

Scriptum zur Vorlesung Zählen und Zahlbereiche

Prof. W. Hoffmann
WS 2010/11

1 Grundlagen aus Logik und Mengenlehre

1.1 Aussagen

Die Mathematik fußt auf der Logik. In der klassischen Logik ist jede Aussage entweder wahr oder falsch. Wertungen wie „Da ist etwas Wahres dran“ oder „Das ist nicht die volle Wahrheit“ werden hier nicht zugelassen. Vermutungen, Fragen, Wünsche und Befehle sind nicht Gegenstand der klassischen Logik.

Aus vorhandenen Aussagen kann man neue Aussagen bilden. So macht die *Negation* (d. h. die Verneinung) aus einer wahren Aussage eine falsche und aus einer falschen Aussage eine wahre Aussage. Zum Beispiel ist die Negation der Aussage

„Ich bin ein Berliner“

die Aussage

„Ich bin kein Berliner.“

Manchmal kürzt man Aussagen durch Buchstaben ab sowie die *Wahrheitswerte* „wahr“ und „falsch“ durch die Buchstaben w und f. Die Negation der Aussage A bezeichnet man dann mit $\neg A$ (gelesen „nicht A “). In einer *Wahrheitstafel* stehen in der Kopfzeile Aussagen, jede weitere Zeile stellt eine mögliche Verteilung der Wahrheitswerte dar:

A	$\neg A$
w	f
f	w

Die Reihenfolge der Zeilen ist unerheblich.

Wenn man das Wort „Negation“ als „Gegenteil“ übersetzt, kommt es leicht zu Missverständnissen. Die Negation der Aussage

„Ich habe immer Zeit“

ist nämlich nicht die Aussage

„Ich habe nie Zeit“,

sondern z. B.

„Ich habe nicht immer Zeit.“

Am sichersten ist es, wenn man die Negation durch Voranstellen der Worte „Es ist nicht wahr, dass ...“ bildet.

Die *Konjunktion* von zwei Aussagen bildet man, indem man sie durch das Wort „und“ verknüpft. Die so entstehende Aussage ist wahr, wenn beide Aussagen wahr sind, andernfalls ist sie falsch. In der Umgangssprache wird dies mitunter mit der Formulierung „sowohl als auch“ verdeutlicht. Manchmal werden sich wiederholende Teile beider Aussagen nur einmal genannt:

„Der Beschuldigte hatte ein Motiv und die Gelegenheit für die Tat.“

Die Konjunktion von zwei Aussagen A , B kürzt man durch $A \wedge B$ ab, sie wird durch die folgende Wahrheitstafel beschrieben:

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

Das Wort „oder“ wird in der Umgangssprache in zwei verschiedenen Bedeutungen verwendet, wie die folgenden Beispiele verdeutlichen:

- (1) Wer Banknoten nachmacht oder verfälscht, wird bestraft.
- (2) Geld oder Leben!

Im ersten Beispiel wird man auch bestraft, wenn man beides tut, während im zweiten Beispiel nur eines von beiden genommen werden soll. Seit einiger Zeit versuchen manche, dieser Doppeldeutigkeit durch die Formulierung „und/oder“ zu entgehen. In der Logik versteht man das Wort „oder“ immer im einschließenden Sinne wie in Beispiel (1), andernfalls sagt man „entweder-oder“.

Die Verbindung von zwei Aussagen mit dem Wort „oder“ nennt man *Disjunktion*. Diese ist wahr, wenn wenigstens eine der beide Aussagen wahr ist. Die Disjunktion von zwei Aussagen A , B bezeichnet man auch kurz mit $A \vee B$. Die entsprechende Wahrheitstafel sieht so aus:

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

Manche Aussagen enthalten eine Bedingung, z. B.:

„Wenn Bello eine Wurst bekommt, ist er glücklich.“

„Wenn die Ware mangelhaft ist, dann haftet der Verkäufer.“

In der Logik spielt der zeitliche Aspekt keine Rolle. Man ersetzt darum das Wort „wenn“ oft durch das Wort „falls“ und lässt das Wort „dann“ weg. Verbindet man zwei Aussagen A , B zu der Aussage „wenn A , dann B “, so bildet man die *Implikation*¹, die man durch $A \Rightarrow B$ abkürzt. Sie ist durch folgende Wahrheitstafel gegeben:

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

Man beachte die vorletzte Zeile, die Anfängern Probleme bereitet. Bello kann auch aus einem anderen Grund glücklich sein, aber dadurch wird die obige Aussage nicht falsch. Man hat sich nur zu dem Fall geäußert, dass er eine Wurst bekommt.

Das Pfeilzeichen bedeutet auch nicht, dass A die Ursache von B sein muss oder früher eintreten muss, wie folgendes Beispiel verdeutlicht:

„Wenn du diese Aufgabe lösen kannst, dann bist du ein Genie.“

Die Bedingung kann auch am Ende des Satzes genannt werden:

„Es lohnt sich, wenn man beizeiten spart.“

Es sind noch weitere sprachliche Variationen möglich, z. B.:

„Ist der Mai kühl und nass, füllt’s dem Bauern Scheuer und Fass.“

Der Beispielsatz mit der Mängelhaftung ist meist nicht als Implikation gemeint, und man sollte dann sagen:

¹auch *Subjunktion* genannt

„Wenn die Ware mangelhaft ist, dann – und nur dann – haftet der Verkäufer.“

Anstelle dieser umständlichen Formulierung sagt man auch:

„Der Verkäufer haftet genau dann, wenn die Ware mangelhaft ist.“

Wenn man zwei Aussagen durch die Worte „genau dann, wenn“ verknüpft, bildet man die *Äquivalenz*². Die Aussage „genau dann A , wenn B “ (oder auch „ A ist äquivalent zu B “) wird abgekürzt durch $A \Leftrightarrow B$, und die Wahrheitstafel ist

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

Die Äquivalenz besagt also, dass die verknüpften Aussagen den selben Wahrheitswert haben.

Man kann Aussagen, die durch eine Verknüpfung entstanden sind, wiederum verknüpfen, wie zum Beispiel bei der Bildung von $\neg\neg A$. Diese berechnen wir Schritt für Schritt, indem wir an die Wahrheitstafel weitere Spalten anfügen, die wir nach den obigen Regeln ausfüllen:

A	$\neg A$	$\neg\neg A$
w	f	w
f	w	f

Da die erste und die letzte Spalte übereinstimmen, stellen wir fest: Ganz gleich, welche Aussage mit A gemeint ist, sie ist in jedem Fall äquivalent zur Aussage $\neg\neg A$, das heißt, die Äquivalenz

$$A \Leftrightarrow \neg\neg A$$

ist immer wahr. Wir haben damit ein logisches Gesetz gefunden.

Ein *logisches Gesetz* ist eine Verknüpfung von Variablen, die bei jeder Belegungen der Variablen mit Aussagen zu einer wahren Aussage wird.

Hier ist ein weiteres Beispiel.

²auch *Bisubjunktion* genannt

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
w	w	w	w	w
w	f	f	w	f
f	w	w	f	f
f	f	w	w	w

Durch Vergleich mit der Wahrheitstafel für die Äquivalenz finden wir, dass die Aussage $A \Leftrightarrow B$ zu der Aussage

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

äquivalent ist, ganz gleich, welche Aussagen man für A und B einsetzt. Dieses logische Gesetz motiviert den Gebrauch des Doppelpfeils als Zeichen der Äquivalenz.

Die Klammern waren im letzten Beispiel nötig, um Verwechslungen auszuschließen. Um Klammern zu sparen, legen wir fest:

- \neg bindet stärker als \wedge, \vee ,
- \wedge, \vee binden stärker als $\Rightarrow, \Leftrightarrow$.

Dies ist ähnlich wie bei den Grundrechenarten, wo \cdot und $:$ stärker binden als $+$ und $-$, das heißt wo Punktrechnung vor Strichrechnung geht. Dazu ein Beispiel:

A	B	$\neg A$	$\neg A \vee B$
w	w	f	w
w	f	f	f
f	w	w	w
f	f	w	w

Vergleichen wir dies mit der Wahrheitstafel der Implikation, so finden wir das logische Gesetz

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B).$$

Anstelle von „Nachts ist die Sonne nicht zu sehen“, womit man meint „Wenn es Nacht ist, kann man die Sonne nicht sehen“, kann man also genauso gut sagen „Es ist Tag oder die Sonne ist nicht zu sehen“.

