n \cup \{n\} \subseteq n$, also insbesondere $n \in n$, genauso wie im zweiten Fall — Widerspruch zur Induktionsannahme! □

Mit diesem Hilfssatz können wir nun zur angesprochenen Ordnungsrelation kommen. Weiter erhalten wir die schon erwähnte Darstellung $n = \{0, 1, \ldots, n - 1\}$.

Satz 87: *Durch $n \leq m :\Leftrightarrow n \subseteq m$ wird auf $\mathbb{N}$ eine totale Ordnung definiert. Zusätzlich gilt $n = \{\, m \in \mathbb{N} \mid m < n \,\}$.*

BEWEIS: Reflexivität, Antisymmetrie und Transitivität sind klar. Für den Rest verwenden wir wieder einen Induktionsbeweis. Die Aussage ist dann

$$A(n)\colon \bigvee_{m\in\mathbb{N}} : n \subseteq m \vee m \subseteq n.$$

Der Induktionsanfang $A(0)$ ist wegen $0 = \emptyset \subseteq m$ für alle $m \in \mathbb{N}$ erfüllt. Sei nun $A(n)$ für ein n gültig. Für ein beliebiges $m \in \mathbb{N}$ gilt immer $n \subseteq m \wedge n \neq m$ oder $m \subseteq n$. Im ersten Fall führt Satz 86.(ii) auf $n \in m$, und somit gilt

$$n + 1 = n \cup \{n\} \subseteq m \cup \{n\} \subseteq m,$$

also $n + 1 \leq m$. Im zweiten Fall ist $m \subseteq n \subseteq n + 1$, also $m \leq n + 1$.

Zur Darstellung von n: Falls $m \in n$ folgt mit Satz 86.(i) direkt $m \subseteq n$ und somit $m \leq n$. Da nach Satz 86.(iii) stets $n \notin n$ gilt, folgt $m \notin n$ und daher $m < n$. Ist umgekehrt $m < n$, so folgt $m \subseteq n$ und $m \neq n$, also $m \in n$ nach Satz 86.(ii). □

5.1.3 Abbildungen zwischen endlichen Mengen

Bevor wir Verknüpfungen zwischen natürlichen Zahlen einführen können, müssen wir zunächst Abbildungen zwischen endlichen Mengen genauer untersuchen.

Satz 88: *Seien $m, n \in \mathbb{N}$.*

(i) Ist eine Abbildung $f\colon n \to n$ injektiv, so ist sie auch surjektiv.

(ii) Gibt es eine Bijektion $f\colon n \to m$, so ist $n = m$.

(iii) Sei M eine Menge. Gibt es Bijektionen $f\colon n \to M$ und $g\colon m \to M$, so ist $n = m$.

BEWEIS:

(i) Wir zeigen die Behauptung wieder durch Induktion nach n und betrachten zunächst $n = 0 = \emptyset$. Eine Abbildung $f\colon \emptyset \to \emptyset$ ist immer surjektiv, da es kein $y \in \emptyset$ gibt, für das man ein $x \in \emptyset$ finden müsste mit $f(x) = y$.

Sei die Behauptung also richtig für ein $n \in \mathbb{N}$, und betrachte eine injektive Abbildung $f\colon n+1 \to n+1$. Dann ist auch die Einschränkung $f|_n$ von f auf $n \subseteq n+1 = n \cup \{n\}$ injektiv, und ihr Bild kann in n enthalten sein oder nicht.

Im ersten Fall ist $f|_n$ nach Induktionsvoraussetzung surjektiv, d. h. das Bild der Menge n unter der Abbildung $f|_n$ und somit auch unter f ist die Menge n. Da f injektiv ist, muss dann das Bild des Elements n das Element n sein. Somit ist f surjektiv.

Sei nun $f|_n(n) \not\subseteq n$. Dann gibt es ein $m < n$ mit $f(m) = n$. Da f injektiv ist, muss $f(n) < n$ gelten. Betrachte nun die Abbildung

$$\widetilde{f}\colon n+1 \longrightarrow n+1\colon x \longmapsto \begin{cases} f(n) & x = m \\ f(x) \quad \text{falls} & x \neq m, n \\ n & x = n. \end{cases}$$

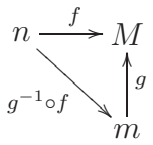
Sie ist ebenfalls injektiv, da nur die Bilder von f permutiert werden. Wegen $\widetilde{f}(n) = n$ ist $\widetilde{f}(x) \neq n$ für alle $x < n$. Damit zeigt die Argumentation des ersten Falls, dass $\widetilde{f}$ surjektiv ist. Dann ist auch f surjektiv.

(ii) Wir können nach Satz 87 o. E. $m \subseteq n$ annehmen. Die kanonische Injektion

$$g\colon m \longrightarrow n\colon x \longmapsto x$$

ist injektiv. Nach Aufgabe 8 a) ist dann auch $g \circ f\colon n \to n$ injektiv und nach Teil (i) auch surjektiv. Nun zeigt Aufgabe 8 b), dass g surjektiv ist, und daher ist $m = g(m) = n$.

(iii) Das Diagramm



kommutiert. Wendet man auf die Bijektion $g^{-1} \circ f\colon n \to m$ Teil (ii) an, so folgt die Behauptung. □

Wir können nun die vormals intuitiv eingeführte Mächtigkeit endlicher Mengen formalisieren.

Definition 57: *Eine Menge M heißt* endlich*, wenn es ein $n \in \mathbb{N}$ und eine Bijektion $n \to M$ gibt. Die Zahl n heißt* Mächtigkeit *von M.*

Diese Bijektion $n \to M\colon k \mapsto x_k$ definiert ein *Aufzählung* $(x_k)_{k\in n}$ der Elemente $x_k \in M$. Benutzt man $n = \{0, \ldots, n-1\}$, so erhält man die gewohnte Notation $(x_k)_{k=0,\ldots,n-1}$ für diese Familie.

Sei nun M eine beliebige Menge. Für ein $n \in \mathbb{N}$ definiert jede Abbildung $n \to M$ (die weder injektiv noch surjektiv zu sein braucht) eine *endliche Folge* aus Elementen von M, geschrieben wieder $(x_k)_{k=0,\ldots,n-1}$. Eine Abbildung $\mathbb{N} \to M$ heißt *unendliche Folge* von Elementen aus M, geschrieben $(x_k)_{k\in\mathbb{N}}$. Die Menge aller endlichen bzw. unendlichen Folgen wird mit M^n bzw. $M^{\mathbb{N}}$ bezeichnet.

5.1.4 Die Addition und Multiplikation in $\mathbb{N}$

Wir führen nun die Bezeichnung $\mathbb{N}^* := \mathbb{N}\setminus\{0\}$ ein. Um die Verknüpfungen natürlicher Zahlen zu erklären, müssen wir zunächst die *Nachfolgerfunktion* auf $\mathbb{N}$ studieren.

Satz 89: *Die Abbildung $f\colon \mathbb{N} \to \mathbb{N}^*\colon n \mapsto n + 1$ ist bijektiv.*

BEWEIS: Wir beweisen die Surjektivität durch Induktion über n. Es ist $f(0) = 0 + 1 = 1$, d. h. 1 hat ein Urbild unter f. Weiter ist $f(n) = n + 1$, also hat $n + 1$ ebenfalls ein Urbild.

Seien nun $m, n \in \mathbb{N}$ mit $m \neq n$. Wir können o. E. $m < n$ annehmen. Nun folgt

$$f(m) = m + 1 \leq n < n + 1 = f(n),$$

also $f(m) \neq f(n)$, wobei Aufgabe 29 verwendet wurde. □

Dieser Satz zeigt, dass für jedes $n \in \mathbb{N}^*$ genau ein $m \in \mathbb{N}$ existiert mit $n = m + 1$. Die Zahl n heißt der *Nachfolger* von m und m der *Vorgänger* von n. Man schreibt $m = n - 1$.

Eine wichtige Eigenschaft der natürlichen Zahlen ist die Tatsache, dass die totale Ordnung auf $\mathbb{N}$ sogar eine Wohlordnung ist (siehe dazu auch Anhang A).

Satz 90 (Wohlordnungsprinzip): *Die Menge der natürlichen Zahlen ist wohlgeordnet, d. h. jede nichtleere Teilmenge von $\mathbb{N}$ besitzt ein Minimum.*

BEWEIS: Angenommen, eine nichtleere Teilmenge $M \subseteq \mathbb{N}$ hätte kein Minimum. Dann muss $0 \notin M$ sein, denn sonst wäre 0 ein Minimum, da nach Satz 2 gilt $0 \leq m$, d. h. $\emptyset \subseteq m$, für alle $m \in \mathbb{N}$. Daher ist $0 < m$ für alle $m \in M$ und folglich Element der Menge $N := \{\, n \in \mathbb{N} \mid n < m \text{ für alle } m \in M \,\}$. Sei nun $n \in N$ gegeben. Dann gilt $n < m$ und nach Aufgabe 29 auch noch $n + 1 \leq m$ für alle $m \in M$. Weil M aber kein Minimum haben sollte, muss sogar $n + 1 < m$ für alle $m \in M$ und somit $n + 1 \in N$ gelten. Durch Induktion folgt also $N = \mathbb{N}$. Für jedes $m \in M \subseteq \mathbb{N}$ gilt daher $m < m$, was ein Widerspruch ist. □

Da wir die Verknüpfungen von natürlichen Zahlen induktiv definieren, müssen wir zunächst zeigen, dass induktive Definitionen überhaupt möglich und wohldefiniert sind. Dies liefert der wichtige

Satz 91 (Rekursionssatz): *Sei M eine Menge, $g\colon M \to M$ eine Abbildung und $x \in M$. Dann gibt es genau eine Abbildung $f\colon \mathbb{N} \to M$, so dass gilt:*

(i) $f(0) = x$

(ii) $f(n+1) = g(f(n))$ *für alle* $n \in \mathbb{N}$.

BEWEIS: Wir zeigen zuerst die Existenz. Dazu konstruieren wir die Abbildung f mengentheoretisch, d. h. über ihren Graphen $\mathrm{Gr} f$. Betrachten wir also die Produktmenge $\mathbb{N} \times M$. Eine Teilmenge $O \subseteq \mathbb{N} \times M$ heißt *rekursiv*, wenn $(0, x) \in O$ und die Implikation

$$(m, y) \in O \Rightarrow (m + 1, g(y)) \in O$$

für alle $m \in \mathbb{N}$ und $y \in M$ gilt. Es bezeichne R die Menge aller rekursiven Teilmengen von $\mathbb{N} \times M$. Wegen $\mathbb{N} \times M \in R$ ist R nicht leer. Wir zeigen nun, dass die Menge

$$D := \bigcap_{O \in R} O$$

rekursiv ist. Zunächst ist $(0, x) \in D$, da $(0, x) \in O$ für alle $O \in R$. Ist weiter $(m, y) \in D$, so ist $(m, y) \in O$ für alle $O \in R$. Da die Mengen O rekursiv sind, ist auch $(m + 1, g(y)) \in O$ für alle $O \in R$, und folglich ist $(m + 1, g(y)) \in D$.

Wir zeigen jetzt, dass D der Graph einer Abbildung $f\colon \mathbb{N} \to M$ ist, d. h. für alle $n \in \mathbb{N}$ gibt es genau ein $y \in M$ mit $(n, y) \in D$. Wir beweisen dies durch Induktion über n.

Für $n = 0$ ist $(0, x) \in D$. Angenommen, es gäbe ein weiteres $x \neq \widetilde{x} \in M$ mit $(0, \widetilde{x}) \in D$. Dann betrachten wir die Menge $\widetilde{D} := D \setminus \{(0, \widetilde{x})\}$. Es ist aber auch $\widetilde{D}$ rekursiv, da $(0, x) \in \widetilde{D}$

und aus $(m, y) \in \widetilde{D}$ folgt $(m+1, g(y)) \in \widetilde{D}$. Nach Konstruktion von D muss also $D \subseteq \widetilde{D}$ sein, was ein Widerspruch zur Wahl von $\widetilde{D}$ ist.

Nun gelte die Behauptung für ein $n \in \mathbb{N}$, d. h. es gebe genau ein $y \in M$ mit $(n, y) \in D$. Es ist auch $(n+1, g(y)) \in D$. Angenommen, es existierte $g(y) \neq z \in M$ mit $(n+1, z) \in D$. Wir betrachten wieder die Menge $\widetilde{D} := D \setminus \{(n+1, z)\}$. Sie ist wieder rekursiv. Denn es gilt $(0, x) \in \widetilde{D}$, und für $(m, \widetilde{y}) \in \widetilde{D}$ ist zunächst $(m+1, g(\widetilde{y})) \in D$. Wir müssen nun die Fälle $m \neq n$ und $m = n$ unterscheiden. Für $m \neq n$ ist $(m+1, g(\widetilde{y})) \neq (n+1, z)$ und daher auch $(m+1, g(\widetilde{y})) \in \widetilde{D}$. Für $m = n$ gilt nach Voraussetzung $\widetilde{y} = y$, also ebenfalls $(m+1, g(\widetilde{y})) \in \widetilde{D}$. Erneut folgt als $D \subseteq \widetilde{D}$ ein Widerspruch zur Konstruktion von $\widetilde{D}$.

Damit ist D der Graph einer Abbildung f mit den gewünschten Eigenschaften, denn wegen $(0, x) \in D$ gilt $f(0) = x$, und aus der Implikation $(n, y) \in D \Rightarrow (n+1, g(y)) \in D$ erhält man $f(n+1) = g(f(n))$ für alle $n \in \mathbb{N}$.

Wir haben nun noch die Eindeutigkeit von f zu zeigen. Sei dazu $\widetilde{f}$ eine weitere Abbildung mit obigen Eigenschaften. Wir zeigen $f(n) = \widetilde{f}(n)$ für alle $n \in \mathbb{N}$.

Zunächst ist $f(0) = x = \widetilde{f}(0)$. Gilt nun für ein $n \in \mathbb{N}$ die Gleichung $f(n) = \widetilde{f}(n)$, so folgt

$$f(n+1) = g(f(n)) = g(\widetilde{f}(n)) = \widetilde{f}(n+1),$$

und damit ist alles bewiesen. □

Mit anderen Worten liefert dieser Satz die Existenz einer Folge $(x_n)_{n\in\mathbb{N}}$ mit $x_{n+1} = g(x_n)$, wenn nur ein $x_0 \in M$ und $g\colon M \to M$ gegeben ist. Man spricht daher von einer *rekursiv definierten Folge*.

Die Addition definieren wir nun über $n + 0 := n$ und $n + (m+1) := (n+m) + 1$, indem wir für g die Nachfolgerfunktion wählen. Man rechnet dann z. B.

$$3 + 2 = 3 + (1+1) = (3+1) + 1 = 4 + 1 = 5.$$

Satz 92: *Das Paar $(\mathbb{N}, +)$ ist ein kommutatives Monoid mit neutralem Element 0. Zusätzlich gilt die Kürzungsregel, und die Addition ist mit der Ordnung auf $\mathbb{N}$ verträglich.*

BEWEIS: Wir beweisen die Eigenschaften durch Induktion. Die Rechtsneutralität der 0 gilt per Definition. Wir beweisen das Assoziativgesetz durch Induktion über k bei beliebigen $n, m \in \mathbb{N}$. Der Induktionsanfang ist

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

Angenommen nun, das Assoziativgesetz gelte für ein beliebiges k. Dann folgt

$$\begin{aligned}(n+m) + (k+1) &= ((n+m)+k) + 1 = (n + (m+k)) + 1) \\ &= n + ((m+k)+1) = n + (m + (k+1)).\end{aligned}$$

Damit ist gezeigt, dass es auch für $k+1$ gilt. Das Kommutativgesetz folgt analog. Mit dem Induktionsanfang $0 + 0 = 0$ und dem Induktionsschluss

$$0 + n = (0 + (n-1)) + 1 = (n-1) + 1 = n$$

erhält man auch die Linksneutralität von 0. Die Kürzungsregel ergibt sich aus der Tatsache, dass die Abbildung $n \mapsto n+1$ injektiv ist (Satz 89). Zum Schluss beweisen wir noch die Verträglichkeit. Wir müssen die Implikation $n \leq m \Rightarrow n+k \leq m+k$ zeigen. Der Induktionsanfang $k = 0$ ist klar. Zum Induktionsschluss betrachtet man

$$n + (k+1) \leq m + (k+1) \Leftrightarrow (n+1) + k \leq (m+1) + k. \qquad \square$$

Man kann nun Satz 89 dahingehend verallgemeinern, dass die Abbildung

$$\mathbb{N} \longrightarrow \{\, m \in \mathbb{N} \mid m \geq k \,\} \colon n \longmapsto n + k$$

für alle $k \in \mathbb{N}$ bijektiv ist (siehe Aufgabe 30). Daher hat die Gleichung $n + k = m$ genau dann eine Lösung, wenn $n \leq m$ gilt. Ist dies erfüllt, so ist die Lösung eindeutig und wird mit $m - n$ bezeichnet.

Damit kommen wir auch schon zur Multiplikation. Diese definieren wird induktiv durch $n \cdot 0 := 0$ und $n \cdot (m+1) := n \cdot m + n$.

Satz 93: *Das Paar $(\mathbb{N}, \cdot)$ ist ein kommutatives Monoid mit neutralem Element 1. Zusätzlich ist jedes $n \neq 0$ kürzbar, das Distributivgesetz gilt, und die Multiplikation ist verträglich mit der Ordnung auf $\mathbb{N}$.*

Wir werden auf den äußerst sperrigen Beweis verzichten. Stattdessen zeigen wir die Nützlichkeit der mengentheoretischen Definition von $\mathbb{N}$. Dazu benötigen wir zunächst einen Hilfssatz.