Anhand der bisherigen Wahrheitstabellen kann man auch leicht nachprüfen, dass die Aussage

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

ein logisches Gesetz ist, ebenso wie die *Kommutativgesetze*

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

Weiter gelten die *Assoziativgesetze*

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

und die *Distributivgesetze*

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

Wir führen die Nachprüfung nur am Beispiel des Assoziativgesetzes der Konjunktion vor:

A	B	C	$A \wedge B$	$(A \wedge B) \wedge C$	$B \wedge C$	$A \wedge (B \wedge C)$
w	w	w	w	w	w	w
w	w	f	w	f	f	f
w	f	w	f	f	f	f
w	f	f	f	f	f	f
f	w	w	f	f	w	f
f	w	f	f	f	f	f
f	f	w	f	f	f	f
f	f	f	f	f	f	f

In der Tat stimmen die Einträge der letzten und der drittletzten Spalte zeilenweise überein. Also ist die Aussage $(A \wedge B) \wedge C$ zur Aussage $A \wedge (B \wedge C)$ äquivalent, egal was die Aussagen A , B , C sind, denn in den linken drei Spalten haben wir alle Möglichkeiten für die Wahrheitswerte von A , B , C betrachtet.

Das Satzfragment „Geld oder Leben!“ war eigentlich ein Befehl und somit keine Aussage, kann aber als Aussage umformuliert werden:

„Entweder du gibst mir Dein Geld oder du verlierst dein Leben.“

Die Verknüpfung „entweder A oder B “ ist wahr, wenn A und B verschiedene Wahrheitswerte haben, und falsch, wenn sie gleiche Wahrheitswerte haben. Diese Verknüpfung wird manchmal als *Alternative* oder *Antivalenz* bezeichnet und mit $A \succ\prec B$ oder $A \dot{\vee} B$ abgekürzt. Meist setzt man sie aus anderen Verknüpfungen zusammen, denn sie ist äquivalent zu $\neg(A \Leftrightarrow B)$, zu $\neg A \Leftrightarrow B$ und zu $A \Leftrightarrow \neg B$. Ihre Wahrheitstafel ist

A	B	$A \succ\prec B$
w	w	f
w	f	w
f	w	w
f	f	f

Beispiel. Ein alter Mann bietet auf einem Basar zwei Kästchen an. In einem von beiden steckt ein Schatz. Auf beiden steht etwas geschrieben.

Kästchen 1: „Wenn in diesem Kästchen kein Schatz ist, dann in dem anderen.“

Kästchen 2: „Im diesem Kästchen steckt ein Schatz.“

„Kleiner Tipp“, sagt der Alte, „die Inschriften sind beide falsch oder beide richtig.“ Welches Kästchen sollte man nehmen?

Eine Lösungsmöglichkeit besteht darin, eine Wahrheitstafel für die Aussagen

A: Der Schatz ist im ersten Kästchen,

B: Der Schatz ist im zweiten Kästchen,

aufzustellen. Die gegebenen Informationen lauten:

$$A \not\Rightarrow B, \quad (\neg A \Rightarrow B) \Leftrightarrow B,$$

zu bestimmen. Nur die Zeilen, in denen diese beiden Aussagen wahr sind, kommen in Frage.

Man kann die Lösung abkürzen. Angenommen, der Schatz ist im ersten Kästchen. Dann ist seine Aufschrift wahr, also auch die auf dem zweiten Kästchen.

Manche Sätze enthalten Worte, deren Bedeutung sich erst aus dem Zusammenhang oder der Situation erschließt, wie z. B. bei dem Wort „ich“ in dem Satz „Ich bin ein Berliner“. Man kann sogar den Satz

„*x* ist ein Berliner“

formulieren, der zu einer wahren oder falschen Aussage wird, wenn man für die Variable *x* den Namen eines Menschen einsetzt. In der Logik nennt dies eine *Aussageform* oder ein *Prädikat*.

1.2 Mengen

Der Mathematiker Cantor erklärte den Begriff der Menge so: „Unter einer Menge verstehen wir jede Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche Elemente der Menge genannt werden) zu einem Ganzen.“ Dies ist aber keine Definition im logischen Sinne, die neue Begriffe auf bereits vorher definierte

Begriffe zurückführt. Dazu muss man mit Grundbegriffen beginnen, die nicht zu definieren sind, und „Menge“ ist ein solcher Grundbegriff.

Die Begriffe Menge und Element sind von verschiedener Art. Die Aussage „ M ist eine Menge“ hat einen Sinn, die Aussage „ x ist ein Element“ hingegen nicht. Man kann sagen „ x ist ein Element von M “, abgekürzt $x \in M$, was man auch salopp mit „ x gehört zu M “ ausdrücken kann. Das Wort „Element“ dient also nur zur Formulierung einer Aussageform über die Objekte x und M , die wahr oder falsch wird, wenn man die Bedeutung der Variablen x und M festlegt.

Eine Möglichkeit zur Beschreibung einer Menge besteht darin, ihre Elemente aufzuzählen, die man dazu in geschweifte Klammer setzt. Wir können z. B. die Menge

$$\{\text{Antje, Beate, Carla}\}$$

betrachten. Die Reihenfolge der Elemente ist unerheblich, und Elemente dürfen mehrfach angegeben werden. Die Zweckmäßigkeit dieser Vereinbarung erkennt man an folgendem Beispiel: Sind Zahlen p und q gegeben, wobei $\left(\frac{p}{2}\right)^2 - q \geq 0$ ist, so hat die quadratische Gleichung

$$x^2 + px + q = 0$$

die Lösungsmenge

$$\left\{ -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}, -\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q} \right\},$$

die nur aus einem Element besteht, wenn die sogenannte Diskriminante $\left(\frac{p}{2}\right)^2 - q$ gleich Null ist.

Ein und dieselbe Menge kann auf verschiedene Weise beschrieben werden. So ist z. B. die Menge der Riesenplaneten (von mindestens tausendfacher Erdmasse) gleich der Menge der Gasplaneten. Wenn wir sagen, dass zwei Mengen M und N gleich sind, abgekürzt $M = N$, dann meinen wir, dass für jedes Objekt x die Aussage $x \in M$ äquivalent zur Aussage $x \in N$ ist.

Die leere Menge, die man mit $\{\}$ oder \emptyset bezeichnet, ist dadurch gekennzeichnet, dass die Aussage $x \in \emptyset$ für jedes Objekt x falsch ist.

Wir führen den Begriff der Teilmenge ein, indem wir auf den Begriff der Implikation zurückgreifen.

Definition 1. *Man sagt, dass die Menge N eine Teilmenge der Menge M ist, abgekürzt $N \subseteq M$, wenn für jedes Objekt x gilt: Wenn $x \in N$, dann $x \in M$.*

Diese Definition hat die logische Struktur einer Äquivalenz, müsste also mit den Worten „genau dann, wenn“ formuliert werden. In der Praxis benutzt man in Definitionen aber meist nur das Wort „wenn“.

Nun formulieren wir unseren ersten mathematischen Satz.

Satz 1. (i) Für Mengen M und N gilt genau dann $M \subseteq N$ und $N \subseteq M$, wenn $M = N$.

(ii) Sind L , M und N Mengen derart, dass $L \subseteq M$ und $M \subseteq N$, so gilt $L \subseteq N$.

Beweis. (i) Die Aussage, dass $M \subseteq N$ und $N \subseteq M$ gilt, ist nach Definition gleichbedeutend damit, dass für jedes Objekt x gilt

$$(x \in M \Rightarrow x \in N) \wedge (x \in N \Rightarrow x \in M).$$

Nach einem logischen Gesetz aus dem vorigen Abschnitt ist dies äquivalent zu der Aussage, dass für alle x gilt

$$x \in M \Leftrightarrow x \in N.$$

Letzteres bedeutet nichts anderes, als dass $M = N$ ist.

(ii) Wenn $L \subseteq M$ und $M \subseteq N$, so bedeutet das nach Definition, dass für jedes Objekt x gilt: Wenn $x \in L$, dann $x \in M$, und wenn $x \in M$, dann $x \in N$. Nun gibt es aber ein logisches Gesetz

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

(siehe Aufgabe 2). Wenden wir dies auf die drei Aussagen $x \in L$, $x \in M$, $x \in N$ an, so folgt, dass für alle x gilt: Wenn $x \in L$, dann $x \in N$. Dies ist gleichbedeutend mit der Aussage $L \subseteq N$. \square

Das Ende eines Beweises markiert man traditionell mit den lateinischen Worten *quod erat demonstrandum* (was zu beweisen war, abgekürzt q.e.d.) oder heutzutage meist mit dem Zeichen \square .

Es gibt Mengen, die man nicht durch Aufzählung ihrer Elemente angeben kann, wie z. B. die Menge der Punkte einer Strecke oder einer Kreisscheibe. Statt dessen beschreibt man Mengen durch Angabe einer Bedingung, der ihre Elemente genügen müssen. Eine solche Bedingung ist eine Aussageform, die eine Variable enthält und genau dann wahr ist, wenn man für die Variable ein Element der Menge einsetzt. In die geschweiften Klammern schreibt man zunächst die Variable, dann nach einem senkrechten Strich³ die Bedingung, wie z. B.

$$\{\text{Jupiter, Saturn, Uranus, Neptun}\} = \{x \mid x \text{ ist Riesenplanet}\}$$

³manche Autoren benutzen einen Doppelpunkt

(gelesen: Die Menge aller x mit der Eigenschaft...). Anstelle von x kann jede Variable benutzt werden, die zu diesem Zeitpunkt nicht mit einer anderen Bedeutung belegt ist.

Definition 2. *Unter dem Durchschnitt oder der Schnittmenge von Mengen M und N (abgekürzt $M \cap N$, gelesen „ M geschnitten [mit] N “) verstehen wir die Menge aller Objekte, die zu der Menge M und der Menge N gehören, d. h.*

$$M \cap N = \{x \mid x \in M \wedge x \in N\}.$$

Unter der Vereinigungsmenge oder kurz der Vereinigung von Mengen M und N (abgekürzt $M \cup N$, gelesen „ M vereinigt [mit] N “) verstehen wir die Menge aller Objekte, die zu der Menge M oder der Menge N gehören, d. h.

$$M \cup N = \{x \mid x \in M \vee x \in N\}.$$

Unter der Differenzmenge von Mengen M und N (abgekürzt $M \setminus N$, gelesen „ M ohne N “) verstehen wir die Menge aller Objekte, die zur Menge M , aber⁴ nicht zur Menge N gehören, d. h.

$$M \setminus N = \{x \mid x \in M \wedge x \notin N\}.$$

Hier ist $x \notin N$ eine Abkürzung für $\neg(x \in N)$. Die Ähnlichkeit der Zeichen \wedge und \vee für die logischen Verknüpfungen mit den Zeichen \cap und \cup für die Mengenoperationen ist eine gute Gedankenstütze.

Wieder kann man Sätze beweisen, indem man sie auf logische Gesetze zurückführt. So folgt aus dem logischen Gesetz

$$A \wedge B \Rightarrow A,$$

indem man es auf die Aussagen $x \in M$ und $x \in N$ anwendet, das Gesetz

$$M \cap N \subseteq M.$$

Weitere Gesetze werden unter dem Begriff der Mengenalgebra zusammengefasst:

Satz 2. *Für beliebige Mengen M und N gelten die Kommutativgesetze*

$$M \cap N = N \cap M, \quad M \cup N = N \cup M.$$

Für beliebige Mengen L , M und N gelten die Assoziativgesetze

$$(L \cap M) \cap N = L \cap (M \cap N), \quad (L \cup M) \cup N = L \cup (M \cup N)$$

und die Distributivgesetze

$$L \cap (M \cup N) = (L \cap M) \cup (L \cap N), \quad L \cup (M \cap N) = (L \cup M) \cap (L \cup N)$$

⁴das Wort „aber“ bedeutet hier einfach „und“

Beweis. Wir beweisen hier nur als Beispiel das zweite Distributivgesetz. Die Aussage

$$x \in L \cup (M \cap N)$$

ist laut Definition der Vereinigung gleichbedeutend mit der Aussage

$$(x \in L) \vee (x \in M \cap N).$$

Nach Definition des Durchschnittes ist diese wiederum äquivalent zu

$$(x \in L) \vee (x \in M \wedge x \in N).$$

Hier kommen keine Mengenoperationen, sondern nur noch logische Verknüpfungen vor. Nach einem der logischen Distributivgesetze ist die letzte Aussage äquivalent zu

$$(x \in L \vee x \in M) \wedge (x \in L \vee x \in N).$$

Dies müssen wir schrittweise in die Sprache der Mengenoperationen zurückübersetzen. Nach Definition der Vereinigung ist die vorige Aussage äquivalent zu

$$(x \in L \cup M) \wedge (x \in L \cup N),$$

und nach Definition des Durchschnitts ist Letzteres äquivalent zu

$$x \in (L \cup M) \cap (L \cup N).$$

Die erste und letzte Aussage in unserer Kette von Umformungen sind für alle Objekte x äquivalent, und daraus folgt die Gleichheit der betreffenden Mengen. \square

Um eine weitere Mengenoperation zu motivieren, betrachten wir Daten, die aus zwei Komponenten bestehen. So werden beispielsweise Zeitfenster im wöchentlichen Stundenplan durch einen Wochentag und ein Zeitintervall festgelegt, wie etwa Dienstag 10-12 Uhr. Ein anderes Beispiel sind die Karten im Rommé, die eine Farbe und einen Wert tragen, sagen wir $\spadesuit 10$. Ein weiteres Beispiel sind die Koordinaten eines Punktes in der Zahlenebene, z. B. $(2.3, 7.4)$ in englischer Schreibweise mit Dezimalpunkt. Will man im Deutschen Dezimalkommas verwenden, so muss man die Koordinaten durch Semikola trennen, also $(2,3; 7,4)$. Die beiden Koordinaten können auch gleich sein.

Definition 3. *Eine Folge von zwei Objekten, bei denen die Reihenfolge festgelegt ist, bezeichnet man als geordnetes Paar. Geordnete Paare (a, b) und (c, d) werden genau dann als gleich angesehen, wenn $a = c$ und $b = d$ gilt. Unter der Produktmenge oder dem Kreuzprodukt oder Cartesischen Produkt*

von Mengen M und N (abgekürzt $M \times N$, gelesen M Kreuz N) versteht man die Menge aller geordneten Paare (x, y) , bei denen $x \in M$ und $y \in N$ ist, also

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

Ist z. B.

$$\begin{aligned} M &= \{\text{Mo, Di, Mi, Do, Fr}\}, \\ N &= \{8-10, 10-12, 12-14, 14-16, 16-18\}, \end{aligned}$$

so ist $M \times N$ die Menge der Zeitfenster in der Unterrichtswoche. Ist hingegen

$$\begin{aligned} F &= \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}, \\ W &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \text{B, D, K}\}, \end{aligned}$$

so ist $F \times W$ die Menge der Karten eines Rommé-Spiels ohne Joker (wobei wir das As mit 1 gleichsetzen).

Satz 3. Für beliebige Mengen K , L , M und N gelten die Distributivgesetze

$$\begin{aligned} (K \cap L) \times (M \cap N) &= (K \times M) \cap (L \times N), \\ L \times (M \cup N) &= (L \times M) \cup (L \times N), \quad (K \cup L) \times M = (K \times M) \cup (L \times M). \end{aligned}$$

Beweis. Wir beweisen beispielhaft das erste dieser Gesetze. Ein geordnetes Paar (x, y) gehört genau dann zu $(K \cap L) \times (M \cap N)$, wenn

$$(x \in K \cap L) \wedge (y \in M \cap N).$$

Diese Aussage ist äquivalent zu

$$(x \in K \wedge x \in L) \wedge (y \in M \wedge y \in N).$$

Mit Hilfe des Kommutativgesetzes und des Assoziativgesetzes sehen wir, dass die letzte Aussage äquivalent ist zu

$$(x \in K \wedge y \in M) \wedge (x \in L \wedge y \in N).$$

Aufgrund der Definitionen ist dies wiederum äquivalent zu

$$((x, y) \in K \times M) \wedge ((x, y) \in L \times N)$$

und schließlich zu

$$(x, y) \in (K \times M) \cap (L \times N).$$

Die erste und die letzte Aussage in unserer Kette sind also für alle geordneten Paare (x, y) von Objekten äquivalent, und dies ist gleichbedeutend mit der Behauptung. \square

1.3 Abbildungen

Der Begriff einer Abbildung, auch Zuordnung oder Funktion genannt, ist zentral in der Mathematik und ihren Anwendungen. Hier einige praktische Beispiele:

- (a) Bei einem Multiple-Choice-Test muss man zu jeder Frage eine der Antworten A, B oder C auswählen.
- (b) Jeder Teilnehmer dieser Veranstaltung muss sich in eine Übungsgruppe einschreiben.
- (c) Fällt Sonnenlicht durch ein Fenster auf den Fußboden, so gehört zu jedem Punkt der Fensterscheibe ein Bildpunkt auf dem Fußboden.
- (d) Zu jedem Zeitpunkt zeigt das Tachometer eine bestimmte Geschwindigkeit an.