Satz 94: *Seien M, N endliche Mengen. Dann ist $|M \times N| = |M| \cdot |N|$.*

BEWEIS: Wir führen den Beweis durch Induktion nach der Anzahl der Elemente n von N. Ist $n = 0$, so ist $N = \emptyset$ und auch $M \times N = \emptyset$, die Formel stimmt also. Sei die Formel nun gültig für n und betrachte eine Menge N mit $n+1$ Elementen. Dann gilt nach Wahl von $x \in N$

$$M \times N = (M \times \{x\}) \cup (M \times (N \setminus \{x\}))$$

und folglich

$$|M \times N| = |M \times \{x\}| + |M \times (N \setminus \{x\})| = |M| + |M| \cdot n = |M| \cdot (n+1) = |M| \cdot |N|$$

nach Induktionsvoraussetzung. $\square$

Wir betrachten nun die Ausdrücke M^2 und $M \times M$. Dabei ist M^2 die Menge aller Abbildungen von $2 = \{\emptyset, \{\emptyset\}\}$ nach M und $M \times M$ das kartesische Produkt. Wir wissen aus obigem Satz, dass $M \times M$ genau m^2 Elemente hat, wenn m die Anzahl der Elemente von M ist. Soviele Elemente hat aber auch M^2. Wir müssen nämlich zur Definition einer Abbildung $2 \to M$ die Bilder von $\emptyset$ und $\{\emptyset\}$ festlegen. Für jedes Urbild gibt es m Möglichkeiten, da M gerade m Elemente hat. Da die Wahl der Bilder unabhängig voneinander ist, erhalten wir somit m^2 Abbildungen von 2 nach M. Wir können auch die Elemente von M^2 und $M \times M$ direkt miteinander identifizieren, und zwar das Element $(x, y) \in M \times M$ mit der Abbildung $\emptyset \mapsto x$,

$\{\emptyset\} \mapsto y$. Wir brauchen die beiden Mengen daher nicht zu unterscheiden. Eine ähnliche Überlegung gilt für den Ausdruck M^n und das n-fache kartesische Produkt von M mit sich selbst. Man könnte daher $m^n := |m^n|$ definieren, wobei links die Potenz und rechts die Familie gemeint ist. Diese beiden Notationen sind also konsistent. Insbesondere ist dann $0^0 = 1$, denn es gibt genau eine Abbildung $\emptyset \to \emptyset$, und zwar die leere.

Es ist bemerkenswert, dass man mit dieser Überlegung, obigem Satz und Aufgabe 31 sämtliche Rechenarten auf die Mächtigkeit von endlichen Mengen zurückführen kann!

5.1.5 Summen- und Produktzeichen

Hat man mehr als zwei Summanden bzw. Faktoren, so ist eine abkürzende Schreibweise wünschenswert. Betrachten wir konkret eine Menge M, auf der Verknüpfungen $+$ und $\cdot$ definiert sind. Für $m, n \in \mathbb{N}$ mit $m \leq n$ können wir dann eine endliche Folge $(x_k)_{k=m,\dots,n}$ aus M wählen. Man definiert dann induktiv

$$\sum_{k=m}^{m} x_k := x_m, \qquad \prod_{k=m}^{m} x_k := x_m$$

und für alle $m \leq l < n$

$$\sum_{k=m}^{l+1} x_k := \left(\sum_{k=m}^{l} x_k\right) + x_{l+1}, \qquad \prod_{k=m}^{l+1} x_k := \left(\prod_{k=m}^{l} x_k\right) \cdot x_{l+1}.$$

Man beachte, dass hier k eine gebundene Variable ist, die lediglich zu Notationszwecken eingeführt wird. Sie kann durch jede andere noch nicht verwendete Variable ersetzt werden.

Sind die Operationen assoziativ, so kann man für alle $m \leq l < n$

$$\sum_{k=m}^{n} x_k = \left(\sum_{k=m}^{l} x_k\right) + \left(\sum_{k=l+1}^{n} x_k\right)$$

und

$$\prod_{k=m}^{n} x_k = \left(\prod_{k=m}^{l} x_k\right) \cdot \left(\prod_{k=l+1}^{n} x_k\right)$$

schreiben. Sind sie zusätzlich kommutativ, so gilt für alle endlichen Folgen $(x_k)_{k=m,\dots,n}$, $(y_k)_{k=m,\dots,n} \subseteq M$

$$\sum_{k=m}^{n} (x_k + y_k) = \left(\sum_{k=m}^{n} x_k\right) + \left(\sum_{k=m}^{n} y_k\right)$$

und

$$\prod_{k=m}^{n} (x_k \cdot y_k) = \left(\prod_{k=m}^{n} x_k\right) \cdot \left(\prod_{k=m}^{n} y_k\right).$$

Besitzt M neutrale Elemente, so kann man sich oft Fallunterscheidungen sparen, indem man für ungültige Summations- bzw. Produktgrenzen den Ausdruck mit dem entsprechenden neutralen Element gleichsetzt. Ist also $n < m$, so ist

$$\sum_{k=m}^{n} x_k := 0, \qquad \prod_{k=m}^{n} x_k := 1.$$

Gilt in M zur Assoziativität auch noch das Distributivgesetzt, so kann man

$$\left(\sum_{k=m}^{n} x_k\right) \cdot \left(\sum_{l=p}^{q} y_l\right) = \sum_{k=m}^{n} \left(\sum_{l=p}^{q} x_k \cdot y_l\right) = \sum_{l=p}^{q} \left(\sum_{k=m}^{n} x_k \cdot y_l\right)$$

rechnen.

Wichtig für das Rechnen sind noch die Indextransformationen. Dabei ist das Ziel, die Summe bzw. das Produkt mit vorgegebener unterer Grenze zu schreiben. Es laufe etwa k von m bis n. Wollen wir erreichen, dass die Laufvariable l bei p startet, so müssen wir $l = k - m + p$ wählen und bis $n - m + p$ laufen. Daher ist

$$\sum_{k=m}^{n} x_k = \sum_{l=p}^{n-m+p} x_{l+m-p}, \qquad \prod_{k=m}^{n} x_k = \prod_{l=p}^{n-m+p} x_{l+m-p}.$$

Manchmal ist es auch unpraktisch, untere und obere Grenze explizit wählen zu müssen. Ist J eine endliche Menge mit Mächtigkeit n, so wählt man eine Aufzählung f der Elemente von J und definiert

$$\sum_{j \in J} x_j := \sum_{k=0}^{n-1} x_{f(k)}, \qquad \prod_{j \in J} x_j := \prod_{k=0}^{n-1} x_{f(k)}.$$

Natürlich müssen die Verknüpfungen dann kommutativ sein, damit das Ergebnis nicht von der Wahl der Aufzählung abhängt.

Oft ist es nützlich, für bestimmte Summen explizite Formeln zu haben. Das berühmteste Beispiel ist der

Satz 95 (Gauß'sche Summenformel): *Für alle $n \in \mathbb{N}^*$ gilt*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

BEWEIS: Es ist

$$\sum_{k=1}^{n} k = \sum_{k=1}^{n} (n + 1 - k),$$

da lediglich die Summationsreihenfolge umgedreht wird. Bezeichnet N den Wert der Summe, so folgt

$$2N = \sum_{k=1}^{n} k + \sum_{k=1}^{n} (n + 1 - k) = \sum_{k=1}^{n} (n + 1) = n(n + 1).$$

Das ist auch schon die Behauptung. □

Dieses Ergebnis verwenden wir nun, um die Beweislücke in Satz 12 zu schließen.

Satz 96: *Die Abbildung*

$$f\colon \mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N}\colon (i,j)\longmapsto \frac{(i+j)(i+j+1)}{2}+j.$$

ist eine Bijektion.

BEWEIS: Wir betrachten zunächst die Teilabbildung $g\colon (i,j)\mapsto(i+j,j)$. Sie ist eine Bijektion von $\mathbb{N}\times\mathbb{N}$ auf die Menge $M := \{\,(n,m)\in\mathbb{N}\times\mathbb{N}\mid m\le n\,\}$. Die Gleichungen $i+j=n$ und $j=m$ sind nämlich genau dann durch $i,j\in\mathbb{N}$ lösbar, wenn $m\le n$ gilt, und diese Lösung ist durch $j=m$ und $i=n-j$ eindeutig bestimmt.

Wir betrachten nun weiter die Abbildung

$$h\colon M\longrightarrow\mathbb{N}\colon (n,m)\longmapsto\sum_{k=0}^{n}(k+1)-(n-m)-1.$$

Sie ist ebenfalls eine Bijektion. Für ein gegebenes $n\in\mathbb{N}$ gibt es genau $n+1$ passende $m\in\mathbb{N}$, so dass $(n,m)\in M$ ist. Die Summe liefert also die Gesamtzahl aller Paare bis zur Zahl n. Davon wird noch $n-m$ abgezogen, was gerade die Zahl der Paare aus M mit erster Komponente n und zweiter Komponente strikt größer als m ist. Daher ist der Wert der ersten beiden Summanden gerade die Anzahl aller Paare bis (n,m). Der letzte Summand legt noch fest, dass das Paar $(0,0)$ auf 0 abgebildet wird.

Durch Komposition dieser beiden Abbildungen erhält man die gesuchte Abbildung f. Es ist nämlich nach Satz 95

$$\sum_{k=0}^{n}(k+1)=\frac{n(n+1)}{2}+(n+1)$$

und folglich

$$h(n,m)=\frac{n(n+1)}{2}+m.$$

Daraus ergibt sich insgesamt

$$f(i,j)=(h\circ g)(i,j)=h(i+j,j)=\frac{(i+j)(i+j+1)}{2}+j.$$ □

Eine weitere wichtige Formel ist die *geometrische Summenformel*. Sie ist deshalb so wichtig, weil geometrische Summen praktisch die einzigen nichttrivialen Summen sind, die man direkt berechnen kann.

Satz 97 (Geometrische Summenformel): *Seien R ein Ring, $x\in R$ und $m,n\in\mathbb{N}$. Dann gilt*

$$(1-x)\sum_{k=m}^{n}x^k=x^m-x^{n+1}.$$

Ist R sogar ein Körper und $x\neq 1$, so ist

$$\sum_{k=m}^{n}x^k=\frac{x^m-x^{n+1}}{1-x}.$$

BEWEIS:

$$(1-x)\sum_{k=m}^{n} x^k = \sum_{k=m}^{n} x^k - \sum_{k=m}^{n} x^{k+1} = x^m + \sum_{k=m+1}^{n} x^k - \sum_{k=m+1}^{n} x^k - x^{n+1} = x^m - x^{n+1}$$

□

5.1.6 Darstellung natürlicher Zahlen im g-al-System

Wir sind es gewöhnt, zur Darstellung von Zahlen ein Stellenwertsystem, und zwar vornehmlich dasjenige zur Basis $g = 10$, zu verwenden. In diesem Abschnitt soll die Theorie dieser Stellenwertsysteme entwickelt werden, um diese Notation und das Rechnen in ihr auf eine solide mathematische Grundlage zu stellen. Grundlegend dafür ist die Division mit Rest, die auch für die elementare Zahlentheorie sehr wichtig ist.

Satz 98 (Satz von Euklid): *In $\mathbb{N}$ gilt die Division mit Rest: Für jedes $n \in \mathbb{N}$ und $m \in \mathbb{N}^*$ exsitieren eindeutig bestimmte $q, r \in \mathbb{N}$ mit $n = q \cdot m + r$ und $r < m$.*

BEWEIS: Sei $m \in \mathbb{N}^*$ gegeben. Wir beweisen zunächst die Existenz von q und r durch Induktion über n. Für $n = 0$ erfüllen sicher $q = r = 0$ die Bedingung.

Die Existenz sei nun für ein $n \in \mathbb{N}$ gesichert, d. h. es existiere eine Darstellung $n = qm + r$ mit $r < m$. Dann ist $n + 1 = qm + r + 1$. Im Fall $r + 1 < m$ sind wir bereits fertig. Falls $r + 1 = m$ gilt, so ist $n + 1 = (q + 1)m$ eine Darstellung der geforderten Art. Damit ist die Existenz für alle $n \in \mathbb{N}$ gezeigt.

Nun nehmen wir an, es gebe eine weitere Darstellung $n = \widetilde{q}m + \widetilde{r}$ mit $\widetilde{r} < m$. Da $qm + r = \widetilde{q}m + \widetilde{r}$ können wir $q \neq \widetilde{q}$ annehmen, ansonsten könnten wir qm kürzen und erhielten $r = \widetilde{r}$. Da $\mathbb{N}$ total geordnet ist, können wir o. E. $q < \widetilde{q}$ annehmen. Dann existiert ein $k \in \mathbb{N}$ mit $q + k = \widetilde{q}$. Daher folgt aus

$$qm + r = \widetilde{q}m + \widetilde{r} = (q + k)m + \widetilde{r} = qm + km + \widetilde{r}$$

die Beziehung $r = km + \widetilde{r} \geq km \geq m$. Widerspruch! □

Wir können nun zunächst die Existenz von g-al-Darstellungen zeigen.

Satz 99: *Sei $g \in \mathbb{N}$ mit $g > 1$ gegeben. Dann gibt es für alle $n \in \mathbb{N}$ ein $m \in \mathbb{N}$ und eine Folge $(a_k)_{k=0,\ldots,m}$ mit $a_k < g$ und*

$$a_m a_{m-1} \cdots a_1 a_{0_g} := \sum_{k=0}^{m} a_k g^k = n,$$

einer g-al Darstellung oder Darstellung im g-al-System von n.

BEWEIS: Nach dem Satz von Euklid können wir $q_0 := n$ darstellen als $q_0 = q_1 g + r_0$ mit $r_0 < g$. Dann zerlegen wir q_1 weiter in $q_1 = q_2 g + r_1$ mit $r_1 < g$ usw. mit immer kleineren q_i. Die Folge der q_i ist eine nichtleere Teilmenge von $\mathbb{N}$ hat als solche nach Satz 90 ein minimales Element. Dieses minimale Element muss 0 sein, da ansonsten eine weitere Zerlegung möglich wäre. Es gibt also ein $m \in \mathbb{N}$, so dass $q_{m+1} = 0$ gilt. Wir erhalten somit

$$\begin{aligned} q_0 &= q_1 g + r_0 \\ &= (q_2 g + r_1) g + a_0 = q_2 g^2 + r_1 g + r_0 \\ &= \cdots \\ &= q_{m+1} g^{m+1} + r_m g^m + \cdots + r_1 g + r_0. \end{aligned}$$

Wegen $q_{m+1} = 0$ ist durch $a_k := r_k$ eine Darstellung der gewünschten Form gefunden. □

Man beachte, dass wir die Konstruktion der Darstellung abgebrochen haben, sobald die führende Ziffer von 0 nicht mehr verschieden sein konnte. Das ist aber bei der Definition der g-al-Darstellung keineswegs gefordert. So sind $1_g = 01_g = 001_g = \cdots$ verschiedene g-al-Darstellungen derselben Zahl.

Von praktischer Bedeutung sind vor allem das Dualsystem mit $g = 2$, das Oktalsystem mit $g = 8$, das Dezimalsystem mit $g = 10$ und das Hexadezimalsystem mit $g = 16$. Im letzteren benötigt man noch zusätzliche Ziffern für die Zahlen 10 bis 15 und verwendet dafür die Buchstaben A bis F. Es ist z. B.

$$47_{10} = 2F_{16} = 57_8 = 101111_2.$$

Natürlich verwenden wir zur Notation von konkreten Zahlen, wenn nichts weiter gesagt wird, immer das Dezimalsystem.

Satz 100: *Seien $a = a_m \cdots a_{0_g}$ und $b = b_n \cdots b_{0_g}$ Darstellungen im g-al-System. Ist $a_m > 0$ und $m > n$, so ist $a > b$.*

BEWEIS: Wegen $b_k < g$ für alle k gilt

$$b = \sum_{k=0}^{n} b_k g^k \leq (g-1) \sum_{k=0}^{n} g^k = g^{n+1} - 1 < g^{n+1} \leq g^m \leq a_m g^m \leq \sum_{k=0}^{m} a_k g^k = a,$$

wobei die geometrische Summenformel[2] benutzt wurde. □

Wir haben damit ein einfaches Kriterium, um verschieden lange g-al-Darstellungen miteinander zur vergleichen. Es unterscheidet sich praktisch nicht von unserem gewohnten Umgang mit dem Dezimalsystem, obwohl es eher unüblich ist, führende Nullen zu schreiben. Auch der Größenvergleich gleich langer g-al-Darstellungen funktioniert wie gewohnt.

Satz 101: *Seien $a = a_m \cdots a_{0_g}$ und $b = b_m \cdots b_{0_g}$ Darstellungen im g-al-System.*

[2] Man überlege sich, wieso man sie hier anwenden darf!

(i) Ist $a_m > b_m$, so ist $a > b$.

(ii) Ist $a_m = b_m$, $a_{m-1} = b_{m-1}$, …, $a_{i+1} = b_{i+1}$ und $a_i > b_i$, so ist $a > b$.

BEWEIS:

(i) Wir benutzen wieder die geometrische Summenformel und rechnen

$$b = \sum_{k=0}^{n} b_k g^k \leq b_m g^m + (g-1)\sum_{k=0}^{m-1} g^k = b_m g^m + g^m - 1$$
$$= (b_m + 1)g^m - 1 \leq a_m g^m - 1 < a_m g^m \leq \sum_{k=0}^{m} a_k g^k = a.$$

(ii) Wir ziehen von a und b die Zahl

$$\sum_{k=i+1}^{m} a_m g^m$$

ab und benutzen Teil (i). □

Wir können nun die Eindeutigkeit von g-al-Darstellungen zeigen, wenn man solche mit führenden Nullen nicht berücksichtigt.