Folgende Definition ist logisch nicht ganz korrekt,⁵ aber für unsere Zwecke ausreichend.

Definition 4. *Eine Abbildung von einer Menge M in eine Menge N ist dadurch gegeben, dass jedem Element von M genau ein Element von N zugeordnet ist.*

Der Name kommt natürlich vom Beispiel (c). Man nennt M den *Definitionsbereich* und N den *Zielbereich* der Abbildung. Besteht N aus Zahlen wie im Beispiel (d), so nennt man die Abbildung auch eine *Funktion*. Wenn man physikalische Größen mit Variablen bezeichnet, muss man die Werte zu verschiedenen Zeiten unterscheiden. Man kann z. B. die Geschwindigkeit zum Zeitpunkt t mit $v(t)$ bezeichnen. Diese Bezeichnungsweise hat sich in der Mathematik durchgesetzt. Ist f der Name einer Abbildung von M in N , so bezeichnet man das Element von N , das einem Element $x \in M$ zugeordnet ist, mit $f(x)$, gelesen „ f von x “, und nennt es den Wert von f an der Stelle x .

Ein wichtiger Bestandteil der obigen Definition ist das Wort „jedem“. Wenn sich manche Teilnehmer noch nicht in eine Übungsgruppe eingetragen haben, so liegt keine Abbildung der Menge der Teilnehmer in die Menge der Übungsgruppen vor. Aber damit nicht genug.

Nicht minder wichtig ist das Wort „genau ein“. Dieses benutzen wir in der Mathematik, wenn wir das Zahlwort und nicht den unbestimmten Artikel meinen. Wenn sich (wenigstens) ein Teilnehmer in mehrere Gruppen

⁵Sie sagt nicht, was eine Abbildung eigentlich *ist*, sondern führt diesen Begriff nur auf den undefinierten Begriff der Zuordnung zurück.

eingetragen hat, so liegt keine Abbildung vor. Früher ließ man bei der Wurzelfunktion zwei Werte zu, man konnte also sagen: Die Wurzel aus 4 ist 2 oder -2 . Heutzutage verlangt man, dass Abbildungen (und insbesondere Funktionen) eindeutig sind.

Kann man alle Elemente der Menge M aufzählen, so lässt sich eine Abbildung f von M in N (oder, wie man kurz schreibt, eine Abbildung $f : M \rightarrow N$) durch eine *Wertetabelle* angeben. So könnte z. B. die Punktetabelle einer Klausur (die zur Wahrung der Unvoreingenommenheit bei der Korrektur keine Namen enthält) so aussehen:

Matr.-Nr.	Punkte
3017542	8
3053751	12
3108408	8
3135262	17
3274906	19

In der Mathematik ist es allerdings eher üblich, die Elemente des Definitionsbereiches in der oberen Zeile und die Werte jeweils darunter anzugeben, vgl. Aufgabe 8.

Aus der Schule ist der Graph einer Funktion bekannt. Aber auch bei Abbildungen zwischen endlichen Mengen wird die selbe Idee verwendet. Bei einem Multiple-Choice-Test wie in Beispiel (a) erzeugt jeder Teilnehmer eine Abbildung von der Menge F der Fragen in die Menge $\{A,B,C\}$. Auf dem Fragebogen gibt er allerdings keine Wertetabelle an, sondern kreuzt Felder in einer Tabelle an. Die Tabellenfelder entsprechen den Elementen des Kreuzproduktes $F \times \{A,B,C\}$.

Definition 5. *Der Graph einer Abbildung $f : M \rightarrow N$ ist die Menge der geordneten Paare (x, y) aus $M \times N$ mit der Eigenschaft $f(x) = y$.*

Der Graph G einer Funktion $f : M \rightarrow N$ hat folgende Eigenschaft: Für jedes Element x von M gibt es genau ein Element y von N mit der Eigenschaft $(x, y) \in G$. Durch diese Eigenschaft werden Graphen charakterisiert: Ist G irgend eine Teilmenge des Kreuzproduktes $M \times N$ mit dieser Eigenschaft, so ist sie der Graph einer Abbildung von M in N , denn sie bestimmt, welches Element von N einem gegebenen Element von M zuzuordnen ist. Statt mit Abbildungen kann man also mit Graphen arbeiten, deren Definition logisch unproblematisch ist.

In der Praxis werden häufig mehrere Zuordnungen verkettet. Wollen z. B. einige Teilnehmer an der o. g. Klausur ihre Ergebnisse wissen, so muss man ihre Einträge in der Namensliste suchen:

Name	Matr.-Nr.
Gudrun Meier	3135262
Fritz Müller	3017542
Egon Schmidt	3274906

Man kann dann jedem Teilnehmer seine Punktzahl zuordnen:

Name	Punkte
Gudrun Meier	17
Fritz Müller	8
Egon Schmidt	19

Bezeichnet man die Menge der Teilnehmer mit L , die Menge der Matrikelnummern mit M und die Menge der möglichen Punktzahlen mit N , so lässt sich das Vorgehen wie folgt abstrakt beschreiben.

Definition 6. Die Verkettung von Abbildungen $f : M \rightarrow N$ und $g : L \rightarrow M$ ist die Abbildung $h : L \rightarrow N$, die durch die Vorschrift $h(x) = f(g(x))$ gegeben ist.

Will man für die Verkettung von f und g keine neue Variable (wie in unserem Fall h) einführen, so bezeichnet man sie mit $f \circ g$. Angesichts der Schreibweise

$$L \xrightarrow{g} M \xrightarrow{f} N$$

erscheint die Reihenfolge in $f \circ g$ unlogisch, aber sie erklärt sich aus der definierenden Gleichung

$$(f \circ g)(x) = f(g(x)).$$

Ein Beispiel einer Abbildung ist die *identische Abbildung* von einer Menge M in die Menge M selbst, die jedem Element das selbe Element zuordnet. Man bezeichnet sie auch mit id_M , das heißt

$$\text{id}_M(x) = x.$$

Oft kann ein und dieselbe Abbildung auf verschiedene Weisen beschrieben werden. Wir schreiben $f = g$, wenn f und g zwei Namen für die selbe Abbildung sind. Das bedeutet, dass sie den selben Definitionsbereich (sagen wir M) und den selben Zielbereich (sagen wir N) haben und dass für alle Elemente x von M gilt $f(x) = g(x)$.

Satz 4. (i) Für beliebige Abbildungen $f : M \rightarrow N$, $g : L \rightarrow M$ und $h : K \rightarrow L$ gilt

$$(f \circ g) \circ h = f \circ (g \circ h).$$

(ii) Für jede Abbildung $f : M \rightarrow N$ gilt

$$f \circ \text{id}_M = f \quad \text{und} \quad \text{id}_N \circ f = f.$$

Beweis. (i) Für jedes $x \in K$ gilt nach Definition der Verkettung (zweimal angewendet) einerseits

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

und andererseits

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

Die Abbildungen $(f \circ g) \circ h$ und $f \circ (g \circ h)$ bilden also ein beliebiges Element von L auf ein und das selbe Element von N ab. Folglich handelt es sich um die selbe Abbildung.

(ii) Für jedes $x \in M$ gilt nach Definition der Verkettung und der identischen Abbildung

$$(f \circ \text{id}_M)(x) = f(\text{id}_M(x)) = f(x).$$

Da die Abbildungen $f \circ \text{id}_M$ und f bei Anwendung auf ein beliebiges Element den gleichen Wert liefern, stimmen sie überein. Genau so beweist man, dass $\text{id}_N \circ f$ und f übereinstimmen. \square

Wegen Aussage (i) kann man also die Klammern weglassen und einfach $f \circ g \circ h$ schreiben.

In der Definition sind die Rollen von Definitionsbereich und Zielbereich nicht vertauschbar. So ist es erlaubt, dass mehreren Elementen des Definitionsbereiches das selbe Element der Zielbereich zugeordnet wird, und nicht jedes Element des Zielbereiches muss ein Wert der Abbildung sein.

Definition 7. Eine Abbildung $f : M \rightarrow N$ heißt injektiv,⁶ wenn es keine verschiedenen Elemente von M gibt, die auf dasselbe Element von N abgebildet werden.