Satz 102: *Seien $a = a_m \cdots a_{0_g}$ und $b = b_n \cdots b_{0_g}$ Darstellungen im g-al-System mit $a_m > 0$ und $b_n > 0$. Dann ist $a = b$ genau dann, wenn $m = n$ ist und $a_k = b_k$ für alle k.*

BEWEIS: Es sei $a = b$. Angenommen $m \neq n$, etwa $m > n$. Dann wäre nach Satz 100 $a > b$. Wäre $m = n$, aber ein $a_k \neq b_k$, so wäre nach Satz 101.(ii) ebenfalls $a \neq b$. Damit bleibt nur $m = n$ und $a_k = b_k$ für alle k übrig. Die Umkehrung ist klar. □

Wir gehen nun noch kurz darauf ein, wie man mit g-al-Darstellungen rechnet. Dazu nehmen wir $a \geq b$ an und betrachten

$$a = \sum_{k=0}^{m} a_k g^k$$

mit $a_m > 0$ und

$$b = \sum_{k=0}^{m} b_k g^k,$$

wobei b_g eventuell führende Nullen haben kann Dann ist zwar $a + b$ durch

$$\sum_{k=0}^{m} (a_k + b_k) g^k$$

gegeben, dies muss aber keine g-al-Darstellung mehr sein! Dafür muss nämlich noch $a_k + b_k < g$ gelten. Wir müssen also eventuell *Überträge* berücksichtigen, welche genau wie im Dezimalsystem behandelt werden. Auch die Subtraktion, Multiplikation und Division mit Rest erfolgt genau wie im Dezimalsystem. Es ist eine gute Übung, den allgemeinen Fall einmal zu betrachten.

5.1.7 Induktionsbeweise

In diesem Abschnitt werden einige schon erwähnte Sätze bewiesen, um das Beweisprinzip der Induktion weiter zu illustrieren.

Satz 103: *Sei M eine total geordnete Menge. Dann hat jede endliche Teilmenge $N \neq \emptyset$ ein Maximum und ein Minimum.*

BEWEIS: Es bezeichne n die Anzahl der Elemente von N. Für $n = 1$ ist nichts zu zeigen. Sind $x, y \in N$, so ist $x \leq y$ oder $y \leq x$, und das Minimum und Maximum kann man sofort ablesen. Die Behauptung gelte nun für $n > 2$, und N habe $n + 1$ Elemente. Dann gilt für $x \in N$ die Beziehung $\max N = \max(\max N \setminus \{x\}, x)$ nach Induktionsvoraussetzung und analog für $\min$. □

Satz 104: *Sei M eine endliche Menge mit $|M| = n$. Dann gilt $|\mathcal{P}(M)| = 2^n$.*

BEWEIS: Induktionsanfang: Im Fall $n = 0$ kommt nur $M = \emptyset$ in Frage, und es ist

$$|\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0.$$

Induktionsvoraussetzung: Für eine Menge M mit n Elementen gelte $|\mathcal{P}(M)| = 2^n$.
Induktionsschluss: Sei nun M eine Menge mit $n+1$ Elementen und $x \in M$. Dann hat $M \setminus \{x\}$ gerade n Elemente und nach Induktionsvoraussetzung ist $|\mathcal{P}(M \setminus \{x\})| = 2^n$. Man erhält nun $\mathcal{P}(M)$, indem man für jedes Element $y \in \mathcal{P}(M \setminus \{x\})$ die Menge $z = y \cup \{x\}$ bildet und die Mengen $\{y, z\}$ vereinigt. Offenbar hat sich damit die Anzahl der Elemente verdoppelt, d. h. es gilt $|\mathcal{P}(M)| = 2 \cdot |\mathcal{P}(M \setminus \{x\})| = 2 \cdot 2^n = 2^{n+1}$. □

Satz 105 (Allgemeines Assoziativgesetz): *In einer Halbgruppe ist die Verknüpfung von Elementen unabhängig von der Klammersetzung.*

BEWEIS: Für $n = 0, 1, 2, 3$ ist nichts zu zeigen. Sei also $n > 3$ und die Aussage gelte für n. Die inneren Klammern des Produkts $x := (x_1 \cdots x_k)(x_{k+1} \cdots x_{n+1})$ seien beliebig. Nach Induktionsvoraussetzung ist der Wert der beiden Klammern unabhängig von den inneren Klammern und daher

$$x = \left(\prod_{i=1}^{k} x_i\right)\left(\prod_{i=1}^{n-k+1} x_{k+i}\right).$$

Wir unterscheiden nun zwei Fälle. Falls $k = n$ steht rechts nur der Faktor x_{n+1}, und wir können direkt das Assoziativgesetz anwenden zu

$$x = \prod_{i=1}^{n+1} x_i.$$

Falls $k < n$ schreiben wir

$$x = \left(\prod_{i=1}^{k} x_i\right)\left(\left(\prod_{i=1}^{n-k} x_{k+i}\right) x_{n+1}\right),$$

was nach Anwendung des Assoziativgesetzes zu

$$x = \left(\left(\prod_{i=1}^{k} x_i \right) \left(\prod_{i=1}^{n-k} x_{k+i} \right) \right) x_{n+1}$$

wird. Nun stehen in der Klammer aber nur noch n Faktoren, und nach Induktionsvoraussetzung erhält man

$$x = \left(\prod_{i=1}^{n} x_i \right) x_{n+1} = \prod_{i=1}^{n+1} x_i.$$

□

Satz 106 (Potenzgesetze): *In einer Halbgruppe M gelten für alle $m, n \in \mathbb{N}^*$ und $x \in M$ die* Potenzgesetze

(i) $x^m x^n = x^{m+n}$

(ii) $(x^m)^n = x^{mn}$.

In einem Monoid gelten sie auch für $m, n = 0$. In einer Gruppe gelten sie für alle $m, n \in \mathbb{Z}$.

BEWEIS: Wir beweisen sie nur für eine Halbgruppe, da die anderen Fälle analog sind. Die Potenzen sind im Falle einer Halbgruppe definiert durch $x^1 := x$ und $x^{n+1} := x^n \cdot x$.

(i) Wir beweisen die Regel durch Induktion über n. Sei also m beliebig. Der Fall $n = 1$ ergibt sich direkt aus der Definition $x^m x^1 = x^m x = x^{m+1}$. Es gelte nun die Aussage für ein n. Dann rechnet man

$$x^m x^{n+1} = x^m x^n x = x^{m+n} x = x^{m+n+1}.$$

(ii) Wir führen wieder Induktion über n mit m beliebig. Der Induktionsanfang $n = 1$ ist klar. Die Aussage gelte nun für ein n. Dann erhält man

$$(x^m)^{n+1} = (x^m)^n (x^m) = x^{mn} x^m = x^{mn+m} = x^{m(n+1)}.$$ □

Satz 107 (Eindeutigkeit der Primfaktorzerlegung): *In einem faktoriellen Ring ist die Zerlegung in Primfaktoren eindeutig bis auf Assoziiertheit, d. h. ist $a = p_1 \cdots p_n = \widetilde{p_1} \cdots \widetilde{p_m}$ mit $p_i, \widetilde{p_i}$ prim, so ist $n = m$ und $p_i \sim \widetilde{p_i}$ nach einer geeigneten Umordnung der Faktoren.*

BEWEIS: Wir führen Induktion über n. Der Fall $n = 1$ führt auf $p_1 = \widetilde{p_1} \cdots \widetilde{p_m}$. Angenommen $m > 1$. Da p_1 prim ist, ist p_1 nach Satz 58 auch irreduzibel. Dann muss $\widetilde{p_2} \cdots \widetilde{p_m} = e$ mit e eine Einheit sein, denn $\widetilde{p_1}$ kann keine Einheit sein, da $\widetilde{p_1}$ prim ist. Umformen ergibt $\widetilde{p_2}(\widetilde{p_3} \cdots \widetilde{p_m} e^{-1}) = 1$. Damit ist aber $\widetilde{p_2}$ invertierbar, also eine Einheit — Widerspruch!

Sei nun $n > 1$. Aus

$$p_1 \cdots p_{n+1} = \widetilde{p_1} \cdots \widetilde{p_m} \tag{5.1}$$

folgt $\widetilde{p_1}|p_1 \cdots p_{n+1}$. Da $\widetilde{p_1}$ prim ist muss also $\widetilde{p_1}|p_i$ für irgendein i gelten. Es gelte o. E. $\widetilde{p_1}|p_1$. Daraus folgt $\widetilde{p_1}e = p_i$ mit e Einheit, da p_1 prim ist. Also ist $\widetilde{p_1} \sim p_i$. Einsetzen in Gleichung (5.1) und Umformen ergibt

$$\widetilde{p_1}(ep_2 \cdots p_{n+1} - \widetilde{p_2} \cdots \widetilde{p_m}) = 0.$$

Wegen $\widetilde{p_1} \neq 0$ muss damit $ep_2 \cdots p_{n+1} - \widetilde{p_2} \cdots \widetilde{p_m} = 0$ oder $p_2 \cdots p_{n+1} = \widetilde{p_2} \cdots \widetilde{p_m}e^{-1}$ sein. Nun stehen links aber nur noch n Primfaktoren, also ist nach Induktionsvoraussetzung die Anzahl der Primfaktoren gleich und nach geeigneter Umordnung $p_i \sim \widetilde{p_i}$. □

5.2 Ganze Zahlen

Die Konstruktion der natürlichen Zahlen war recht aufwändig, da wir sie mengentheoretisch durchführen mussten. Die Konstruktion der ganzen Zahlen ist dagegen viel einfacher, weil wir uns auf die schon bekannte Algebra zurückziehen können.

Definition 58 (Menge der ganzen Zahlen): *Die Grothendieck-Gruppe $\mathbb{Z}$ von $(\mathbb{N}, +)$ heißt* Menge der ganzen Zahlen.

Da in $\mathbb{N}$ bzgl. $+$ die Kürzungsregel gilt, ist die in Satz 42 benutzte Abbildung f injektiv, wir können also $\mathbb{N}$ in $\mathbb{Z}$ einbetten. Weiter bemerken wir, dass sich die Äquivalenzrelation nun reduziert zu

$$(n_1, m_1)R(n_2, m_2) \Leftrightarrow n_1 + m_2 = n_2 + m_1.$$

Daher sind die natürlichen Zahlen gerade die ganzen Zahlen der Form $[n + n, n] = [n, 0]$. Wir wissen schon, dass $(\mathbb{Z}, +)$ eine abelsche Gruppe mit neutralem Element $[0, 0]$ und dem zu $[n, m]$ inversen Element $[m, n]$ ist. Im Rest dieses Abschnitts wird es darum gehen, $\mathbb{Z}$ zu einem total geordneten Integritätsring zu machen.

Satz 108: *Die Menge ganzen Zahlen $\mathbb{Z}$ wird durch die Multiplikation*

$$[n_1, m_1] \cdot [n_2, m_2] := [n_1n_2 + m_1m_2, n_1m_2 + n_2m_1]$$

zu einem Integritätsring.

BEWEIS: Wie immer ist zuerst die Wohldefiniertheit zu zeigen. Sei dazu $[n_1, m_1] = [\widetilde{n_1}, \widetilde{m_1}]$. Dann ist

$$\begin{aligned} n_1n_2 + m_1m_2 + \widetilde{n_1}m_2 + n_2\widetilde{m_1} &= (n_1 + \widetilde{m_1})n_2 + (m_1 + \widetilde{n_1})m_2 \\ &= (\widetilde{n_1} + m_1)n_2 + (\widetilde{m_1} + n_1)m_2 \\ &= \widetilde{n_1}n_2 + \widetilde{m_1}m_2 + n_1m_2 + n_2m_1. \end{aligned}$$

Damit ist gezeigt, dass das Produkt von der Wahl des ersten Repräsentanten unabhängig ist. Analog zeigt man, dass es auch nicht von der Wahl des zweiten Repräsentanten abhängt. Also ist es insgesamt unabhängig von der Wahl von Repräsentanten.

Die Kommutativität erhält man aus der Kommutativität der Multiplikation in $\mathbb{N}$. Das neutrale Element ist die Klasse $[1,0]$. Die Assoziativität und Distributivität nachzurechnen, wird dem Leser als Übung empfohlen.

Sei nun $[n_1,m_1]\cdot[n_2,m_2]=[0,0]$, d. h.

$$n_1n_2+m_1m_2=n_1m_2+n_2m_1.$$

Wir nehmen nun an $[n_1,m_1]\neq[0,0]$, also $n_1\neq m_1$. Wir können o. E. $n_1>m_1$ annehmen. Dann folgt

$$(n_1-m_1)n_2=m_2(n_1-m_1).$$

Da in $(\mathbb{N},\cdot)$ jedes von 0 verschiedene Element kürzbar ist, gilt $n_2=m_2$, d. h. $[n_2,m_2]=[0,0]$. Damit ist $\mathbb{Z}$ nullteilerfrei. □

Es ist wichtig zu bemerken, dass die Multiplikation für natürliche Zahlen in $\mathbb{Z}$ dasselbe Ergebnis liefert wie in $\mathbb{N}$. Die Einbettung der natürlichen in die ganzen Zahlen ist also auch mit der Multiplikation verträglich.

Da $[0,m]=-[m,0]$ gilt, kann man jede ganze Zahl in der Form $[n,m]=[n,0]-[m,0]$ schreiben. Die Klassen $[n,0]$ und $[m,0]$ können wir aber mit den natürlichen Zahlen n und m identifizieren, weshalb wir $[n,m]=n-m$ erhalten. Wir können also jede ganze Zahl formal als Differenz zweier natürlicher Zahlen schreiben.

Nun können wir von der Klassenschreibweise abstrahieren, indem wir die Fälle $n\geq m$ und $n<m$ unterscheiden. Wir vereinbaren die Konvention

$$[n,m]=\begin{cases}n-m & \text{falls } n\geq m\\ -(m-n) & \text{falls } n<m.\end{cases}$$

Somit lässt sich jede ganze Zahl in eindeutiger Weise als vorzeichenbehaftete natürliche Zahl a schreiben.

Satz 109: *Durch $a\leq b:\Leftrightarrow b-a\in\mathbb{N}$ wird $\mathbb{Z}$ zu einem total geordneten Ring.*

BEWEIS: Dass $\leq$ eine Ordnungsrelation ist, sieht man leicht. Auch klar ist, dass immer $a-b$ oder $b-a$ eine natürliche Zahl sein muss. Es bleibt also nur noch, die Verträglichkeit mit der Ringstruktur zu zeigen. Sei dazu $a\leq b$ und $c\in\mathbb{Z}$. Dann ist offenbar $b+c-(a+c)=b-a\in\mathbb{N}$, also $a+c\leq b+c$. Sei weiter $a\leq b$ und $c\geq 0$, also $b-a\in\mathbb{N}$ und $c\in\mathbb{N}$. Dann ist natürlich auch $bc-ac=(b-a)c\in\mathbb{N}$, d. h. $ac\leq bc$. □

Die Ordnung auf $\mathbb{Z}$ ist mit der Ordnung auf $\mathbb{N}$ verträglich. Ein ganze Zahl $a\in\mathbb{Z}$ heißt

(i) *positiv*, wenn $a\in\mathbb{N}^*$

(ii) *nichtnegativ*, wenn $a\in\mathbb{N}$

(iii) *nichtpositiv*, wenn $-a\in\mathbb{N}$

(iv) *negativ*, wenn $-a\in\mathbb{N}^*$.

In Abschnitt 4.4 wurde darauf hingewiesen, dass man abelsche Gruppen auf genau eine Weise zu einem $\mathbb{Z}$-Modul machen kann. Eine analoge Überlegung führt auf den folgenden

Satz 110: *Sei R ein Ring. Dann gibt es genau einen unitären Homomorphismus $f\colon \mathbb{Z} \to R$, und dieser ist durch $f(n) = \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n \cdot 1$ gegeben.*

BEWEIS: Für einen unitären Homomorphismus muss $f(0) = 0$ und $f(1) = 1$ gelten. Dann folgt induktiv $f(n+1) = f(n) + f(1) = n \cdot 1 + 1 = (n+1) \cdot 1$ für $n \geq 1$. Weiter ist $f(-n) = -f(n) = -n \cdot 1$, und damit ist die Formel für alle $n \in \mathbb{Z}$ gezeigt. Dass dies tatsächlich ein Homomorphismus ist, rechnet man leicht nach. □

Wir sehen also, dass die ganz zu Beginn der Algebra eingeführte Notation mit der Theorie konsistent ist.

Definition 59: *Eine geordnete Gruppe heißt* archimedisch geordnet*, wenn es für alle $g, h \in G$ mit $g, h > 0$ ein $n \in \mathbb{N}$ gibt mit $nh > g$.*

Satz 111: *Die ganzen Zahlen $\mathbb{Z}$ sind archimedisch geordnet.*

BEWEIS: Wir müssen zeigen, dass für alle $a, b \in \mathbb{N}^*$ ein $n \in \mathbb{N}$ existiert mit $nb > a$. Wir führen Induktion über a. Sei also $b > 0$ beliebig gegeben. Für $a = 1$ ist sicher $2b > a$. Die Behauptung gelte nun für ein $a \in \mathbb{N}^*$, d. h. es gebe ein $n \in \mathbb{N}$ mit $nb > a$. Dann ist $(n+1)b = nb + b > a + b \geq a + 1$. Damit folgt die Behauptung. □

5.3 Rationale Zahlen

Auch die Konstruktion der rationalen Zahlen ist sehr einfach.

Definition 60 (Menge der rationalen Zahlen): *Der Quotientenkörper $\mathbb{Q}$ der ganzen Zahlen $\mathbb{Z}$ heißt* Menge der rationalen Zahlen.

Schreiben wir eine rationale Zahl $r = a/b$ als Quotient mit $a, b \in \mathbb{Z}$ und $b \neq 0$, so heißt r

(i) *positiv*, wenn a, b positiv oder a, b negativ

(ii) *nichtnegativ*, wenn r positiv oder $a = 0$

(iii) *nichtpositiv*, wenn r negativ oder $a = 0$

(iv) *negativ*, wenn a positiv (negativ) und b negativ (positiv).

Es bezeichne $\mathbb{Q}_+$ die Menge der nichtnegativen rationalen Zahlen.

Satz 112: *Durch $r \leq s :\Leftrightarrow s - r \in \mathbb{Q}_+$ wird $\mathbb{Q}$ zu einem total geordneten Körper.*

BEWEIS: Völlig analog zu Satz 109. □

Natürlich ist auch hier für ganze Zahlen die Ordnung auf $\mathbb{Q}$ mit der Ordnung auf $\mathbb{Z}$ identisch. Damit sind die ganzen Zahlen sowohl bzgl. der Ordnungsstruktur als auch bzgl. der algebraischen Struktur in den rationalen Zahlen eingebettet.

Satz 113: *Die Ordnung von $\mathbb{Q}$ ist archimedisch.*

BEWEIS: Seien $r, s > 0$ gegeben. Dann sind r, s von der Form $r = a/b$ und $s = c/d$ mit $a, b, c, d \in \mathbb{N}^*$. Wegen $r = ad/bd$ und $s = bc/bd$ ist zu zeigen, dass es ein $n \in \mathbb{N}$ gibt mit $nbc > ad$. Da aber ad, bc positive ganze Zahlen sind, folgt die Behauptung aus Satz 111. □

Es gibt einen wichtigen Unterschied zwischen der Ordnung auf $\mathbb{Z}$ und der Ordnung auf $\mathbb{Q}$.

Definition 61: *Eine Ordnung $\leq$ auf einer Menge M heißt* dicht, *wenn es für alle $x, y \in M$ mit $x < y$ ein $z \in M$ gibt mit $x < z < y$.*

Satz 114: *Die rationalen Zahlen $\mathbb{Q}$ sind dicht.*

BEWEIS: Seien $r, s \in \mathbb{Q}$ mit $r < s$. Für $t := (r + s)/2$ gilt

$$s = \frac{s+s}{2} > \frac{r+s}{2} = t > \frac{r+r}{2} = r.$$

□

Die rationalen Zahlen lassen sich auch abstrakt charakterisieren. Wir zeigen, dass $\mathbb{Q}$ der „kleinste“ total geordnete Körper ist.

Sei dazu K ein total geordneter Körper. Dann ist natürlich auch jeder Unterkörper von K total geordnet. Das gilt insbesondere für seinen Primkörper. Nach Satz 81 ist dieser isomorph zu $\mathbb{Q}$ oder $\mathbb{Z}/p\mathbb{Z}$. Da aber Aufgabe 27 e) zeigt, dass ein total geordneter Körper unendlich viele Elemente hat, bleibt nur $\mathbb{Q}$ übrig. Diese Überlegung zeigt auch, dass total geordnete Körper Charakteristik 0 haben müssen.

Die im Beweis von Satz 81 benutzte Abbildung $\overline{f}\colon \mathbb{Q} \to K$ respektiert übrigens auch die Ordnung. Ist nämlich $r \leq s$, so gilt $r + t = s$ mit $t \geq 0$. Weiter ist $\overline{f}(s) = \overline{f}(r + t) = \overline{f}(r) + \overline{f}(t)$. Da in total geordneten Körpern stets $0 < 1$ gilt und sie Charakteristik 0 haben, gilt nach Satz 44.(v) auch $0 < \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n \cdot 1$ sowie $0 < n/m \cdot 1$ für $n, m \in \mathbb{N}^*$. Ist $t = n/m$, so ist $\overline{f}(t) = n/m \cdot 1 \geq 0$ und daher $\overline{f}(s) \geq \overline{f}(r)$.

Satz 115 (Monomorphiesatz): *Sei K ein total geordneter Körper. Dann gibt es einen Körpermonomorphismus $f\colon \mathbb{Q} \to K$. Zusätzlich ist der Körper der rationalen Zahlen $\mathbb{Q}$ bis auf Isomorphie der einzige total geordnete Körper mit dieser Eigenschaft, und die Abbildung f ist ordnungstreu und eindeutig bestimmt.*

5.4 Reelle Zahlen

5.4.1 Fundamentalfolgen

Es gibt mehrere Möglichkeiten, die reellen aus den rationalen Zahlen zu konstruieren. Wir wählen hier einen Weg, der sowie algebraische als auch analytische Ideen benutzt. Die verwendete Analysis kann man problemlos direkt für metrische Räume formulieren. Es empfiehlt sich daher aus ökonomischen Gründen nicht, hier die Theorie der Grenzwertsätze voll auszubreiten, sondern wir entwickeln sie nur soweit, wie es die Konstruktion der reellen Zahlen unbedingt erfordert.

Unter einer *rationalen Folge* verstehen wir eine Folge $(r_k)_{k\in\mathbb{N}}$ mit $r_k \in \mathbb{Q}$ für alle $k \in \mathbb{N}$. Wir erinnern daran, dass Addition und Multiplikation von Abbilundgen, und insbesondere also von Folgen, punktweise definiert sind, d. h. man setzt $(a_k)_{k\in\mathbb{N}} + (b_k)_{k\in\mathbb{N}} := (a_k + b_k)_{k\in\mathbb{N}}$ und $(a_k)_{k\in\mathbb{N}} \cdot (b_k)_{k\in\mathbb{N}} := (a_k \cdot b_k)_{k\in\mathbb{N}}$. Offensichtlich sind die rationalen Folgen bzgl. Addition und Multiplikation abgeschlossen.

Satz 116: *Die rationalen Folgen bilden einen Ring.*

Für uns sind nicht alle rationalen Folgen interessant. Wir interessieren uns nur für den Unterring der rationalen Folgen, die „fast konvergent“ sind. Um Distanzen rationaler Zahlen messen zu können, führen wir den *Betrag*

$$|r| := \max(r, -r) = \begin{cases} r & \text{falls } r \geq 0 \\ -r & \text{falls } r < 0 \end{cases}$$

ein. Offenbar ist $|r| = |-r|$ und $|r| = 0$ genau dann, wenn $r = 0$ ist. Außerdem erfüllt der Betrag $|rs| = |r||s|$. Weniger offensichtlich ist die *Dreiecksungleichung* $|r + s| \leq |r| + |s|$ und die *umgekehrte Dreiecksungleichung* $|r - s| \geq |r| - |s|$. Ihr Beweis bleibt dem Leser als Übung überlassen. Wir bemerken noch $\pm r \leq |r|$ und $|r - s| \leq t \Leftrightarrow t - s \leq r \leq s + t$.

Definition 62: *Eine rationale Folge $(r_k)_{k\in\mathbb{N}}$ heißt* Fundamentalfolge*, wenn es für alle rationalen $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt mit $|r_k - r_l| \leq \varepsilon$ für alle $k, l \geq N$.*

Eine rationale Folge $(r_k)_{k\in\mathbb{N}}$ heißt rational konvergent *gegen ein $r \in \mathbb{Q}$, wenn es für alle rationalen $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt mit $|r_k - r| \leq \varepsilon$ für alle $k \geq N$.*

Klarerweise ist die konstante Folge $(r)_{k\in\mathbb{N}}$ konvergent gegen r. Das wichtigste Beispiel ist aber die Folge $(1/k)_{k\in\mathbb{N}^*}$, die gegen 0 konvergiert. Sei nämlich $\varepsilon > 0$ gegegen. Dann ist für jedes $N \geq 1/\varepsilon$ und alle $k \geq N$ die Ungleichung $|1/k - 0| = |1/k| \leq 1/N \leq \varepsilon$ erfüllt.

Satz 117: *Ist eine rationale Folge $(r_k)_{k\in\mathbb{N}}$ rational konvergent gegen $r \in \mathbb{Q}$ und $\widetilde{r} \in \mathbb{Q}$, so ist $r = \widetilde{r}$.*

BEWEIS: Angenommen $r \neq \widetilde{r}$. Dann betrachte $\varepsilon := |r - \widetilde{r}|/2$. Es gibt $N_r, N_{\widetilde{r}} \in \mathbb{N}$ mit $|r_k - r| \leq \varepsilon/2$ für alle $k \geq N_r$ und $|r_k - \widetilde{r}| \leq \varepsilon/2$ für alle $k \geq N_{\widetilde{r}}$. Damit folgt für alle $k \geq \max(N_r, N_{\widetilde{r}})$

$$2\varepsilon = |r - \widetilde{r}| = |r - r_k + r_k - \widetilde{r}| \leq |r - r_k| + |r_k - \widetilde{r}| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

ein Widerspruch. □

Der *Grenzwert* oder *Limes* der Folge $(r_k)_{k\in\mathbb{N}}$ ist also, wenn er existiert, eindeutig bestimmt und wird mit $\lim_{k\to\infty} r_k$ oder kurz $\lim_k r_k$ bezeichnet. Wir haben hier das erste Mal den Fundamentaltrick der Analysis, die Nulladdition, benutzt.

Satz 118: *Jede rational konvergente Folge ist eine Fundamentalfolge.*

BEWEIS: Sei $\varepsilon > 0$ gegeben. Für $r := \lim_k r_k$ gibt es ein $N \in \mathbb{N}$, so dass für alle $k \geq N$ gilt $|r_k - r| \leq \varepsilon/2$. Damit folgt für alle $k, l \geq N$

$$|r_k - r_l| = |r_k - r + r - r_l| \leq |r_k - r| + |r - r_l| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \qquad \square$$

Die Umkehrung dieses Satzes gilt nicht, d. h. es gibt Fundamentalfolgen, die nicht rational konvergent sind. Das ist der Grund, weshalb wir die rationalen Zahlen noch erweitern müssen, um Analysis treiben zu können.

Satz 119: *Die Fundamentalfolgen bilden einen Ring.*

BEWEIS: Seien zwei Fundamentalfolgen $(r_k), (s_k)$ und $\varepsilon > 0$ gegeben. Es gibt ein $N \in \mathbb{N}$, so dass $|r_k - r_l| \leq \varepsilon/2$ und $|s_k - s_l| \leq \varepsilon/2$ für alle $k, l \geq N$. Dann gilt

$$|r_k + s_k - r_l - s_l| \leq |r_k - r_l| + |s_k - s_l| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Für $\varepsilon = 1$ gibt es ein N mit $|r_k| - |r_l| \leq |r_k - r_l| \leq 1$ für alle $k, l \geq N$ und folglich $|r_k| \leq 1 + |r_N|$ für alle $k \geq N$. Daher ist $|r_k|$ kleiner als

$$M_r := \max(|r_0|, |r_1|, \ldots, |r_{N-1}|, 1 + |r_N|).$$

Analog ist $|s_k| \leq M_s$ für ein $M_s \geq 1$.

Sei nun wieder $\varepsilon > 0$ beliebig. Nach Obigem existiert ein $N \in \mathbb{N}$ und ein $M \geq 1$, so dass $|r_k - r_l| \leq \varepsilon/2M$ und $|s_k - s_l| \leq \varepsilon/2M$ sowie $|r_k|, |s_k| \leq M$ für alle $k, l \geq N$. Dann folgt

$$\begin{aligned} |r_k s_k - r_l s_l| &= |r_k(s_k - s_l) + (r_k - r_l)s_l| \leq |r_k||s_k - s_l| + |r_k - r_l||s_l| \\ &\leq M\frac{\varepsilon}{2M} + \frac{\varepsilon}{2M}M \leq \varepsilon. \end{aligned}$$

Damit sind Summe und Produkt von Fundamentalfolgen wieder Fundamentalfolgen. Zuletzt bemerkt man noch, dass die neutralen Elemente rational konvergent und daher nach Satz 118 Fundamentalfolgen sind. Die weiteren Eigenschaften sind klar. $\square$

Der Fundamentalfolgenring wird nun mit R bezeichnet. Von besonderer Bedeutung sind die rational konvergenten Folgen, die gegen 0 konvergieren, die sog. *Nullfolgen*.

Satz 120: *Die Nullfolgen bilden ein Ideal I in R.*

BEWEIS: Wegen Satz 118 sind die Nullfolgen sicher in R enthalten. Seien (r_k) und (s_k) zwei Nullfolgen, d. h. zu $\varepsilon > 0$ gibt es ein $N \in \mathbb{N}$, so dass für alle $k \geq N$ gilt $|r_k| \leq \varepsilon/2$ und $|s_k| \leq \varepsilon/2$. Dann ist $|r_k + s_k| \leq |r_k| + |s_k| \leq \varepsilon$. Sei nun (r_k) eine Nullfolge und (s_k) eine beliebige Fundamentalfolge. Nach obigem Beweis gibt es ein $M \geq 1$ mit $|s_k| \leq M$ für alle $k \in \mathbb{N}$. Zu $\varepsilon > 0$ existiert ein $N \in \mathbb{N}$, so dass $|r_k| \leq \varepsilon/M$ für alle $k \geq N$. Damit folgt $|r_k s_k| \leq M|r_k| \leq \varepsilon$. $\square$

Nun liegt es nahe, die Restklassen $(r_k) + I$ zu betrachten. Sie enthalten alle Fundamentalfolgen, die sich nur um eine Nullfolge unterscheiden.

Satz 121: *Der Restklassenring R/I ist ein Körper.*

BEWEIS: Wir müssen nur die Existenz von multiplikativ inversen Elementen zeigen. Sei dazu $(r_k) + I \in R/I$. Ist dieses Element von 0 verschieden, so können nur endlich viele $r_k = 0$ sein. Für diese k setzen wir $r_k = 1$, denn dadurch ändert sich die Restklasse nicht, da wir eine Nullfolge addieren. Nun ist die Restklasse $(1/r_k) + I$ zu $(r_k) + I$ invers. Wir müssen nur noch zeigen, dass $(1/r_k)$ auch eine Fundamentalfolge ist.

Da $|r_k| > 0$ für alle k gibt es ein $s > 0$ mit $|r_k| \geq s$ für alle k (Aufgabe 36). Zu $\varepsilon > 0$ gibt es ein $N \in \mathbb{N}$, so dass $|r_k - r_l| \leq s^2\varepsilon$ für alle $k, l \geq N$. Dann gilt

$$\left|\frac{1}{r_k} - \frac{1}{r_l}\right| = \frac{|r_l - r_k|}{|r_k r_l|} \leq \frac{s^2\varepsilon}{s^2} = \varepsilon. \qquad \square$$

Definition 63 (Menge der reellen Zahlen): *Der Körper $\mathbb{R} := R/I$ heißt* Menge der reellen Zahlen.

Der Vorteil dieser Konstruktion ist, dass man sämtliche Rechenregeln auf $\mathbb{R}$ sofort gegeben hat. Der Nachteil ist, dass man die analytischen Eigenschaften von $\mathbb{R}$ erst nachrechnen muss. Dazu müssen wir $\mathbb{R}$ anordnen.

5.4.2 Die Ordnung auf $\mathbb{R}$

Uns bleibt natürlich nichts anderes übrig, als die Ordnung auf $\mathbb{R}$ auf die Ordnung von $\mathbb{Q}$ zurückzuführen. Diese müssen wir jedoch zunächst auf den Fundamentalfolgenring R übertragen.

Wir nennen eine Fundamentalfolge $(r_k) \in R$ positiv (bzw. negativ), wenn es ein $0 < s \in \mathbb{Q}$ und ein $N \in \mathbb{N}$ gibt mit $r_k \geq s$ (bzw. $-r_k \geq s$) für alle $k \geq N$. Wir schreiben dann $(r_k) > 0$ (bzw. $(r_k) < 0$).

Die Positivität (bzw. Negativität) bleibt bei Addition einer Nullfolge erhalten. Denn sei $(r_k) > 0$ und $(\widetilde{r_k})$ die Summe von (r_k) und einer Nullfolge (s_k). Dann ist $\lim_k(\widetilde{r_k} - r_k) = \lim_k s_k = 0$. Da (r_k) positiv ist, gibt es ein $s > 0$ und ein $N_r \in \mathbb{N}$ mit $r_k \geq 2s$ für alle $k \geq N_r$. Weiter gibt es zu $\varepsilon := s$ ein $N_{\widetilde{r}} \in \mathbb{N}$ mit $|r_k - \widetilde{r_k}| \leq s$ für alle $k \geq N_{\widetilde{r}}$. Also gilt für alle $k \geq \max(N_r, N_{\widetilde{r}})$

$$\widetilde{r_k} = r_k - (r_k - \widetilde{r_k}) \geq r_k - |r_k - \widetilde{r_k}| \geq 2s - s = s.$$

Wir nennen nun eine Restklasse positiv (negativ), wenn ein Repräsentant positiv (negativ) ist. Der folgende Satz zeigt, dass diese Ordnung auf $\mathbb{R}$ total ist.

Satz 122: *Eine Fundamentalfolge ist entweder positiv, negativ oder eine Nullfolge.*

BEWEIS: Es ist klar, dass nicht zwei der Eigenschaften gleichzeitig erfüllt sein können. Es reicht daher zu zeigen, dass eine Fundamentalfolge (r_k), die weder positiv noch negativ ist, eine Nullfolge sein muss.

Da (r_k) eine Fundamentalfolge ist, gibt es zu $\varepsilon > 0$ ein $N \in \mathbb{N}$, so dass $|r_k - r_l| \leq \varepsilon/2$ für alle $k, l \geq N$. Weil weiter (r_k) weder positiv noch negativ ist, existieren $N_p, N_n \geq N$ mit $r_{N_p} < \varepsilon/2$ und $-r_{N_n} < \varepsilon/2$. Also ist für $k \geq N_p$

$$r_k = r_{N_p} + (r_k - r_{N_p}) \leq r_{N_p} + |r_{N_p} - r_k| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

und für $k \geq N_n$

$$r_k = r_{N_n} - (r_{N_n} - r_k) \geq r_{N_n} - |r_{N_n} - r_k| \geq -\frac{\varepsilon}{2} - \frac{\varepsilon}{2} = -\varepsilon.$$

Insgesamt gilt für alle $k \geq \max(N_n, N_p)$ die Ungleichung $|r_k| \leq \varepsilon$. □

Seien nun $x, y \in \mathbb{R}$. Dann setzen wir $x \leq y$ genau dann, wenn für die Repräsentanten (r_k) von x und (s_k) von y gilt $(s_k - r_k) > 0$ oder $(s_k - r_k) + I = I$. Insbesondere ist eine reelle Zahl positiv, wenn ihre Repräsentanten positiv sind, sie ist 0, wenn ihre Repräsentanten Nullfolgen sind usw. Da wir die rationalen Zahlen durch die konstanten Folgen in $\mathbb{R}$ einbetten können, ist diese Ordnung mit der Ordnung auf $\mathbb{Q}$ verträglich. Man definiert den Betrag in $\mathbb{R}$ genau wie in $\mathbb{Q}$, und er hat auch dieselben Eigenschaften.