Man kann die Bedingung auch so formulieren, dass für alle Elemente u und v von M gelten muss:

$$\text{Wenn } u \neq v, \text{ dann } f(u) \neq f(v).$$

Hier ist $u \neq v$ eine Abkürzung für $\neg(u = v)$. Mit Hilfe des logischen Gesetzes von der Kontraposition (erster Teil der Übungsaufgabe 2) kann man die Bedingung noch anders formulieren:

⁶Im Deutschen nennt man solche Abbildungen eineindeutig, aber die französische Bezeichnung hat sich mittlerweile allgemein durchgesetzt. Sie geht auf eine Autorengruppe unter dem Pseudonym **Nicolas Bourbaki** zurück.

Wenn $f(u) = f(v)$, dann $u = v$.

Die Abbildung in Beispiel (c) am Anfang des Abschnittes ist injektiv, die in Beispiel (a) meist nicht.

Definition 8. Eine Abbildung $f : M \rightarrow N$ heißt surjektiv,⁷ wenn es zu jedem Element y von N ein Element x von M gibt, so dass $f(x) = y$.

Man nennt die Menge derjenigen Elemente y von N , zu denen es ein $x \in M$ mit der Eigenschaft $f(x) = y$ gibt, den Wertebereich oder Wertevorrat von f . Man kann also sagen, dass eine Abbildung genau dann surjektiv ist, wenn ihr Wertebereich gleich dem gesamten Zielbereich ist.

Die Abbildung in Beispiel (b) sollte surjektiv sein, die in Beispiel (d) nicht.

Die Eigenschaften der Injektivität und Surjektivität vererben sich bei Verkettungen. Außerdem kann man aus den Eigenschaften der Verkettung mitunter Rückschlüsse auf die beteiligten Abbildungen ziehen:

Satz 5. Es seien $f : M \rightarrow N$ und $g : L \rightarrow M$ Abbildungen. Dann gilt:

- (i) Wenn f und g injektiv sind, dann ist $f \circ g$ injektiv.
- (ii) Wenn $f \circ g$ injektiv ist, dann ist g injektiv.
- (iii) Wenn f und g surjektiv sind, dann ist $f \circ g$ surjektiv.
- (iv) Wenn $f \circ g$ surjektiv ist, dann ist f surjektiv.

Beweis. (i) Sind u und v verschiedene Elemente des Definitionsbereiches der Abbildung $f \circ g$, also⁸ $u, v \in L$ und $u \neq v$, so ist wegen der Injektivität von g dann $g(u) \neq g(v)$, und wegen der Injektivität von f folgt $f(g(u)) \neq f(g(v))$. Die letzte Ungleichung bedeutet laut Definition der Verknüpfung $(f \circ g)(u) \neq (f \circ g)(v)$, was zu beweisen war.

Man kann einen anderen Beweis geben, indem man die Umformulierung der Definition benutzt: Es seien $u, v \in L$. Ist $(f \circ g)(u) = (f \circ g)(v)$, also nach Definition $f(g(u)) = f(g(v))$, so folgt wegen der Injektivität von f , dass $g(u) = g(v)$, und daraus folgt wegen der Injektivität von g , dass $u = v$. Da dies für beliebige u und v gilt, ist $f \circ g$ injektiv.

Der Beweis von (ii) und (iii) ist Inhalt der Übungsaufgabe 9.

⁷Im Deutschen sagt man in diesem Fall, f sei eine Abbildung von M **auf** N , aber dieser feine Unterschied kann der Aufmerksamkeit leicht entgehen, und die französische Bezeichnung hat sich auch hier allgemein durchgesetzt.

⁸Strenggenommen müsste man schreiben: $u \in L$ und $v \in L$.

(iv) Ist $z \in N$, so gibt es wegen der Surjektivität von $f \circ g$ ein $x \in L$, so dass $(f \circ g)(x) = z$. Bezeichnen wir $g(x)$ mit y , so gilt

$$f(y) = f(g(x)) = (f \circ g)(x) = z.$$

Wir haben also zu jedem $z \in N$ ein $y \in M$ gefunden, so dass $f(y) = z$. Somit ist f surjektiv. \square

Aus der Schule ist der Begriff der Umkehrfunktion bekannt. Einen analogen Begriff gibt es für Abbildungen.

Definition 9. Eine Abbildung heißt bijektiv,⁹ wenn sie injektiv und surjektiv ist. Die Abbildung $g : N \rightarrow M$ heißt Umkehrabbildung der Abbildung $f : M \rightarrow N$, wenn für beliebige Elemente $x \in M$ und $y \in N$ die Aussagen $f(x) = y$ und $g(y) = x$ äquivalent sind.

Satz 6. (i) Eine Abbildung besitzt genau dann eine Umkehrabbildung, wenn sie bijektiv ist.

(ii) Eine Abbildung $g : N \rightarrow M$ ist genau dann die Umkehrabbildung einer Abbildung $f : M \rightarrow N$, wenn gilt

$$f \circ g = \text{id}_N, \quad g \circ f = \text{id}_M.$$

Beweis. Beide Aussagen haben die Struktur einer Äquivalenz $A \Leftrightarrow B$. Es genügt darum, jeweils die Implikation $A \Rightarrow B$ und ihre Umkehrung $B \Rightarrow A$ zu beweisen.

(i) Angenommen, f besitzt eine Umkehrabbildung g . Um zu beweisen, dass f injektiv ist, betrachten wir Elemente u und v von M , die von f auf das selbe Element y abgebildet werden, also $f(u) = y$ und $f(v) = y$. Aus der ersten Gleichung folgt $g(y) = u$, aus der zweiten $g(y) = v$, also $u = v$, und die Injektivität von f ist bewiesen. Zum Beweis der Surjektivität von f betrachten wir ein beliebiges Element y von N . Dann gibt es ein Element x von M mit der Eigenschaft $f(x) = y$, nämlich $x = g(y)$. Also ist f surjektiv.

Umgekehrt nehmen wir an, dass f bijektiv ist. Ist ein Element y von N gegeben, so gibt es wegen der Surjektivität ein Element x von M , so dass $f(x) = y$ ist, und wegen der Injektivität von f ist dieses Element eindeutig bestimmt. Wir können also festlegen, dass $g(y) = x$ ist. Die so definierte Abbildung g ist offensichtlich die Umkehrabbildung von f .

(ii) Angenommen, g ist die Umkehrabbildung von f . Ist $x \in M$ und bezeichnen wir das Element $f(x)$ mit y , also $f(x) = y$, so ist nach Definition

⁹Im Deutschen „umkehrbar eindeutig“

der Umkehrabbildung $g(y) = x$, und es folgt $g(f(x)) = g(y) = x$. Wir haben also gezeigt, dass für jedes Element x von M gilt $(g \circ f)(x) = x$, und das bedeutet, dass $g \circ f = \text{id}_M$. Genauso zeigt man, dass $f \circ g = \text{id}_N$.

Umgekehrt nehmen wir an, dass die letzten beiden Gleichungen erfüllt sind. Ist nun $x \in M$ und $y \in N$, so folgt aus der Aussage $f(x) = y$, dass

$$g(y) = g(f(x)) = (g \circ f)(x) = \text{id}_M(x) = x.$$

Genauso folgert man aus $g(y) = x$, dass $f(x) = y$. Die Aussagen $f(x) = y$ und $g(y) = x$ sind also für beliebige $x \in M$ und $y \in N$ äquivalent, und somit ist g die Umkehrabbildung von f . \square

2 Kardinalzahlen

Man unterscheidet zwischen Grundzahlen (eins, zwei, drei, ...) und Ordnungszahlen (erstes, zweites, drittes, ...). Mit Grundzahlen gibt man an, wieviele Elemente eine Menge hat, mit Ordnungszahlen gibt man ihnen eine Reihenfolge. In der Mathematik benutzt man meist die (zur Hälfte) lateinischen Bezeichnungen Kardinalzahlen und Ordinalzahlen. Zunächst beschäftigen wir uns mit den Kardinalzahlen.

2.1 Mächtigkeit von Mengen

Es ist gar nicht einfach, den Begriff „Zahl“ zu definieren. Wollten wir einem Außerirdischen, der unsere Sprache nicht versteht, klarmachen, was wir mit dem Wort „fünf“ meinen, so sollten wir mehrmals auf Mengen von fünf Objekten zeigen und das Wort „fünf“ sagen. Er wird daraus (hoffentlich) schließen, dass wir etwas meinen, das all diese Mengen gemeinsam haben. Dabei wird ihm als erstes auffallen, dass die gezeigten Mengen gleich viele Elemente haben. Diese Eigenschaft ist fundamentaler als der Zahlbegriff. Wenn auf einem gedeckten Tisch auf jeder Untertasse eine Tasse steht, dann weiß man ohne zu zählen, dass sich dort gleich viele Tassen wie Untertassen befinden.

Definition 10. *Wir sagen, dass eine Menge M gleichmächtig zu einer Menge N ist (abgekürzt $M \sim N$), wenn es eine bijektive Abbildung von M auf N gibt.*

Die folgenden Aussagen sind zwar intuitiv klar, aber man muss sie strikt aus der Definition der Gleichmächtigkeit herleiten.

Satz 7. *Die Relation der Gleichmächtigkeit ist eine Äquivalenzrelation, das heißt, für beliebige Mengen L , M und N gilt:*

(i) $M \sim M$. (Reflexivität)

(ii) Genau dann $M \sim N$, wenn $N \sim M$. (Symmetrie)

(iii) Wenn $L \sim M$ und $M \sim N$, dann $L \sim N$. (Transitivität)

Beweis. (i) Die identische Abbildung von M in M ist bijektiv.

(ii) Wenn M gleichmächtig zu N ist, dann gibt es eine bijektive Abbildung $f : M \rightarrow N$, und zu dieser existiert eine Umkehrabbildung $g : N \rightarrow M$,

die bekanntlich ebenfalls bijektiv ist.¹⁰ Also ist N gleichmächtig zu M . Die umgekehrte Implikation beweist man ebenso.

(iii) Ist L gleichmächtig zu M und M gleichmächtig zu N , so gibt es bijektive Abbildungen $g : L \rightarrow M$ und $f : M \rightarrow N$. Ihre Verkettung $f \circ g$ ist eine Abbildung von L in N , und nach Satz 5(i) und (iii) ist sie bijektiv. \square

Man beachte, dass hier die leere Menge zugelassen ist. Von der leeren Menge in eine beliebige andere Menge N gibt es genau eine Abbildung. Ihr Graph ist die einzige Teilmenge des Kreuzproduktes $\emptyset \times N = \emptyset$.

Wir können leicht klären, ob eine Menge genau ein Element hat, ohne die Zahl Eins definiert zu haben. Eine Einermenge kann man definieren als eine Menge, die gleichmächtig zur Menge $\{\text{Erde}\}$ ist. Ebenso kann man festlegen, dass eine Zweiermenge eine solche Menge ist, die gleichmächtig zur Menge $\{\text{Sonne, Mond}\}$ ist.

Wir klassifizieren Mengen nach ihrer Mächtigkeit,¹¹ ähnlich wie man Lebewesen, Steuerpflichtige oder Schüler in Klassen einteilt. So gibt es die Klasse der Einermengen, die Klasse der Zweiermengen usw., aber auch die Klasse, die nur aus der leeren Menge besteht.

Definition 11. Die Mächtigkeitsklasse einer Menge M umfasst all diejenigen Mengen, die gleichmächtig zu M sind.

Nach der obigen Festlegung ist die Mächtigkeitsklasse der Menge $\{\text{Erde}\}$ gerade die Klasse der Einermengen. Statt Mächtigkeitsklasse sagen wir oft kurz Klasse, was wohl niemand mit Steuerklasse oder sozialer Klasse verwechseln wird. Ein Element einer Klasse nennt man auch einen Vertreter oder *Repräsentanten* der Klasse.

Satz 8. Jede Menge gehört zu genau einer Klasse.

Beweis. Wegen der Reflexivität gehört jede Menge zu mindestens einer Klasse, nämlich ihrer eigenen. Angenommen, die Menge M gehört außerdem zur Klasse der Menge N , d.h. $M \sim N$. Wir müssen zeigen, dass diese beiden Klassen übereinstimmen.

Ist L in der Klasse von M , d.h. $L \sim M$, so ist wegen der Transitivität auch $L \sim N$. Somit ist die Klasse von M in der von N enthalten. Wegen der Symmetrie gilt aber auch $N \sim M$, und wir sehen auf die gleiche Weise, dass die Klasse von N in der Klasse von M enthalten ist. \square

¹⁰Da id_N injektiv ist, folgt wegen Satz 4(ii) und Satz 5(ii), dass g injektiv ist, und da id_M surjektiv ist, folgt wegen Satz 4(ii) und Satz 5(iv), dass g surjektiv ist. Somit ist g bijektiv.

¹¹Dieser Begriff ist offenbar durch die Mächtigkeit von Gesteinsschichten motiviert.

Wir sehen, dass man ein und die selbe Klasse auf verschiedene Weise beschreiben kann. So ist die Klasse der Zweiermengen auch beschreibbar als die Klasse der Menge $\{a, b\}$, wobei wir a und b hier als Objekte und nicht als Variablen betrachten.

Nun wollen wir den Begriff einer Kardinalzahl definieren, so dass man jeder Menge eine Kardinalzahl zuordnen kann, die angibt, wieviele Elemente sie enthält. Dann brauchen wir natürlich für jede Klasse eine Kardinalzahl. Anstatt Kardinalzahlen als neue Objekte zu erschaffen, gehen wir hier den einfachen Weg, sie mit den Klassen gleichzusetzen.¹²

Definition 12. *Eine Kardinalzahl ist eine Mächtigkeitsklasse von Mengen. Insbesondere ist Null (abgekürzt 0) die Klasse, die nur die leere Menge enthält, Eins (abgekürzt 1) die Klasse der Einermengen, Zwei (abgekürzt 2) ist die Klasse der Zweiermengen usw.*

Man kann für ein und die selbe Kardinalzahl verschiedene Bezeichnungen vereinbaren, z. B.

$$\#\, \boxtimes, \text{fünf}, 5, \bar{V}, \circ$$

für die Klasse der Menge $\{\text{Wasser, Feuer, Erde, Holz, Metall}\}$.

Definition 13. *Die Mächtigkeit einer Menge M , abgekürzt $|M|$, ist die Mächtigkeitsklasse von M .*

Da wir unendliche Mengen bisher nicht ausgeschlossen haben, sprechen wir nicht von der Anzahl, sondern der Mächtigkeit. So ist zum Beispiel

$$\begin{aligned} |\emptyset| &= 0, \\ |\{\text{Erde}\}| &= 1, \\ |\{\text{Sonne, Mond}\}| &= 2, \\ |\{\text{Caesar, Pompeius, Crassus}\}| &= 3, \\ |\{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}| &= 4, \\ |\{\text{Wasser, Feuer, Erde, Holz, Metall}\}| &= 5, \dots \end{aligned}$$

Nun hat der Satz „In der taoistischen Tradition gibt es *fünf* Elemente“ einen mathematischen Sinn.

¹²Das ist nicht ganz befriedigend (weil man dann nicht von der *Menge* der Kardinalzahlen sprechen kann), aber für diese erste Einführung ausreichend.

2.2 Operationen mit Kardinalzahlen

Wir kommen jetzt zu den Rechenoperationen. Die Addition lässt sich mit Hilfe der Vereinigung von Mengen einführen. Dabei ist gewisse Vorsicht geboten. Obwohl die Mengen

$$\{a, b, c\}, \quad \{b, d\}$$

drei bzw. zwei Elemente haben, hat die Vereinigungsmenge

$$\{a, b, c, d\}$$

nur vier Elemente, was wir nicht als Summe von 3 und 2 definieren wollen. Wir dürfen bei der Definition der Addition nur Mengen betrachten, die kein gemeinsames Element besitzen. Zwei solche Mengen heißen *elementfremd* oder *disjunkt*.¹³ Offensichtlich ist die Menge M genau dann disjunkt zur Menge N , wenn $M \cap N = \emptyset$.

Ein weiteres Problem besteht darin, dass die selbe Kardinalzahl durch verschiedene Mengen dargestellt werden kann. Man muss gewissermaßen sicherstellen, dass beim Rechnen mit Stäbchen das selbe Ergebnis herauskommt wie beim Rechnen mit Fingern.

Satz 9. *Sind K, L, M und N Mengen mit der Eigenschaft*

$$K \sim M \quad \text{und} \quad L \sim N$$

und ist K disjunkt zu L und ist M disjunkt zu N , so gilt

$$K \cup L \sim M \cup N.$$

Beweis. Die Gleichmächtigkeit von K und M bedeutet, dass es eine bijektive Abbildung $f : K \rightarrow M$ gibt, und wegen der Gleichmächtigkeit von L und N gibt es eine bijektive Abbildung $g : L \rightarrow N$. Wir definieren nun eine Abbildung

$$h : K \cup L \rightarrow M \cup N$$

wie folgt: Ist $x \in K$, so setzen wir $h(x) = f(x)$, ist hingegen $x \in L$, so setzen wir $h(x) = g(x)$. Da K und L nach Voraussetzung keine gemeinsamen Elemente haben, geraten diese beiden Vorschriften nicht in Konflikt. Wenn wir zeigen können, dass h bijektiv ist, dann ist der Beweis abgeschlossen.