Satz 123: *$\mathbb{R}$ ist ein total geordneter Körper.*

BEWEIS: Der Beweis ist eine gute Übungsaufgabe. □

Die Definition der Ordnung zeigt, dass es für jedes reelle $x > 0$ ein rationales r gibt mit $0 < r < x$.

Satz 124 (Satz von Archimedes): *Die Ordnung auf $\mathbb{R}$ ist archimedisch.*

BEWEIS: Seien $x, y \in \mathbb{R}$ mit $x, y > 0$ gegeben. Betrachte die positive reelle Zahl y/x. Dann gibt es eine rationale Zahl m/n mit $m, n \in \mathbb{N}^*$ und $0 < m/n < y/x$. Daraus folgt $x/y < n/m < n + 1$, also $x < (n + 1)y$. □

Manchmal ist es nützlich, reelle Zahlen durch ganze Zahlen zu approximieren.

Satz 125: *Für jedes $x \in \mathbb{R}$ existiert genau ein $a \in \mathbb{Z}$ mit $a \leq x < a + 1$.*

BEWEIS: Für $x = 0$ kommt nur $a = 0$ in Frage. Für $x > 0$ betrachte man die Menge $M := \{\, n \in \mathbb{N} \mid n > x \,\}$. Nach Satz 124 existiert für $y := 1$ ein $n \in \mathbb{N}$ mit $n > x$. Daher ist M nicht leer. Somit besitzt nach Satz 90 $M \subseteq \mathbb{N}$ ein (eindeutig bestimmtes) minimales Element n. Nun setze $a := n - 1$. Dann gilt $a + 1 > x$. Angenommen, es wäre nicht $a \leq x$, d. h. $a > x$. Im Fall $n > 0$ wäre $a \in M$, was der Minimalität von n widerspräche, und falls $n = 0$, also $-1 > x$, hätten wir einen Widerspruch zu $x > 0$.

Für $x < 0$ erhält man ein $\widetilde{a}$ mit $\widetilde{a} \leq -x < \widetilde{a} + 1$. Dann ist $a := -\widetilde{a} - 1$ die gesuchte Zahl. □

Man schreibt $[x] := a$ und nennt $[x]$ die *Gauß-Klammer* von x. Die Abbildung

$$[\cdot]\colon \mathbb{R} \longrightarrow \mathbb{Z}\colon x \longmapsto [x]$$

ordnet jeder reellen Zahl die nächstkleinere ganze Zahl zu, d. h.

$$[x] = \max\{\, a \in \mathbb{Z} \mid a \leq x \,\}.$$

Manchmal unterscheidet man auch zwischen unterer und oberer Gauß-Klammer. Dann setzt man $\lfloor x \rfloor := [x]$ und $\lceil x \rceil := [x]+1$. Nun ist $\lceil x \rceil$ die nächstgrößere ganze Zahl. Es gilt ebenfalls $\lceil x \rceil = -\lfloor -x \rfloor$ und

$$\lceil x \rceil = \min\{\, a \in \mathbb{Z} \mid a \geq x \,\}.$$

Für alle $x \in \mathbb{R}$ gilt also $\lfloor x \rfloor \leq x \leq \lceil x \rceil$.

Man kann völlig analog zum Fall der rationalen Zahlen zeigen, dass die Ordnung auf $\mathbb{R}$ dicht ist. Es gilt aber noch mehr:

Satz 126: *Die Menge $\mathbb{Q}$ liegt dicht in $\mathbb{R}$, d. h. für alle $x \in \mathbb{R}$ und $\varepsilon > 0$ existiert ein $r \in \mathbb{Q}$ mit $|x - r| \leq \varepsilon$. Anders formuliert gibt es für alle $x, y \in \mathbb{R}$ mit $x < y$ ein $r \in \mathbb{Q}$ mit $x < r < y$.*

BEWEIS: Sei $(r_k)_{k\in\mathbb{N}}$ ein Repräsentant von x. Dann ist für jedes $l \in \mathbb{N}$ die Fundamentalfolge $(|r_k - r_l|)_{k\in\mathbb{N}}$ ein Repräsentant von $|x - r_l|$. Damit $|x - r_l| \leq \varepsilon$ gilt, muss $(\varepsilon - |r_k - r_l|)_{k\in\mathbb{N}} > 0$ oder $(\varepsilon - |r_k - r_l|)_{k\in\mathbb{N}}$ eine Nullfolge sein. Da $(r_k)_{k\in\mathbb{N}}$ aber eine Fundamentalfolge ist, existiert zu $\varepsilon > 0$ ein $N \in \mathbb{N}$, so dass $|r_k - r_l| \leq \varepsilon$ für alle $k, l \geq N$. Mit $l := N$ ist dann $\varepsilon - |r_k - r_l| \geq 0$ für alle $k \geq N$. Damit ist gezeigt, dass $(\varepsilon - |r_k - r_l|)_{k\in\mathbb{N}}$ nicht negativ sein kann, und mit Satz 122 folgt die Behauptung.

Zum Beweis der zweiten Aussage wähle man ein r mit

$$\left| \frac{x+y}{2} - r \right| \leq \frac{y-x}{4}. \qquad \square$$

Es ist einfach, die Definition der Konvergenz rationaler Folgen auf reelle Folgen zu übertragen, und es ist klar, was eine reelle Fundamentalfolge ist. Ist x eine reelle Zahl und $(r_k)_{k\in\mathbb{N}}$ ein Repräsentant, so zeigt obiger Beweis, dass $\lim_k |x - r_k| = 0$ gilt. Das heißt, dass es für jede reelle Zahl ein Folge rationaler Zahlen gibt, die gegen sie konvergiert. Damit können wir das Hauptergebnis unserer Beschäftigung mit reellen Folgen beweisen.

Satz 127: $\mathbb{R}$ *ist* vollständig*, d. h. jede reelle Fundamentalfolge ist konvergent.*

BEWEIS: Die eine Richtung ist klar. Sei für die andere Richtung (x_k) eine reelle Fundamentalfolge. Sei $\varepsilon > 0$ gegeben und $N \in \mathbb{N}$ mit $|x_k - x_l| \leq \varepsilon/3$ für alle $k, l \geq N$. Nach Satz 126 gibt es zu $3/\varepsilon \leq k \in \mathbb{N}^*$ ein $r_k \in \mathbb{Q}$ mit $|x_k - r_k| \leq 1/k \leq \varepsilon/3$. Dann folgt

$$\begin{aligned} |r_k - r_l| &= |r_k - x_k + x_k - x_l + x_l - r_l| \leq |r_k - x_k| + |x_k - x_l| + |x_l - r_l| \\ &\leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon \end{aligned}$$

für alle $k, l \geq \max(\lceil 3/\varepsilon \rceil, N)$. Damit ist gezeigt, dass $(r_k)_{k\in\mathbb{N}}$ eine Fundamentalfolge ist. Es bezeichne x die zu dieser Folge gehörige reelle Zahl. Für sie gilt

$$|x - x_k| = |x - r_k + r_k - x_k| \leq |x - r_k| + |r_k - x_k| \leq |x - r_k| + \frac{1}{k}.$$

Wegen $\lim_k |x - r_k| = 0$ und $\lim_k 1/k = 0$ hat man also $\lim_k x_k = x$ und damit die Behauptung. □

Wir führen noch eine generelle Notation ein. Sei M eine der Mengen $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$. Dann setzen wir $M^* := M \setminus \{0\}$, $M_+ := \{\, x \in M \mid x \geq 0 \,\}$ und $M_- := \{\, x \in M \mid x \leq 0 \,\}$. Weiter kann man diese Notation kombinieren zu $M_+^* := \{\, x \in M \mid x > 0 \,\}$ und analog $M_-^* := \{\, x \in M \mid x < 0 \,\}$.

5.4.3 Suprema und Infima

Die Menge der natürlichen Zahlen ist bekanntlich wohlgeordnet, d. h. jede nichtleere Teilmenge besitzt ein Minimum. Das wird man von den reellen Zahlen natürlich nicht erwarten können, wie das Gegenbeispiel $\mathbb{R}_+^*$ zeigt. Für jede reelle Zahl $x \in \mathbb{R}_+^*$ existiert ein $y \in \mathbb{R}_+^*$ mit $y < x$. Stattdessen haben die reellen Zahlen eine andere wichtige Eigenschaft, mit der wir uns in diesem Abschnitt beschäftigen werden.

Definition 64: *Es sei M eine geordnete Menge und $(x_k)_{k\in\mathbb{N}}$ eine Folge von Elementen aus M. Dann heißt die Folge* wachsend *(bzw.* fallend*), wenn für alle $k \in \mathbb{N}$ gilt $x_k \leq x_{k+1}$ (bzw. $x_k \geq x_{k+1}$). Sie heißt* streng wachsend *(bzw.* streng fallend*), wenn die Ungleichungen strikt sind.*

Anstatt wachsend und fallend sagt man auch monoton wachsend und monoton fallend. Will man nicht spezifizieren, ob die Folge wachsend oder fallend ist, so nennt man die Folge schlicht *monoton*.

Offenbar ist die Folge (x_k) genau dann (streng) wachsend, wenn die Folge $(-x_k)$ (streng) fallend ist. Der wichtigste Satz über wachsende bzw. fallende Folgen ist der

Satz 128: *Sei (x_k) eine wachsende (bzw. fallende) Folge in $\mathbb{R}$. Die Folge ist genau dann konvergent, wenn sie nach oben (bzw. unten) beschränkt ist.*

BEWEIS: Wir können o. E. annehmen, dass die Folge (x_k) wachsend ist, da wir sonst nur die Folge $(-x_k)$ betrachten müssen. Wir zeigen zunächst, dass die Beschränktheit notwendig ist. Denn ist die Folge (x_k) konvergent gegen x, so gibt es ein $N \in \mathbb{N}$ mit $|x_k - x| \leq 1$ für alle $k \geq N$. Da die Folge wachsend ist, gilt also $x_k \leq x + 1$ für alle $k \in \mathbb{N}$. Damit ist $x + 1$ eine obere Schranke der Folge (x_k).

Zum Beweis der umgekehrten Implikation benutzen wir die Kontraposition, d. h. wir nehmen an, dass die Folge nicht konvergent ist und zeigen dann, dass sie nicht beschränkt sein kann. Nach Satz 127 ist sie nicht konvergent, wenn es ein $\varepsilon > 0$ gibt, so dass es für alle $N \in \mathbb{N}$ Indizes $k, l \geq N$ gibt mit $|x_k - x_l| > \varepsilon$. Es seien k_0, l_0 zwei solcher Indizes mit $k_0 \geq l_0$. Analog gibt es für $N := k_0$ Indizes $k_1 \geq l_1$ mit $|x_{k_1} - x_{l_1}| > \varepsilon$. So konstruieren wir induktiv eine

wachsende Folge von Indizes $l_0, k_0, l_1, k_1, \ldots$ und erhalten damit, da die Folge (x_k) wachsend ist,

$$\begin{aligned} x_{k_n} - x_{l_0} &= x_{k_n} - x_{k_{n-1}} + x_{k_{n-1}} - x_{k_{n-2}} + x_{k_{n-2}} \mp \cdots - x_{k_0} + x_{k_0} - x_{l_0} \\ &\geq x_{k_n} - x_{l_n} + x_{k_{n-1}} - x_{l_{n-1}} + x_{k_{n-2}} \mp \cdots - x_{l_1} + x_{k_0} - x_{l_0} \geq (n+1)\varepsilon. \end{aligned}$$

Nach dem Satz von Archimedes kann man stets n so wählen, dass $x_{k_n} - x_{l_0}$ beliebig groß wird. Daher kann die Folge (x_k) nicht nach oben beschränkt sein. □

Wie wir oben festgestellt haben, hat die Menge $\mathbb{R}_+^*$ kein Minimum, sie hat aber ein Infimum in $\mathbb{R}$, und zwar 0.

Satz 129 (Satz von Dedekind): *Jede nichtleere nach oben (bzw. unten) beschränkte Teilmenge von $\mathbb{R}$ hat ein Supremum (bzw. Infimum).*

BEWEIS: Wir beweisen den Satz nur für das Supremum, denn die andere Aussage ist analog. Sei also $\emptyset \neq M \subseteq \mathbb{R}$ eine nach oben beschränkte Teilmenge und m eine obere Schranke. Wir konstruieren nun induktiv eine fallende Folge von oberen Schranken und eine wachsende Folge von Elementen aus M. Dazu setzen wir $m_0 := m$ und wählen ein $x_0 \in M$. Falls $m_0 = x_0$ gilt, so ist m_0 ein Maximum und insbesondere ein Supremum. Ist dagegen $m_0 > x_0$, so betrachten wir $y := (m_0 + x_0)/2$. Ist y eine obere Schranke, so setzen wir $m_1 := y$ und $x_1 := x_0$. Gibt es dagegen ein $x_1 \in M$ mit $x_1 > y$, so setzen wir $m_1 := m_0$. In beiden Fällen gilt $x_1 \leq m_1$ und $m_1 - x_1 \leq (m_0 - x_0)/2$.

Diese Konstruktion setzen wir induktiv fort und erhalten so eine fallende Folge von oberen Schranken (m_k) und eine wachsende Folge (x_k) von Elementen aus M, die die Bedingungen $x_k \leq m_k$ und $m_{k+1} - x_{k+1} \leq (m_k - x_k)/2$ erfüllen für alle $k \in \mathbb{N}$. Insbesondere ist $x_0 \leq m_k$ für alle $k \in \mathbb{N}$, d. h. die Folge (m_k) ist durch x_0 nach unten beschränkt. Nach Satz 128 ist daher die Folge (m_k) konvergent. Analog ist die Folge (x_k) durch m_0 nach oben beschränkt und ebenfalls konvergent.

Man kann sich überlegen, dass obige Ungleichungen beim Übergang zum Grenzwert erhalten bleiben, d. h. es gilt $\lim_k x_k \leq \lim_k m_k$ sowie $\lim_k m_k - \lim_k x_k \leq (\lim_k m_k - \lim_k x_k)/2$, woraus $\lim_k m_k \leq \lim_k x_k$ folgt. Insgesamt gilt also $\lim_k m_k = \lim_k x_k$. Wir zeigen, dass $x := \lim_k x_k$ das gesuchte Supremum ist.

Zunächst ist x eine obere Schranke von M. Denn angenommen, dem wäre nicht so. Dann gäbe es ein $y \in M$ mit $y > x$. Für $\varepsilon := y - x$ existiert ein $N \in \mathbb{N}$ mit $|m_N - x| \leq \varepsilon/2$. Damit gilt die Abschätzung

$$m_N \leq \frac{\varepsilon}{2} + x = \frac{y-x}{2} + x = \frac{y+x}{2} < \frac{y+y}{2} = y,$$

was nicht sein kann, da m_N eine obere Schranke von M ist.

Weiter ist x die kleinste obere Schranke. Denn gäbe es eine kleinere Schranke $\widetilde{x}$ mit $\widetilde{x} < x$ und $y \leq \widetilde{x}$ für alle $y \in M$, so würde für die Folge $(x_k) \subseteq M$ gelten $x = \lim_k x_k \leq \widetilde{x} < x$, ein Widerspruch. □

Für manche Überlegungen ist es nützlich, die reellen Zahlen um Punkte im Unendlichen zu erweitern. Formal ist das z. B. möglich, indem man dem Körper R/I die Restklassen $(k)_{k\in\mathbb{N}} + I$ und $(-k)_{k\in\mathbb{N}} + I$ hinzufügt, die man als ∞ und $-\infty$ bezeichnet. Natürlich sind die Folgen $(\pm k)_{k\in\mathbb{N}}$ keine Fundamentalfolgen, und die so erhaltene Menge $\overline{\mathbb{R}}$ ist kein Körper mehr. Dagegen lässt sich die Ordnung von $\mathbb{R}$ auf $\overline{\mathbb{R}}$ übertragen, und es gilt $-\infty < x < \infty$ für alle $x \in \mathbb{R}$. Somit ist $-\infty$ das Minimum und ∞ das Maximum von $\overline{\mathbb{R}}$.

Satz 130: *Die Menge $\overline{\mathbb{R}}$ ist total geordnet, und jede Teilmenge von $\overline{\mathbb{R}}$ hat ein Supremum und ein Infimum in $\overline{\mathbb{R}}$. Insbesondere gilt $\sup\emptyset = -\infty$ und $\inf\emptyset = \infty$. Eine Teilmenge $M \subseteq \overline{\mathbb{R}}$ ist genau dann nicht nach oben (bzw. unten) beschränkt, wenn $\sup M = \infty$ (bzw. $\inf M = -\infty$) gilt.*

Wir werden nun zunächst einige Suprema und Infima berechnen und dann allgemeine Rechenregeln für sie besprechen.

Satz 131: *Die Menge der natürlichen Zahlen $\mathbb{N}$ ist in $\mathbb{R}$ nicht beschränkt.*

BEWEIS: Angenommen, es existierte $s := \sup\mathbb{N} \in \mathbb{R}$, dann wäre $n \leq s$ für alle $n \in \mathbb{N}$. Insbesondere hätte man $n + 1 \leq s$ und somit $n \leq s - 1$, d. h. $s - 1$ wäre schon eine obere Schranke von $\mathbb{N}$, Widerspruch. □

Das wichtigste Beispiel für ein Infimum liefert der folgende

Satz 132: *Es gilt*

$$\inf_{k\in\mathbb{N}^*} \frac{1}{k} = 0.$$

Gilt für ein $x \in \mathbb{R}$ die Bedingung $x \leq \varepsilon$ für alle $\varepsilon > 0$, so ist $x \leq 0$.

BEWEIS: Natürlich ist 0 eine untere Schranke von $(1/k)_{k\in\mathbb{N}^*}$. Gäbe es eine untere Schranke $m > 0$, so hätten wir $m \leq 1/k$ bzw. $k \leq 1/m$ für alle $k \in \mathbb{N}^*$, was Satz 131 widerspricht.

Sei nun x gegeben mit $x \leq \varepsilon$ für alle $\varepsilon > 0$. Dann gilt insbesondere $x \leq 1/k$ für alle $k \in \mathbb{N}^*$, was nach Obigem auf $x \leq \inf_{k\in\mathbb{N}^*} 1/k = 0$ führt. □

Zum Rechnen benötigen wir noch den

Satz 133 (Bernoulli-Ungleichung): *Für alle $n \in \mathbb{N}$ und $x \in \mathbb{R}$ mit $x \geq -1$ gilt*

$$(1 + x)^n \geq 1 + nx.$$

BEWEIS: Wir führen den Beweis durch Induktion nach n. Der Fall $n = 0$ ist klar. Nun gelte die Behauptung für ein $n \in \mathbb{N}$. Dann folgt

$$(1 + x)^{n+1} = (1 + x)(1 + x)^n \geq (1 + x)(1 + nx) = 1 + x + nx + nx^2 \geq 1 + (n + 1)x.$$

□

Wir untersuchen nun die Folgen, die durch Potenzieren einer reellen Zahl entstehen.

Satz 134: *Sei $x \in \mathbb{R}_+^*$.*

(i) Ist $x > 1$, so ist die Folge $(x^k)_{k\in\mathbb{N}}$ streng wachsend, und für alle $y \in \mathbb{R}_+^*$ existiert ein $n \in \mathbb{N}$ mit $x^n \geq y$. Insbesondere gilt

$$\sup_{k\in\mathbb{N}} x^k = \infty.$$

(ii) Ist $0 < x < 1$, so ist die Folge $(x^k)_{k\in\mathbb{N}}$ streng fallend, und für alle $y \in \mathbb{R}_+^*$ existiert ein $n \in \mathbb{N}$ mit $x^n \leq y$. Insbesondere gilt

$$\inf_{k\in\mathbb{N}} x^k = 0.$$

BEWEIS:

(i) Wegen $x > 1$ und $x^k > 0$ ist folglich $x^{k+1} > x^k$. Da $x - 1 > 0$ gibt es nach dem Satz von Archimedes ein $n \in \mathbb{N}$ mit $n(x-1) \geq y$. Mit der Bernoulli-Ungleichung folgt

$$x^n = (1 + (x-1))^n \geq 1 + n(x-1) \geq y.$$

(ii) Mit $x < 1$ und $x^k > 0$ erhält man $x^{k+1} < x^k$. Für ein $y \in \mathbb{R}_+^*$ erhält man nach Teil (i) ein $n \in \mathbb{N}$ mit $(1/x)^n \geq 1/y$, also $y \geq x^n$. Offenbar ist 0 eine untere Schranke der Folge (x^k). Gäbe es eine untere Schranke $m > 0$, so lieferte Teil (i) zu $y := 2/m$ ein $n \in \mathbb{N}$ mit $(1/x)^n \geq 2/m$, also $x^n \leq m/2 < m$, Widerspruch. □

Zur konkreten Berechnung von Suprema und Infima sind einige Rechenregeln nützlich, die es z. B. ermöglichen, Suprema einer Menge durch Infima einer anderen Menge auszudrücken. So gelingt es häufig, sich auf einen schon bekannten Fall zurückzuziehen.

Satz 135: *Seien $M, N \subseteq \mathbb{R}$ nichtleere Teilmengen.*

(i) Ist $M \subseteq N$ und N nach oben beschränkt, so ist auch M nach oben beschränkt, und es gilt

$$\sup M \leq \sup N.$$

(ii) Ist die Familie $(x_{j,k})_{(j,k)\in J\times K}$ nach oben beschränkt, so gilt dies auch für die Familien $(x_{j,k})_{j\in J}$, $(x_{j,k})_{k\in K}$, $(\sup_{j\in J} x_{j,k})_{k\in K}$ und $(\sup_{j\in J} x_{j,k})_{k\in K}$, und es ist

$$\sup_{(j,k)\in J\times K} x_{j,k} = \sup_{k\in K}(\sup_{j\in J} x_{j,k}) = \sup_{j\in J}(\sup_{k\in K} x_{j,k}).$$

(iii) Ist M nach unten beschränkt, so ist $-M$ nach oben beschränkt, und es gilt

$$\inf M = -\sup(-M).$$

(iv) Ist $x \in \mathbb{R}$ und N nach oben beschränkt, so ist $x + N$ nach oben beschränkt, und es gilt

$$\sup(x + N) = x + \sup N.$$

(v) *Sind M, N nach oben beschränkt, so ist dies auch $M + N$, und es gilt*

$$\sup(M + N) = \sup_{x \in M}(x + N) = \sup M + \sup N.$$

(vi) *Ist $x \in \mathbb{R}_+$ und N nach oben beschränkt, so gilt dies auch für $x \cdot N$, und es ist*

$$\sup(x \cdot N) = x \cdot \sup N.$$

(vii) *Ist $M \subseteq \mathbb{R}_+$ und N nach oben beschränkt, so ist auch $M \cdot N$ nach oben beschränkt, und es gilt*

$$\sup(M \cdot N) = \sup_{x \in M}(x \cdot N) = \sup M \cdot \sup N.$$

(viii) *Ist $M \subseteq \mathbb{R}_+^*$ nach oben beschränkt, so ist $1/M$ nach unten beschränkt, und es gilt*

$$\inf \frac{1}{M} = \frac{1}{\sup M}.$$

BEWEIS:

(i) Ist s eine obere Schranke von N, so ist s auch eine obere Schranke von M, also ist M nach oben beschränkt. Da die Menge der oberen Schranken von M die Menge der oberen Schranken von N enthält, ist die kleinste obere Schranke von M kleiner also die kleinste von N.

(ii) Es sei $s \in \mathbb{R}$ eine obere Schranke der Familie $(x_{j,k})_{(j,k) \in J \times K}$. Dann ist s insbesondere für jedes $k \in K$ obere Schranke der Familie $(x_{j,k})_{j \in J}$. Nach dem Satz von Dedekind existiert $\sup_{j \in J} x_{j,k}$, und es gilt $\sup_{j \in J} x_{j,k} \leq s$ für alle $k \in K$. Damit ist auch die Familie $(\sup_{j \in J} x_{j,k})_{k \in K}$ nach oben beschränkt mit $\sup_{k \in K}(\sup_{j \in J} x_{j,k}) \leq s$. Diese Ungleichung gilt für alle oberen Schranken s, und da $\sup_{k \in K}(\sup_{j \in J} x_{j,k})$ per Definition selbst eine obere Schranke der Familie $(x_{j,k})_{(j,k) \in J \times K}$ ist, ist sie somit die kleinste. Die weiteren Aussagen folgen durch Symmetrie.

(iii) Offenbar ist m genau dann untere Schranke von M, wenn $-m$ obere Schranke von $-M$ ist. Insbesondere ist $-M$ nach oben beschränkt, und es gilt $\sup -M = -\inf M$.

(iv) Die Abbildung $s \mapsto x + s$ ist eine Bijektion zwischen den oberen Schranken von N und von $x + N$. Da $\sup(x + N)$ die kleinste obere Schranke von $x + N$ ist, muss sie gleich $x + \sup N$ sein.

(v) Mit Teil (ii) und (iv) erhält man

$$\begin{aligned}\sup(M + N) &= \sup_{(x,y) \in M \times N} x + y = \sup_{x \in M} \sup_{y \in N}(x + y) = \sup_{x \in M}(\sup(x + N)) \\ &= \sup_{x \in M}(x + \sup N) = \sup_{x \in M} x + \sup N = \sup M + \sup N.\end{aligned}$$

(vi) Analog zu Teil (iv).

(vii) Analog zu Teil (v).

(viii) Analog zu Teil (iii). □

Der Satz von Archimedes, die Vollständigkeit und der Satz von Dedekind sind wichtige Charakteristika der reellen Zahlen. Wir werden darauf noch einmal zurückkommen.

5.4.4 Potenzen reeller Zahlen

Wir benutzen in diesem Abschnitt den Satz von Dedekind, um die Quadratwurzel bzw. allgemeiner n-te Wurzeln für reelle Zahlen einzuführen. Wir bemerken zunächst, dass die Abbildung $\mathrm{id}^n\colon \mathbb{R}_+ \to \mathbb{R}_+ \colon x \mapsto x^n$ ordnungstreu ist.

Satz 136: *Für $x, y \in \mathbb{R}$ gilt:*

(i) Es ist $x^2 \leq y^2$ genau dann, wenn $|x| \leq |y|$ ist.

(ii) Für $n \in \mathbb{N}^*$ und $x, y \geq 0$ ist $x^n \leq y^n$ genau dann, wenn $x \leq y$ ist.

BEWEIS:

(i) Es gilt $x^2 \leq y^2$ genau dann, wenn $(y - x)(y + x) \geq 0$ ist. Nach Aufgabe 27 b) ist dies äquivalent zu $y - x, y + x \geq 0$ oder $y - x, y + x \leq 0$. Dies bedeutet $y \geq \pm x$ bzw. $y \geq |x|$ oder $\pm x \leq -y$ bzw. $|x| \leq -y$. Beide Bedingungen lassen sich zusammenfassen zu $|x| \leq |y|$.

(ii) Der Fall $n = 1$ ist klar, und der Fall $n = 2$ wurde in Teil (i) erledigt. Die Aussage gelte nun für ein $n \in \mathbb{N}$. Dann folgt aus $x \leq y$ und der Induktionsvoraussetzung $x^n \leq y^n$

$$x^{n+1} = x^n x \leq y^n x \leq y^n y = y^{n+1}.$$

Damit ist die Rückrichtung gezeigt. Zum Beweis der Hinrichtung verwenden wir die Kontraposition „$x > y$ genau dann, wenn $x^n > y^n$ ist“. Ist $x > y$, so erhält man mit der Induktionsvoraussetzung $x^n > y^n$

$$x^{n+1} = x^n x > y^n x > y^n y = y^{n+1}.$$ □

Die Kontraposition von Teil (ii) zeigt, dass die Abbildung $\mathrm{id}^n\colon \mathbb{R}_+ \to \mathbb{R}_+$ injektiv ist, aber das bringt uns nicht viel weiter. Damit die Wurzel einer positiven reellen Zahl existiert, muss sie auch surjektiv sein.

Satz 137: *Für jedes $x \in \mathbb{R}_+$ und $n \in \mathbb{N}^*$ existiert genau ein $y \in \mathbb{R}_+$ mit $x = y^n$. Die Zahl y heißt n-te* Wurzel *von x und wird mit $\sqrt[n]{x}$ bezeichnet. Es gilt $\sqrt[n]{x} = \sup\{\, z \in \mathbb{R}_+ \mid z^n \leq x \,\}$.*

BEWEIS: Im Fall $x = 0$ ist $y = 0$ und die Behauptung klar. Ansonsten setzen wir $M := \{\, z \in \mathbb{R}_+ \mid z^n \leq x \,\}$. Die Menge M ist wegen $0 \in M$ nicht leer. Wegen $1 \leq \max(1, x)$ gilt $z^n \leq x \leq \max(1, x) \leq \max(1, x)^n$. Mit Satz 136.(ii) ergibt sich $z \leq \max(1, x)$. Folglich ist M durch $\max(1, x)$ nach oben beschränkt, also existiert nach dem Satz von Dedekind $s := \sup M > 0$.

Wir zeigen nun zunächst, dass s eine Lösung der Gleichung $s^n = x$ ist. Dazu beweisen wir $s^n \leq x$ und führen $s^n < x$ zu einem Widerspruch. Aus Satz 135.(vii) folgt durch Induktion

$$s^n = (\sup M)^n = \sup(\underbrace{M \cdots M}_{n \text{ mal}}) = \sup \left\{ \prod_{k=1}^{n} z_k \middle| z_k \in M \right\} \leq x,$$

denn für $z_k \in M$ gilt $z_k \in \mathbb{R}_+$ und $z_k^n \leq x$, also auch

$$\left(\prod_{k=1}^{n} z_k \right)^n = \prod_{k=1}^{n} z_k^n \leq x^n.$$

Angenommen $s^n < x$, so setzen wir

$$\varepsilon := \min \left(s, \frac{x - s^n}{(2^n - 1)s^{n-1}} \right) > 0.$$

Nach Aufgabe 39 gilt für $0 \leq z \leq 1$ die Ungleichung $(1+z)^n \leq 1 + (2^n - 1)z$. Mit $z := \varepsilon/s$ erhält man

$$(s+\varepsilon)^n = s^n \left(1 + \frac{\varepsilon}{s}\right)^n \leq s^n \left(1 + (2^n - 1)\frac{\varepsilon}{s}\right) = s^n + (2^n - 1)s^{n-1}\varepsilon \leq s^n - x + s^n = x.$$

Damit ist $s + \varepsilon \in M$, ein Widerspruch zur Voraussetzung $s = \sup M$.

Es bleibt noch der Beweis der Eindeutigkeit. Dieser besteht aus der bereits bewiesenen Injektivität von id^n auf $\mathbb{R}_+$. □

Im Fall $n = 2$ spricht man auch von der *Quadratwurzel* von x und schreibt kurz $\sqrt{x}$.

Jede rationale Zahl r lässt sich in eindeutiger Weise in der Form $r = n/m$ mit $n \in \mathbb{Z}$, $m \in \mathbb{N}^*$ und m, n teilerfremd schreiben.

Definition 65: *Für $x \in \mathbb{R}_+^*$ und $r \in \mathbb{Q}$ definiert man $x^r := (\sqrt[m]{x})^n$.*

Wir kommen nun zu den Potenzgesetzen für rationale Exponenten. Teil (ii) zeigt, dass man m und n auch mit gemeinsamen Teilern wählen kann, da sie sich herauskürzen.

Satz 138: *Für alle $x, y \in \mathbb{R}_+^*$ und $r, s \in \mathbb{Q}$ gilt:*

(i) $x^r \cdot x^s = x^{r+s}$.

(ii) $(x^r)^s = x^{r \cdot s}$.

(iii) $x^r \cdot y^r = (x \cdot y)^r$.

(iv) Ist $r < s$, so ist $x^r < x^s$ für $x > 1$ und $x^r > x^s$ für $x < 1$.

(v) Ist $x < y$, so ist $x^r < y^r$ für $r > 0$ und $x^r > y^r$ für $r < 0$.

BEWEIS: Beim Beweis benutzt man die schon bewiesenen Potenzgesetze für ganze Zahlen und die Eindeutigkeit der Wurzel. Wir lassen ihn als Übungsaufgabe. □

Natürlich liegt es nun nahe, zu reellen Exponenten ρ überzugehen. Dazu schränken wir uns zunächst auf $x \in \mathbb{R}$ mit $x \geq 1$ ein und betrachten die Menge $M := \{ x^r \mid r \in \mathbb{Q}, r \leq \rho \}$. Offenbar ist sie nicht leer, und wegen $x \geq 1$ ist $x^r \leq x^{\lceil \rho \rceil}$ für alle $r \in \mathbb{Q}$ mit $r \leq \rho$. Folglich ist M durch $x^{\lceil \rho \rceil}$ nach oben beschränkt. Nach dem Satz von Dedekind existiert also $\sup M$.

Definition 66: *Für $x \in \mathbb{R}_+^*$ und $\rho \in \mathbb{R}$ definiert man*

$$x^\rho := \begin{cases} \sup\{ x^r \mid r \in \mathbb{Q}, r \leq \rho \} & \text{falls } x \geq 1 \\ \left(\frac{1}{x}\right)^{-\rho} & \text{falls } x < 1. \end{cases}$$

Für rationale ρ wird das Supremum ein Maximum, und die neue Definition stimmt mit der alten überein.

Satz 139 (Potenzgesetze): *Für alle $x, y \in \mathbb{R}_+^*$ und $\rho, \sigma \in \mathbb{R}$ gilt:*

(i) $x^\rho \cdot x^\sigma = x^{\rho+\sigma}$

(ii) $(x^\rho)^\sigma = x^{\rho \cdot \sigma}$

(iii) $x^\rho \cdot y^\rho = (x \cdot y)^\rho$.

(iv) Ist $\rho < \sigma$, so ist $x^\rho < x^\sigma$ für $x > 1$ und $x^\rho > x^\sigma$ für $x < 1$.

(v) Ist $x < y$, so ist $x^\rho < y^\rho$ für $\rho > 0$ und $x^\rho > y^\rho$ für $\rho < 0$.

BEWEIS: Wir benutzen die Potenzgesetze für rationale Exponenten.