Zum Beweis der Injektivität betrachten wir Elemente $u \neq v$ in $K \cup L$. Liegen beide in K , so ist $h(u) = f(u)$ und $h(v) = f(v)$, aber diese Bilder

¹³Die Verwendung des lateinischen Wortes *disjunkt* (deutsch: getrennt) hat nichts mit der logischen Disjunktion zu tun.

sind wegen der Injektivität von f verschieden. Analog behandelt man den Fall, dass u und v beide in L liegen. Ist aber $u \in K$ und $v \in L$, so gilt $h(u) = f(u) \in M$ und $h(v) = g(v) \in N$, und da M und N disjunkt sind, folgt auch in diesem Fall $h(u) \neq h(v)$. Genauso behandelt man den Fall, dass $u \in L$ und $v \in K$. Wir sehen also, dass h injektiv ist.

Zum Beweis der Surjektivität betrachten wir ein beliebiges Element y von $M \cup N$. Dann ist $y \in M$ oder $y \in N$. Im ersten Fall gibt es wegen der Surjektivität von f ein $x \in K$, so dass $f(x) = y$, während es im zweiten Fall wegen der Surjektivität von g ein $x \in L$ gibt, so dass $g(x) = y$. In beiden Fällen folgt $h(x) = y$, also ist die Abbildung h surjektiv. \square

Definition 14. Sind m und n Kardinalzahlen, so definieren wir ihre Summe, abgekürzt $m + n$, als die Mächtigkeit von $M \cup N$, wobei M und N solche disjunkten Mengen sind, dass $|M| = m$ und $|N| = n$.

Diese Definition erfordert eine Erläuterung. Erstens muss man sicherstellen, dass man zu vorgegebenen Kardinalzahlen disjunkte Repräsentanten M und N finden kann. Das ist intuitiv klar und kann auch streng begründet werden.¹⁴ Zweitens muss man sich überzeugen, dass man bei anderer Wahl der Repräsentanten dieselbe Kardinalzahl als Summe erhält. Das ist aber gerade der Inhalt von Satz 9.

Die Definition der Addition schließt den Fall ein, dass einer der Summanden gleich Null ist. Wegen $M \cup \emptyset = M$ gilt

$$m + 0 = m \tag{1}$$

für alle Kardinalzahlen m .

Nun kommen wir zu den Rechengesetzen der Addition.

Satz 10. Für alle Kardinalzahlen m und n gilt das Kommutativgesetz

$$m + n = n + m,$$

und für alle Kardinalzahlen l , m und n gilt das Assoziativgesetz

$$(l + m) + n = l + (m + n).$$

Beweis. Für die erste Behauptung wählen wir disjunkte Repräsentanten M und N der Kardinalzahlen m und n , d. h. $|M| = m$, $|N| = n$ und $M \cap N = \emptyset$. Nach Satz 2 gilt das Kommutativitätsgesetz der Vereinigung

$$M \cup N = N \cup M.$$

¹⁴Hat man zunächst irgendwelche Repräsentanten M und N , so kann man sie durch die disjunkten Repräsentanten $M \times \{a\}$ und $N \times \{b\}$ ersetzen.

Hier haben wir also zwei Beschreibungen der selben Menge, und für ihre Mächtigkeit gilt

$$|M \cup N| = |N \cup M|.$$

Mit der Definition der Addition folgt die erste Behauptung.

Zum Beweis der zweiten wählen wir Repräsentanten L , M und N für die gegebenen Kardinalzahlen l , m und n . Es genügt nicht, dass $L \cap M \cap N = \emptyset$ ist, sondern wir müssen sie so wählen, dass L disjunkt zu M , L disjunkt zu N und M disjunkt zu N ist. Man sagt dann, die Mengen seien paarweise disjunkt.

Nach Satz 2 gilt das Assoziativgesetz der Vereinigung

$$(L \cup M) \cup N = L \cup (M \cup N).$$

Aus der paarweisen Disjunktheit folgt auch, dass $L \cup M$ disjunkt zu N und dass L disjunkt zu $M \cup N$ ist. Also gilt nach der Definition der Addition

$$|L \cup M| + |N| = |L| + |M \cup N|.$$

Eine weitere Anwendung der Definition liefert

$$(|L| + |M|) + |N| = |L| + (|M| + |N|).$$

Wegen $|L| = l$, $|M| = m$ und $|N| = n$ ist das genau unsere Behauptung. \square

Als Nächstes wenden wir uns der Multiplikation zu. Um z. B. $3 \cdot 2$ zu berechnen, würde man zunächst daran denken, drei disjunkte Zweiermengen zu vereinigen, z. B. die Mengen $\{a, b\}$, $\{c, d\}$ und $\{e, f\}$. Wie aber drückt man aus, dass es sich um drei Mengen handelt? Die Kardinalzahl 3 haben wir über Dreiermengen definiert, und mit etwas Nachdenken findet man, dass hier die Dreiermenge

$$\{\{a, b\}, \{c, d\}, \{e, f\}\}$$

im Spiel ist. In der Tat könnte man das Produkt von Kardinalzahlen m und n so definieren, dass man eine Menge der Mächtigkeit m wählt, deren Elemente ihrerseits Mengen der Mächtigkeit n sind, und all diese Elemente vereinigt. Dann wäre der Beweis der Rechengesetze aber sehr mühsam.

Geschickter ist es, die zu zählenden Objekte in einem rechteckigen Schema anzuordnen:

$$\begin{array}{cc} a & b \\ c & d \\ e & f \end{array}$$

Sie füllen dann die Felder einer Tabelle, und diese Felder entsprechen genau den Elementen eines Kreuzproduktes. Das bringt uns auf die Idee, das Produkt von Kardinalzahlen mit Hilfe des Kreuzproduktes ihrer Repräsentanten

zu definieren. Genau wie bei der Addition muss man sicherstellen, dass das Ergebnis nicht von der Wahl der Repräsentanten abhängt.

Satz 11. *Sind K, L, M und N Mengen mit der Eigenschaft*

$$K \sim M \quad \text{und} \quad L \sim N,$$

so gilt

$$K \times L \sim M \times N.$$

Der Beweis dieses Satzes ist dem von Satz 9 ähnlich (sogar einfacher, da die Disjunktheit keine Rolle spielt) und ist als Übungsaufgabe 14 zu bearbeiten. Er rechtfertigt folgende Definition.

Definition 15. *Sind m und n Kardinalzahlen, so definieren wir ihr Produkt, abgekürzt $m \cdot n$, als die Mächtigkeit von $M \times N$, wobei M und N solche Mengen sind, dass $|M| = m$ und $|N| = n$.*

Man beachte, dass für jede Menge M gilt $M \times \emptyset = \emptyset$. Also folgt für alle Kardinalzahlen m , dass

$$m \cdot 0 = 0.$$

Außerdem gibt es eine bijektive Abbildung $f : M \rightarrow M \times \{a\}$, nämlich $f(x) = (x, a)$ (vgl. auch Aufgabe 12b). Folglich gilt für alle Kardinalzahlen m , dass

$$m \cdot 1 = m.$$

Zur Herleitung der Rechengesetze der Multiplikation beweisen wir zunächst ähnliche Gesetze für das Kreuzprodukt:

Satz 12. *Für beliebige Mengen M und N gilt*

$$M \times N \sim N \times M,$$

und für beliebige Mengen L, M und N gilt

$$(L \times M) \times N \sim L \times (M \times N).$$

Beweis. Wir definieren eine Abbildung

$$f : M \times N \rightarrow N \times M,$$

indem wir festlegen

$$f((x, y)) = (y, x).$$

Diese Abbildung ist bijektiv (z. B. weil man leicht eine Umkehrabbildung angeben kann), und die erste Behauptung folgt.

Wir definieren eine Abbildung

$$g : (L \times M) \times N \rightarrow L \times (M \times N)$$

durch die Festlegung

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

Auch diese Abbildung ist offensichtlich bijektiv, woraus die zweite Behauptung folgt. \square

Oft unterscheidet man nicht zwischen den verschachtelten geordneten Paaren $((x, y), z)$ und $(x, (y, z))$ und schreibt sie als sogenannte Tripel

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

So bilden z. B. die Koordinaten eines Punktes bezüglich eines Koordinatensystems im Raum ein Tripel. Zwei Tripel (r, s, t) und (x, y, z) sind genau dann gleich, wenn $r = x$, $s = y$ und $t = z$.