(i) Sei zunächst $x > 1$. Mit Satz 135.(vii) und Aufgabe 40 a) erhält man

$$\begin{aligned} x^\rho \cdot x^\sigma &= \sup\{ x^r \mid r \in \mathbb{Q}, r < \rho \} \cdot \sup\{ x^s \mid s \in \mathbb{Q}, s < \sigma \} \\ &= \sup\{ x^r \cdot x^s \mid r, s \in \mathbb{Q}, r < \rho, s < \sigma \} \\ &= \sup\{ x^{r+s} \mid r, s \in \mathbb{Q}, r < \rho, s < \sigma \}. \end{aligned}$$

Sei nun $t \in \mathbb{Q}$ mit $t < \rho + \sigma$. Da $\mathbb{Q}$ dicht ist in $\mathbb{R}$, gibt es ein $r \in \mathbb{Q}$ mit $t - \rho < r < \sigma$. Für $s := t - r \in \mathbb{Q}$ gilt $t = r + s$ und $s < \rho$. Daher ist

$$x^\rho \cdot x^\sigma = \sup\{ x^{r+s} \mid r, s \in \mathbb{Q}, r < \rho, s < \sigma \} = \sup\{ x^t \mid t \in \mathbb{Q}, t < \rho + \sigma \} = x^{\rho+\sigma}.$$

Für $x < 1$ rechnet man

$$x^\rho \cdot x^\sigma = \left(\frac{1}{x}\right)^{-\rho} \cdot \left(\frac{1}{x}\right)^{-\sigma} = \left(\frac{1}{x}\right)^{-(\rho+\sigma)} = x^{\rho+\sigma}.$$

(ii) Es sei wieder $x > 1$. Nach Aufgabe 40 gilt für $\rho, \sigma > 0$

$$\begin{aligned}(x^\rho)^\sigma &= \sup\{\, (x^\rho)^s \mid s \in \mathbb{Q}, 0 < s < \sigma \,\} \\ &= \sup\{\, (\sup\{\, x^r \mid r \in \mathbb{Q}, 0 < r < \rho \,\})^s \mid s \in \mathbb{Q}, 0 < s < \sigma \,\} \\ &= \sup\{\, \sup\{\, (x^r)^s \mid r \in \mathbb{Q}, 0 < r < \rho \,\} \mid s \in \mathbb{Q}, 0 < s < \sigma \,\} \\ &= \sup\{\, \sup\{\, x^{rs} \mid r \in \mathbb{Q}, 0 < r < \rho \,\} \mid s \in \mathbb{Q}, 0 < s < \sigma \,\} \\ &= \sup\{\, x^{rs} \mid r, s \in \mathbb{Q}, 0 < r < \rho, 0 < s < \sigma \,\}.\end{aligned}$$

Sei nun $t \in \mathbb{Q}$ mit $0 < t < \rho \cdot \sigma$. Weil $\mathbb{Q}$ in $\mathbb{R}$ dicht liegt, gibt es $s \in \mathbb{Q}$ mit $t/\rho < s < \sigma$. Für $r := t/s \in \mathbb{Q}$ gilt $t = r \cdot s$ und $r < \rho$. Somit gilt

$$\begin{aligned}(x^\rho)^\sigma &= \sup\{\, x^{rs} \mid r, s \in \mathbb{Q}, 0 < r < \rho, 0 < s < \sigma \,\} \\ &= \sup\{\, x^t \mid t \in \mathbb{Q}, 0 < t < \rho \cdot \sigma \,\} = x^{\rho \cdot \sigma}.\end{aligned}$$

Für alle $\rho \in \mathbb{R}$ gilt per Definition $(x^{-1})^\rho = x^{-\rho}$. Weiter ist nach Teil (i) $x^{-\rho} \cdot x^\rho = x^{-\rho+\rho} = x^0 = 1$ und folglich $x^{-\rho} = (x^\rho)^{-1}$. Nun rechnen wir für $\rho, \sigma < 0$

$$(x^\rho)^\sigma = (x^{-(-\rho)})^\sigma = ((x^{-\rho})^{-1})^\sigma = (x^{-\rho})^{-\sigma} = x^{(-\rho)\cdot(-\sigma)} = x^{\rho\cdot\sigma}.$$

Der einzige weitere nichttriviale Fall ist $\rho < 0$ und $\sigma > 0$. In diesem Fall gilt

$$(x^\rho)^\sigma = ((x^{-1})^{-\rho})^\sigma = (x^{-1})^{(-\rho)\cdot\sigma} = (x^{-1})^{-\rho\cdot\sigma} = x^{\rho\cdot\sigma}.$$

Es bleibt nur noch, die Behauptung für $x < 1$ zu prüfen. Hier ist für beliebige ρ, σ

$$(x^\rho)^\sigma = ((x^{-1})^{-\rho})^\sigma = (x^{-1})^{-\rho\cdot\sigma} = x^{\rho\cdot\sigma}.$$

(iii) Für $x, y \geq 1$ folgt aus Satz 135.(vii)

$$\begin{aligned}x^\rho \cdot y^\rho &= \sup\{\, x^r \mid r \in \mathbb{Q}, r \leq \rho \,\} \cdot \sup\{\, x^s \mid s \in \mathbb{Q}, s \leq \rho \,\} \\ &= \sup\{\, x^r \cdot y^s \mid r, s \in \mathbb{Q}, r, s \leq \rho \,\} \\ &= \sup\{\, (x \cdot y)^r \mid r \in \mathbb{Q}, r \leq \rho \,\} = (x \cdot y)^\rho.\end{aligned}$$

Die anderen Fälle rechnet man analog.

(iv) Da $\mathbb{Q}$ dicht liegt in $\mathbb{R}$, existieren $r, s \in \mathbb{Q}$ mit $\rho < r < s < \sigma$. Im Fall $x > 1$ ist dann

$$x^\rho = \sup\{\, x^t \mid t \in \mathbb{Q}, t \leq \rho \,\} \leq x^r < x^s \leq \sup\{\, x^t \mid t \in \mathbb{Q}, t \leq \sigma \,\} = x^\sigma$$

und für $x < 1$

$$\begin{aligned}x^\sigma &= (x^{-1})^{-\sigma} = \sup\{\, (x^{-1})^t \mid t \in \mathbb{Q}, t \leq -\sigma \,\} \leq (x^{-1})^s \\ &< (x^{-1})^r \leq \sup\{\, (x^{-1})^t \mid t \in \mathbb{Q}, t \leq -\rho \,\} = (x^{-1})^{-\rho} = x^\rho.\end{aligned}$$

(v) Sei zunächst $\rho > 0$. Dann gilt nach Teil c)

$$\frac{y^\rho}{x^\rho} = \left(\frac{y}{x}\right)^\rho = \sup\left\{ \left(\frac{y}{x}\right)^r \middle| \, r \in \mathbb{Q}, r \leq \rho \right\}.$$

Wegen $y/x > 1$ ist $(y/x)^r > 1$ für alle $r \in \mathbb{Q}$ mit $r > 0$. Daraus folgt $y^\rho/x^\rho > 1$, also $y^\rho > x^\rho$. Analog argumentiert man im Fall $\rho < 0$. □

5.4.5 Charakterisierung der reellen Zahlen

An dieser Stelle ist es an der Zeit, einmal das bisher Erreichte zu rekapitulieren. Die natürlichen Zahlen hatten wir rein mengentheoretisch konstruiert. Natürlich war das Unendlichkeitsaxiom gerade so gewählt, dass dies in der gezeigten Form gelingt. Die ganzen und die rationalen Zahlen waren dann rein algebraische Erweiterungen der natürlichen Zahlen. Wir hatten aber bereits bei den rationalen Zahlen festgestellt, dass sie als kleinster total geordneter Körper ein ganz natürliches mathematisches Objekt sind, das praktisch unabhängig von seiner Vorgeschichte interessant ist.

Bei den reellen Zahlen kommt nun ein neues Element ins Spiel, und zwar die Analysis. Die Konstruktion als Quotient der Fundamentalfolgen über den Nullfolgen macht sehr deutlich, wie eng die reellen Zahlen mit der Analysis verbunden sind. Wir haben ja auch zum Beweis der Vollständigkeit explizit diese Konstruktion verwendet. Ganz analog zu den rationalen Zahlen kann man auch die reellen Zahlen abstrakt charakterisieren, wobei aber stets analytische (man könnte auch sagen topologische) Eigenschaften auftreten. Wir geben jetzt, soweit es an dieser Stelle schon möglich ist, einige dieser Charakterisierungen an.

Definition 67 (Teilfolge): *Ist $\alpha\colon \mathbb{N} \to \mathbb{N}\colon l \mapsto \alpha(l)$ eine streng wachsende Abbildung und $(x_k)_{k\in\mathbb{N}}$ eine Folge von Elementen aus M, so heißt die Abbildung*

$$\mathbb{N} \longrightarrow M\colon l \longmapsto x_{\alpha(l)}$$

eine Teilfolge *der Folge $(x_k)_{k\in\mathbb{N}}$. Man schreibt $(x_{\alpha(l)})_{l\in\mathbb{N}}$ oder $(x_{k_l})_{l\in\mathbb{N}}$.*

Wichtig für unsere Zwecke ist der

Satz 140: *Ist K ein total geordneter Körper und $(x_k)_{k\in\mathbb{N}}$ eine Folge von Elementen aus K, so existiert eine monotone Teilfolge $(x_{\alpha(l)})_{l\in\mathbb{N}}$.*

BEWEIS: Wir setzen $M := \{\, k \in \mathbb{N} \mid x_l \leq x_k \text{ für alle } l \geq k \,\}$. Es können nun zwei Fälle eintreten: M ist endlich oder M ist unendlich. Ist M unendlich, so erhält man durch eine Aufzählung α der Elemente von M eine fallende Teilfolge $(x_{\alpha(l)})_{l\in\mathbb{N}}$. Ist M dagegen endlich, so setzen wir $\alpha(0) := \max M + 1$. Wegen $\alpha(0) \notin M$ existiert ein Index $\alpha(1)$ mit $\alpha(1) \geq \alpha(0)$ und $x_{\alpha(1)} > x_{\alpha(0)}$. Da wiederum $\alpha(1) \notin M$ erhält man so induktiv eine wachsende Teilfolge $(x_{\alpha(l)})_{l\in\mathbb{N}}$. □

Wir hatten für die reellen Zahlen zunächst den Satz von Archimedes und die Vollständigkeit gezeigt. Dann hatten wir beide Eigenschaften für den Beweis benutzt, dass monotone beschränkte Folgen konvergent sind. Daraufhin hatten wir allein aus dieser Tatsache den Satz von Dedekind abgeleitet. Der folgende Satz zeigt nun, dass wir auch anders hätten vorgehen können.

Satz 141: *Es sei K ein total geordneter Körper. Dann sind folgende Aussagen äquivalent:*

(i) Jede nichtleere nach oben (bzw. unten) beschränkte Teilmenge von K hat ein Supremum (bzw. Infimum).

(ii) Jede wachsende (bzw. fallende) Folge, die nach oben (bzw. unten) beschränkt ist, konvergiert.

(iii) Die Ordnung auf K ist archimedisch, und K ist vollständig.

BEWEIS:
„(i) $\Rightarrow$ (ii)“: Es sei (x_k) eine nach oben beschränkte, wachsende Folge. Nach Voraussetzung existiert $s := \sup_{k\in\mathbb{N}} x_k$. Nun sei $\varepsilon > 0$ gegeben. Aufgrund der Approximationseigenschaft gibt es ein $N \in \mathbb{N}$ mit $x_N > s - \varepsilon$. Da die Folge (x_k) wachsend ist, gilt $s - \varepsilon \leq x_N \leq x_k \leq s$ und somit $|x_k - s| \leq \varepsilon$ für alle $k \geq N$.
„(ii) $\Rightarrow$ (iii)“: Wir zeigen zunächst, dass die Ordnung archimedisch ist. Seien dazu $x, y > 0$ gegeben. Angenommen, es wäre $ny < x$ für alle $n \in \mathbb{N}$. Dann wäre x eine obere Schranke der wachsenden Folge $(ny)_{n\in\mathbb{N}}$, welche nach Voraussetzung gegen $s \in K$ konvergiert. Damit existiert $N \in \mathbb{N}$ mit $|ny - s| \leq y$, d. h. $s - y \leq ny \leq s$, für alle $n \geq N$. Wegen $s - (s - y) = y$ kann dies nicht sein.

Zum Beweis der Vollständigkeit betrachten wir eine Fundamentalfolge (x_k) aus Elementen von K. Völlig analog zum Beweis von Satz 119 zeigt man, dass die Folge (x_k) beschränkt ist. Außerdem besitzt diese Folge nach Satz 140 eine monotone Teilfolge (x_{k_l}), die natürlich ebenfalls beschränkt ist. Nach Voraussetzung existiert $s := \lim_l x_{k_l}$. Nun sei $\varepsilon > 0$ gegeben. Dann gibt es ein $N \in \mathbb{N}$ mit $|x_k - x_m| \leq \varepsilon/2$ für alle $k, m \geq N$. Ferner existiert ein $l \in \mathbb{N}$, so dass $k_l \geq N$ ist und $|x_{k_l} - s| \leq \varepsilon/2$ gilt. Dann folgt für alle $k \geq N$

$$|x_k - s| = |x_k - x_{k_l} + x_{k_l} - s| \leq |x_k - x_{k_l}| + |x_{k_l} - s| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

„(iii) $\Rightarrow$ (i)“: In den entsprechenden Beweisen dieses Kapitels kann man $\mathbb{R}$ durch K ersetzen, ohne dass ein Argument geändert werden müsste. □

Dies sind nur drei von vielen weiteren Eigenschaften der reellen Zahlen, die untereinander äquivalent sind. Unser Ziel ist es zu zeigen, dass ein total geordneter Körper, der eine dieser äquivalenten Eigenschaften erfüllt, schon isomorph zum Körper der reellen Zahlen ist. Nach dem Monomorphiesatz ist $\mathbb{Q}$ isomorph zum Primkörper eines total geordneten Körpers, und zur Vereinfachung der Notation identifizieren wir beide miteinander.

Satz 142: *Es sei K ein total geordneter Körper. Der Primkörper $\mathbb{Q}$ liegt genau dann dicht in K, wenn K archimedisch geordnet ist.*

BEWEIS: Es sei $\mathbb{Q}$ dicht in K. Dann gibt es zu gegebenen $x, y \in K$ mit $x, y > 0$ rationale r, s mit $x < r$ und $0 < s < y$. Da die Ordnung auf $\mathbb{Q}$ archimedisch ist, existiert ein $n \in \mathbb{N}$ mit $ns > r$ und folglich $ny > ns > r > x$.

Sei nun umgekehrt K archimedisch geordnet. Wir müssen zu $x, y \in K$ mit $x < y$ ein $r \in \mathbb{Q}$ finden mit $x < r < y$. Zunächst gibt es ein $n \in \mathbb{N}$ mit $(y - x)^{-1} < n$. Für $m := [nx]$ gilt $m/n \leq x < (m + 1)/n$. Insgesamt folgt $x < (m + 1)/n \leq x + 1/n < y$. □

Es ist erstaunlich, dass die Anzahl der Körperautomorphismen von $\mathbb{R}$ sehr übersichtlich ist.

Satz 143: *Ein total geordneter Körper mit den Eigenschaften aus Satz 141 hat die Identität als einzigen Automorphismus.*

BEWEIS: Es sei K ein solcher Körper. Jeder Automorphismus f erfüllt $f(0) = 0$ und $f(1) = 1$. Wie im Beweis von Satz 81 zeigt man nun $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.

Wir wissen aus dem letzten Abschnitt, dass in K Quadratwurzeln existieren. Nun ist $x \leq y$ genau dann, wenn $y - x \in K_+$ ist, d. h. wenn es ein $z \in K_+$ gibt mit $y - x = z^2$. Anwendung von f liefert $f(y) - f(x) = f(z)^2 \geq 0$, also $f(x) \leq f(y)$. Daher ist f ordnungstreu.

Da nach Obigem $\mathbb{Q}$ in K dicht liegt, existiert zu $x \in K$ eine rationale Folge (r_k) mit $\lim_k r_k = x$. Nach Satz 140 besitzt sie eine monotone Teilfolge (r_{k_l}), und wir gehen o. E. davon aus, dass sie wachsend ist. Man kann sich überlegen, dass diese Teilfolge denselben Grenzwert hat. Dann gibt es für jedes rationale $\varepsilon > 0$ ein $N \in \mathbb{N}$ mit $0 \leq x - x_{k_l} \leq \varepsilon$ für alle $k \geq N$. Da f ordnungstreu und die Identität auf $\mathbb{Q}$ ist, folgt $0 \leq f(x) - x_{k_l} \leq \varepsilon$ für alle $k \geq N$. Damit ergibt sich $f(x) = \lim_l x_{k_l} = x$, d. h. $f = \mathrm{id}_K$. □

Wir kommen nun zum Hauptergebnis dieses Abschnitts.

Satz 144: *Ist K ein total geordneter Körper, der die äquivalenten Eigenschaften aus Satz 141 erfüllt, so ist K isomorph zu Körper der reellen Zahlen $\mathbb{R}$.*

BEWEIS: Wir konstruieren einen Isomorphismus $f\colon K \to \mathbb{R}$. Wie oben liegt $\mathbb{Q}$ dicht in K, also existiert zu $x \in K$ eine rationale Folge (r_k) mit $\lim_k r_k = x$. Da konvergente Folgen Fundamentalfolgen sind, ist die Abbildung $f\colon x \mapsto (r_k) + I$ wohldefiniert, wobei I das Nullfolgenideal bezeichnet.

Wir zeigen nun, dass f ein Körperhomomorphismus ist. Seien dazu $x, y \in K$ und $(r_k), (s_k)$ rationale Folgen mit $\lim_k r_k = x$ und $\lim_k s_k = y$. Dann konvergiert $(r_k + s_k)$ gegen $x + y$ (siehe Aufgabe 41), und es gilt

$$f(x + y) = (r_k + s_k) + I = ((r_k) + I) + ((s_k) + I) = f(x) + f(y).$$

Analog zeigt man $f(x \cdot y) = f(x) \cdot f(y)$.

Per Konstruktion ist f injektiv. Da K vollständig ist, ist f auch surjektiv: Jeder Repräsentant (r_k) einer reellen Zahl definiert in K eine Fundamentalfolge, und diese konvergiert gegen ein $x \in K$ mit $f(x) = (r_k) + I$. Insgesamt ist f ein Isomorphismus. □

Übungsaufgaben

Aufgabe 29: Zeige, dass für alle $m, n \in \mathbb{N}$ mit $m < n$ gilt $m + 1 \leq n$.

Aufgabe 30: Zeige: Die Abbildung $\mathbb{N} \to \{\, m \in \mathbb{N} \mid m \geq k \,\}\colon n \mapsto n + k$ ist für alle $k \in \mathbb{N}$ bijektiv.

Aufgabe 31: Seien M, N disjunkte endliche Mengen. Zeige, dass für die Mächtigkeiten gilt $|M \cup N| = |M| + |N|$.

Aufgabe 32: Seien $m, n \in \mathbb{N}$ und M, N Mengen mit $|M| = m$ und $|N| = n$. Finde hinreichende und notwendige Bedingungen an die Zahlen m, n, so dass eine Abbildung $M \to N$ existiert, die

a) injektiv

b) surjektiv

c) bijektiv

ist.

Aufgabe 33: Zeige: Ist M eine endliche Menge und $f\colon M \to M$ eine surjektive Abbildung, so ist f auch injektiv.

Aufgabe 34: Zeige, dass in einer kommutativen Halbgruppe M für alle $x, y \in M$ und $m, n \in \mathbb{N}^*$ die *Potenzgesetze*

a) $x^n y^m = y^m x^n$

b) $(xy)^n = x^n y^n$.

gelten. In einem kommutativen Monoid gelten sie auch für $m, n = 0$ und in einer abelschen Gruppe für alle $m, n \in \mathbb{Z}$.

Aufgabe 35: Beweise die folgenden Summenformeln:

a) $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

b) $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$

c) $\displaystyle\sum_{k=1}^{n} k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$.

Aufgabe 36: Sei (r_k) mit $r_k \neq 0$ für alle $k \in \mathbb{N}$ eine Fundamentalfolge, die keine Nullfolge ist. Zeige, dass es ein $s > 0$ gibt mit $|r_k| \geq s$ für alle $k \in \mathbb{N}$.

Aufgabe 37: Zeige, dass für alle $x, y \in \mathbb{R}$ gilt

a) $\max(x, y) + \min(x, y) = x + y$

b) $\max(x, y) = \dfrac{x + y + |x + y|}{2}$

c) $\min(x, y) = \dfrac{x + y - |x + y|}{2}$.

Aufgabe 38: Es seien $M, N \subseteq \mathbb{R}$ nichtleer und beschränkt. Zeige:

a) $\sup(M \cup N) = \max(\sup M, \sup N)$ und $\inf(M \cup N) = \min(\inf M, \inf N)$.

b) Sind M, N nicht disjunkt, so gilt $\sup(M \cap N) \leq \min(\sup M, \sup N)$ und $\inf(M \cup N) \geq \max(\inf M, \inf N)$. Können die Ungleichungen auch strikt sein?

Aufgabe 39: Zeige: Für $n \in \mathbb{N}$ und $x \in \mathbb{R}$ mit $0 \leq x \leq 1$ gilt $(1+x)^n \leq 1 + (2^n - 1)x$.

Aufgabe 40: Zeige:

a) Für $x \in \mathbb{R}$ mit $x \geq 1$ und $\rho \in \mathbb{R}$ gilt $x^\rho = \sup\{\, x^r \mid r \in \mathbb{Q}, r < \rho \,\}$.

b) Ist $(M_j)_{j \in J}$ eine Familie beschränkter Teilmengen von $\mathbb{R}$, so dass $\bigcup_{j \in J} M_j$ ebenfalls beschränkt ist, so gilt

$$\sup\{\, \sup M_j \mid j \in J \,\} = \sup \bigcup_{j \in J} M_j.$$

c) Ist M eine durch 1 nach unten beschränkte Teilmenge von $\mathbb{R}$ und $r \in \mathbb{Q}_+^*$, so ist $\sup M^r = (\sup M)^r$.

Aufgabe 41: In einem total geordneten Körper K gelte $\lim_k x_k = x$ und $\lim_k y_k = y$. Zeige:

a) $\lim_k (x_k + y_k) = x + y$

b) $\lim_k (x_k \cdot y_k) = x \cdot y$.

A Das Zorn'sche Lemma

Für die Anwendungen ist eine Umformulierung des Auswahlaxioms wichtig, die Zorn'sches Lemma genannt wird. Das Zorn'sche Lemma ist auf Basis der restlichen Axiome äquivalent zum Auswahlaxiom. Es wird z. B. für den Beweis verwendet, dass jeder Vektorraum eine Basis besitzt. In diesem Anhang wird gezeigt, dass das Zorn'sche Lemma aus dem Auswahlaxiom folgt. Dies erfordert zunächst eine Beschäftigung mit geordneten Mengen.

Definition 68 (Wohlordnung): *Eine geordnete Menge heißt* wohlgeordnet *und die betreffende Ordnung eine* Wohlordnung*, wenn jede ihrer nichtleeren Teilmengen ein Minimum besitzt.*

Offenbar gilt der

Satz 145: *Jede wohlgeordnete Menge ist total geordnet.*

BEWEIS: Seien M eine wohlgeordnete Menge und $x, y \in M$. Dann besitzt die Menge $\{x, y\}$ ein Minimum, also gilt $x \leq y$ oder $y \leq x$. □

Nun vereinfachen wir die Sprechweise. Eine total geordnete Menge nennen wir eine *Kette*. Eine Teilmenge einer Kette ist dann ebenfalls eine Kette, die wir Teilkette nennen.

Sei nun M eine wohlgeordnete Menge und K eine Kette in M. Eine Teilkette A von K heißt *Anfangsstück* von K, wenn

$$A = \left\{ x \in K \,\middle|\, \exists_{a \in A} : x \leq a \right\}$$

gilt. Weiter definieren wir für $x \in K$ den *Abschnitt* K_x von K als

$$K_x := \{\, y \in K \mid y < x \,\}.$$

Ist umgekehrt $N \subseteq K$ eine Teilkette, und gibt es ein $x \in K$ mit $K_x = N$, so heißt K eine *Fortsetzung* von N.

Offenbar gilt dann der

Satz 146: *Die Anfangsstücke einer wohlgeordneten Kette K sind genau die Abschnitte K_x mit $x \in K$ und K selbst.*

Die leere Menge ist als Abschnitt des Minimums von K ebenfalls Anfangsstück.

Definition 69: *Man nennt zwei wohlgeordnete Ketten von M* vergleichbar*, wenn die eine Anfangsstück der anderen ist.*

Für später notieren wir den

Satz 147: *Sei $(K_i)_{i\in I}$ eine Familie wohlgeordneter Ketten von M, von denen je zwei vergleichbar sind. Dann ist $K := \bigcup_{i\in I} K_i$ wohlgeordnet, und alle K_i sind Anfangsstücke von K.*

BEWEIS: Sei $\emptyset \neq K' \subseteq K$ eine nichtleere Teilkette. Dann gibt es ein $i \in I$ mit $K_i \cap K' \neq \emptyset$. Da K_i wohlgeordnet und $K_i \cap K' \subseteq K_i$ ist, gibt es ein Minimum x von $K_i \cap K'$. Wir zeigen nun, dass x schon Minimum von K' ist. Sei dazu $y \in K'$ mit $y \leq x$. Es gibt es $j \in I$ mit $y \in K_j$. Es können nun zwei Fälle auftreten: K_j ist Anfangsstück von K_i oder umgekehrt. Im ersten Fall folgt direkt $y \in K_i$. Im zweiten Fall folgt wegen $y \leq x$ ebenfalls $y \in K_i$. Da nun $y \in K_i$, ist auch $y \in K_i \cap K'$. Es ist aber x Minimum von $K_i \cap K'$, woraus sofort $y = x$ folgt.

Nun sei $i \in I$, $x \in K$ und $x_i \in K_i$ mit $x \leq x_i$. Können wir zeigen, dass $x \in K_i$ ist, so ist K_i Anfangsstück von K. Es gibt ein $j \in I$ mit $x \in K_j$. Wegen der Vergleichbarkeit von K_i und K_j folgt wie oben die Behauptung. □

Wir wiederholen nun kurz das Auswahlaxiom: „Das kartesische Produkt einer nichtleeren Familie von nichtleeren Mengen ist nichtleer." Die Bezeichnung Auswahlaxiom ergibt sich unmittelbar aus dem folgenden

Satz 148 (Auswahlfunktion): *Sei $(M_i)_{i\in I}$ eine Familie nichtleerer Mengen. Dann gibt es eine* Auswahlfunktion *$f\colon I \to \bigcup_{i\in I} M_i$ mit $f(i) \in M_i$ für alle $i \in I$.*

BEWEIS: Laut Auswahlaxiom ist das kartesische Produkt der M_i nichtleer. Also existiert

$$f \in \prod_{i\in I} M_i.$$

Nach Definition des kartesischen Produkts ist f eine Familie $(y_i)_{i\in I}$ mit $y_i \in M_i$ für alle $i \in I$. Wegen $y_i = f(i)$ folgt schon die Behauptung. □

Die Auswahlfunktion wählt also aus jeder Menge M_i ein Element aus. Nun haben wir alle nötigen Vorbereitungen gemacht.

Satz 149 (Zorn'sches Lemma): *Sei $M \neq \emptyset$ eine geordnete Menge, und jede wohlgeordnete Kette von M besitze eine obere Schranke. Dann hat M mindestens ein maximales Element.*

BEWEIS: Es sei W die Menge aller wohlgeordneten Ketten von M. Dann gilt nach Voraussetzung für alle $K \in W$

$$\widetilde{S}(K) := \{\, s \in M \mid s \text{ ist obere Schranke von } K \,\} \neq \emptyset.$$

Daher können wir definieren

$$S(K) := \begin{cases} \{\, s \in \widetilde{S}(K) \mid s \notin K \,\} & \text{falls } \widetilde{S}(K) \not\subseteq K \\ \widetilde{S}(K) & \text{falls } \widetilde{S}(K) \subseteq K, \end{cases}$$

und es ist $S(K) \neq \emptyset$. Jetzt wählen wir eine Auswahlfunktion

$$f\colon W \longrightarrow \bigcup_{K \in W} S(K)$$

mit $f(K) \in S(K)$ für alle $K \in W$. Wir betrachten nun die Menge

$$W' := \{\, K \in W \mid f(K_x) = x \text{ für alle } x \in K \,\}.$$

Da die leere Menge wohlgeordnet ist, ist $\emptyset \in W$. Sie besitzt aber keine Abschnitte, weswegen auch $\emptyset \in W'$ folgt. Daher ist $W' \neq \emptyset$.

Wir zeigen nun, dass je zwei Ketten $K_1, K_2 \in W'$ vergleichbar sind. Anfangsstücke derselben wohlgeordneten Kette sind immer vergleichbar. Sei also K die Vereinigung aller gemeinsamen Anfangsstücke von K_1 und K_2. Nach Satz 147 ist K eine wohlgeordnete Kette, und zwar das bzgl. der Inklusion größte gemeinsame Anfangsstück von K_1 und K_2. Nun nehmen wir $K_1 \neq K$ sowie $K_2 \neq K$ an. Es gibt $x_1 \in K_1$, $x_2 \in K_2$ mit $K = K_{1x_1} = K_{2x_2}$. Es gilt aber $x_1 = f(K_{1x_1}) = f(K_{2x_2}) = x_2$, also ist $K \cup \{x_1\}$ echte Obermenge von K und Anfangsstück von K_1 und K_2, im Widerspruch zur Konstruktion von K.

Nun ist also

$$K' := \bigcup_{K \in W'} K$$

eine wohlgeordnete Kette, deren Anfangsstücke die $K \in W'$ sind. Zu jedem $x \in K'$ gibt es ein $K \in W'$ mit $x \in K$. Da K Anfangsstück von K' ist, folgt $K'_x = K_x$ und somit $f(K'_x) = f(K_x) = x$. Insgesamt ist also $K' \in W'$. Per Konstruktion enthält K' alle Ketten von W', also gilt $f(K') \in K'$. Andernfalls wäre $K' \cup \{f(K')\}$ eine echte Obermenge von K' aus W'.

Es bleibt nur noch zu zeigen, dass $f(K')$ ein maximales Element von M ist. Aus $f(K') \in K'$ ergibt sich $\widetilde{S}(K') \subseteq K'$. Sei nun $x \in M$ und $f(K') \leq x$. Dann ist $x \in \widetilde{S}(K')$ und daher $x \in K'$. Es ist aber $f(K')$ obere Schranke von K', also $x \leq f(K')$ und schließlich $x = f(K')$. □

Die Mächtigkeit des Zorn'schen Lemmas zeigt sich z. B. in dem erstaunlichen

Satz 150 (Wohlordnungssatz): *Jede Menge lässt sich wohlordnen.*

BEWEIS: Sei M eine Menge. Wir betrachten die Menge W aller Teilmengen von M, die sich wohlordnen lassen. Dann führen wir auf W eine Ordnungsrelation dadurch ein, dass $x \leq y$ gelten soll, wenn y eine Fortsetzung von x ist. Wegen $\emptyset \in W$ ist $W \neq \emptyset$. Sei nun K eine Kette aus W. Dann ist nach Satz 147 die Vereinigung V aller Elemente von K wohlgeordnet, und V ist eine obere Schranke bzgl. der Ordnungsrelation der Fortsetzung. Nun folgt aus Satz 149, dass W ein maximales Element besitzt, also eine bzgl. Fortsetzung größte wohlgeordnete Menge X. Es bleibt nur noch $M = X$ zu zeigen. Gäbe es aber ein $x \in M \setminus X$, so wäre $X \cup \{x\}$ echte Obermenge von X. Ändert man die Ordnung von $X \cup \{x\}$ so ab, dass x das größte Element wird, so erhält man wieder eine Wohlordnung, im Widerspruch zur Wahl von X. □

Man mache sich klar, wie verrückt dieser Satz ist: Wie soll etwa eine Wohlordnung von $\mathbb{C}$ aussehen?! Hier zeigt sich bereits, weshalb viele Mathematiker das Auswahlaxiom ablehnen.

Es ist eine interessante Tatsache, dass man das Prinzip der vollständigen Induktion auf wohlgeordnete Mengen, d. h. auch auf überabzählbare Mengen, übertragen kann.

Satz 151 (Prinzip der transfiniten Induktion): *Sei M eine wohlgeordnete Menge und $N \subseteq M$ eine Teilmenge, so dass für alle $x \in M$ gilt*

$$M_x \subseteq N \Rightarrow x \in N.$$

Dann ist $N = M$.

BEWEIS: Angenommen $N \neq M$, d. h. $M \setminus N \neq \emptyset$. Dann besitzt $M \setminus N$ ein kleinstes Element x. Somit gilt aber $M_x \subseteq N$, also $x \in N$. Widerspruch. □

B Die Konstruktion des Polynomrings

Wir gehen nun auf die explizite Konstruktion des Polynomrings ein. Wie schon erwähnt, geschieht dies, indem man Abbildungen $p\colon \mathbb{N} \to R$ mit $p(k) \neq 0$ nur für endlich viele $k \in \mathbb{N}$ betrachtet. Es bezeichne $R[X]$ die Menge solcher Abbildungen.

Wir müssen nun zunächst Verknüpfungen auf $R[X]$ einführen, so dass $R[X]$ ein Ring wird. Wie gehabt setzen wir dazu für $a, b \in R[X]$

$$(a+b)(n) = a(n) + b(n)$$

und

$$(a \cdot b)(n) = \sum_{k=0}^{n} a(k) \cdot b(n-k)$$

für alle $n \in \mathbb{N}$. Definiert man für jedes Element $r \in R$ eine Abbildung $r\colon \mathbb{N} \to R$ mit $r(0) = r$ und $r(k) = 0$ für $k > 0$, so ist damit eine Ringeinbettung von R in $R[X]$ gegeben.

Es ist an dieser Stelle hilfreich, das *Kronecker-Delta*

$$\delta_{i,j} := \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

einzuführen. Wir können dann nämlich die Abbildung $X\colon \mathbb{N} \to R$ mit $X(1) = 1$ und $X(m) = 0$ für $m \neq 1$ kurz schreiben als $X(m) = \delta_{1,m}$. Vereinbaren wir $X^0 := 1 \in R$, so gilt der

Satz 152: *Es ist* $X^n(m) = \delta_{n,m}$.

BEWEIS: Der Induktionsanfang ist schnell gemacht. Die Behauptung gelte nun für ein $n \geq 1$. Dann folgt

$$X^{n+1}(m) = X^n(m) \cdot X(m) = \sum_{k=0}^{m} X^n(k) \cdot X(m-k) = \sum_{k=0}^{m} \delta_{n,k} \cdot \delta_{1,m-k}.$$

Der Summand verschwindet nur dann nicht, wenn sogleich $n = k$ und $1 = m - k$, also $k = m - 1$ ist. Daraus folgt $m = n + 1$, also die Behauptung. □

Wenn wir nun zeigen können, dass sich jede Abbildung $p \in R[X]$ in eindeutiger Weise als Summe über die X^k schreiben lässt, so haben wir die Konstruktion abgeschlossen. Dann ist nämlich das vormals naive Rechnen mit dem Platzhalter X auf das wohlbekannte Rechnen mit Abbildungen zurückgeführt.

Satz 153: *Zu jedem* $0 \neq p \in R[X]$ *existieren eindeutig bestimmte Elemente* $p_1, \ldots, p_n \in R$*, so dass*

$$p = \sum_{k=0}^{n} p_k X^k$$

und $p_n \neq 0$ *ist.*

BEWEIS: Existenz: Wir setzen $p_m := p(m)$ und überprüfen die Gleichheit punktweise. Da p im Polynomring liegt, gibt es eine größte Zahl $n \in \mathbb{N}$, so dass $p(n) \neq 0$ und $p(m) = 0$ für alle $m > n$ ist. Für $m \leq n$ rechnet man

$$\left(\sum_{k=0}^{n} p_k X^k\right)(m) = \sum_{k=0}^{n} p_k X^k(m) = \sum_{k=0}^{n} p_k \delta_{k,m} = p_m = p(m)$$

und für $m > n$

$$\left(\sum_{k=0}^{n} p_k X^k\right)(m) = \sum_{k=0}^{n} p_k X^k(m) = \sum_{k=0}^{n} p_k \delta_{k,m} = 0 = p(m).$$

Eindeutigkeit: Es sei

$$\sum_{k=0}^{n} p_k X^k = \sum_{k=0}^{\widetilde{n}} \widetilde{p}_k X^k$$

mit $\widetilde{p}_{\widetilde{n}} \neq 0$. Wir müssen nun zeigen, dass $n = \widetilde{n}$ und $\widetilde{p}_k = p_k$ für alle k gilt. Dabei können wir o. E. $n \leq \widetilde{n}$ annehmen. Dann ist

$$\sum_{k=0}^{\widetilde{n}} (\widetilde{p}_k - p_k) X^k = 0.$$

Dies gilt wieder punktweise, so dass für $m \leq \widetilde{n}$

$$0 = \left(\sum_{k=0}^{\widetilde{n}} (\widetilde{p}_k - p_k) X^k\right)(m) = \sum_{k=0}^{\widetilde{n}} (\widetilde{p}_k - p_k) X^k(m) = \sum_{k=0}^{\widetilde{n}} (\widetilde{p}_k - p_k)\delta_{k,m} = \widetilde{p}_m - p_m$$

folgt. Insbesondere gilt $n = \widetilde{n}$. □

Index