Aus Satz 12 ergeben sich die vertrauten Rechengesetze der Multiplikation:

Satz 13. *Für beliebige Kardinalzahlen m und n gilt das Kommutativgesetz*

$$m \cdot n = n \cdot m,$$

und für beliebige Kardinalzahlen l , m und n gilt das Assoziativgesetz

$$(l \cdot m) \cdot n = l \cdot (m \cdot n)$$

sowie das Distributivgesetz

$$l \cdot (m + n) = l \cdot m + l \cdot n.$$

Beweis. Zum Beweis des Kommutativgesetzes wählen wir Repräsentanten M und N der Kardinalzahlen m und n . Nach Satz 12 ist

$$|M \times N| = |N \times M|,$$

und mit der Definition der Multiplikation folgt hieraus das Kommutativgesetz.

Zum Beweis des Assoziativgesetzes wählen wir Repräsentanten L , M und N von l , m und n . Aus Satz 12 folgt

$$|(L \times M) \times N| = |L \times (M \times N)|.$$

Mit der Definition der Multiplikation ergibt sich

$$|L \times M| \cdot |N| = |L| \cdot |M \times N|$$

und, durch nochmalige Anwendung,

$$(|L| \cdot |M|) \cdot |N| = |L| \cdot (|M| \cdot |N|).$$

Damit ist das Assoziativgesetz bewiesen. Der Beweis des Distributivgesetzes ist Gegenstand einer Übungsaufgabe. \square

Es gibt eine weitere Operation mit Kardinalzahlen, nämlich das Potenzieren. Auch diese lässt sich mit Hilfe einer Mengenoperation einführen.

Definition 16. Die Menge aller Abbildungen von einer Menge M in eine Menge N bezeichnen wir mit N^M .

Ähnlich wie bei den früheren Mengenoperationen müssen wir nachprüfen, dass sich die Mächtigkeit der Potenz nicht ändert, wenn wir M und N durch gleichmächtige Mengen ersetzen.

Satz 14. Sind K, L, M und N Mengen mit der Eigenschaft

$$K \sim M \quad \text{und} \quad L \sim N,$$

so gilt

$$L^K \sim N^M.$$

Beweis. Die Voraussetzungen besagen, dass es bijektive Abbildungen

$$p : M \rightarrow K \quad \text{und} \quad q : L \rightarrow N$$

gibt. Mit Ihrer Hilfe können wir jeder Abbildung $f : K \rightarrow L$ eine Abbildung $M \rightarrow N$ zuordnen, nämlich $q \circ f \circ p$. (Aufgrund von Satz 4 ist eine Klammersetzung hier überflüssig.) Mit Hilfe der Umkehrabbildungen

$$r : K \rightarrow M \quad \text{und} \quad s : N \rightarrow L$$

von p und q können wir aber auch jeder Abbildung $g : M \rightarrow N$ eine Abbildung $K \rightarrow L$ zuordnen, nämlich $s \circ g \circ r$.

Kommt g wie oben beschrieben von einer Abbildung $f : K \rightarrow L$, also $g = q \circ f \circ p$, so folgt wegen $p \circ r = \text{id}_K$ und $s \circ q = \text{id}_L$, dass

$$s \circ g \circ r = s \circ q \circ f \circ p \circ r = \text{id}_L \circ f \circ \text{id}_K = f,$$

wobei wir Satz 4 angewendet haben. Wir erhalten also die Abbildung f zurück.

Ordnet man hingegen einer Abbildung $g : M \rightarrow N$ erst auf die oben beschriebene Weise eine Abbildung $f : K \rightarrow L$ und dieser wiederum eine Abbildung $M \rightarrow N$ zu, so erhält man die Abbildung g zurück, wie man auf ähnliche Weise nachprüfen kann.

Die oben konstruierten Abbildungen zwischen L^K und N^M sind also die Umkehrabbildungen voneinander, und nach Satz 4 sind sie bijektiv. \square

Der Satz rechtfertigt folgende Definition.

Definition 17. Sind m und n Kardinalzahlen, so definieren wir die Potenz n^m als die Mächtigkeit der Menge N^M , wobei M und N Mengen mit $|M| = m$ und $|N| = n$ sind.

Satz 15. Für beliebige Kardinalzahlen l , m und n gelten die Potenzgesetze

$$(m \cdot n)^l = m^l \cdot n^l, \quad n^{l+m} = n^l \cdot n^m, \quad n^{l \cdot m} = (n^l)^m.$$

Beweis. Wir wählen Repräsentanten L , M und N für die Kardinalzahlen l , m und n . Laut einer Übungsaufgabe gilt

$$(M \times N)^L \sim M^L \times N^L,$$

also

$$|(M \times N)^L| = |M^L \times N^L|.$$

Wir können die linke Seite mit Hilfe der Definition der Potenz und die rechte Seite mit Hilfe der Definition des Produktes umschreiben:

$$|M \times N|^{|L|} = |M^L| \cdot |N^L|.$$

Nun schreiben wir die linke Seite mit Hilfe der Definition des Produktes und die rechte Seite mit Hilfe der Definition der Potenz um:

$$(|M| \cdot |N|)^{|L|} = |M|^{|L|} \cdot |N|^{|L|}.$$

Dies ist das erste Potenzgesetz.

Zum Beweis des zweiten Potenzgesetzes wählen wir die Repräsentanten so, dass L und M disjunkt sind, und definieren eine Abbildung

$$N^{L \cup M} \rightarrow N^L \times N^M,$$

das heißt, wir ordnen jeder Abbildung $f : L \cup M \rightarrow N$ ein geordnetes Paar (g, h) von Abbildungen $g : L \rightarrow N$ und $h : M \rightarrow N$ zu. Wir setzen nämlich $g(x) = f(x)$ für alle $x \in L$, und wir setzen $h(x) = f(x)$ für alle $x \in M$. (Man nennt übrigens g die Einschränkung von f auf L und h die Einschränkung von f auf M .) Umgekehrt definieren wir eine Abbildung

$$N^L \times N^M \rightarrow N^{L \cup M},$$

das heißt, wir ordnen jedem Paar (g, h) von Abbildungen $g : L \rightarrow N$ und $h : M \rightarrow N$ eine Abbildung $f : L \cup M \rightarrow N$ zu. Dazu setzen wir $f(x) = g(x)$, falls $x \in L$, und wir setzen $f(x) = h(x)$, falls $x \in M$ ist. Wegen der Disjunktheit von L und M kommen diese beiden Vorschriften nicht in Konflikt.

Es ist klar, dass die eben konstruierten Abbildungen zwischen $N^{L \cup M}$ und $N^L \times N^M$ die Umkehrabbildungen voneinander sind, sie sind also nach Satz 4 bijektiv. Damit haben wir bewiesen, dass

$$N^{L \cup M} \sim N^L \times N^M.$$

Nehmen wir von beiden Seiten der Gleichung die Mächtigkeit und wenden wir wie im ersten Teil des Beweises die Definitionen der Potenz, des Produktes und der Summe an, so erhalten wir das zweite Potenzgesetz.

Der Beweis des dritten Potenzgesetzes ist Inhalt einer Übungsaufgabe. \square

Es sei m eine beliebige Kardinalzahl. Wählen wir einen Repräsentanten M , so gibt es genau eine Abbildung $\emptyset \rightarrow M$, also gilt

$$m^0 = 1.$$

Ist M nicht leer, so gibt es keine Abbildung $M \rightarrow \emptyset$, also gilt

$$m \neq 0 \quad \Rightarrow \quad 0^m = 0.$$

Es gibt genau eine Abbildung $M \rightarrow \{a\}$, also gilt

$$1^m = 1.$$

Jedem Element x von M können wir eine Abbildung $f : \{a\} \rightarrow M$ zuordnen, indem wir $f(a) = x$ festlegen. Auf diese Weise erhalten wir eine bijektive Abbildung $M \rightarrow M^{\{a\}}$, und es folgt

$$m^1 = m.$$

Mit Hilfe der Potenzgesetze finden wir auch, dass

$$\begin{aligned} m^2 &= m^{1+1} = m^1 \cdot m^1 = m \cdot m, \\ m^3 &= m^{2+1} = m^2 \cdot m^1 = m \cdot m \cdot m \end{aligned}$$

und so weiter.

Wir haben gesehen, dass die Rechengesetze für das Produkt von Kardinalzahlen sehr einfach aus den Gesetzen für das Kreuzprodukt folgen. Die auf S. 25 angedeutete alternative Einführung des Produktes als mehrfache Vereinigung hätte uns die Arbeit sehr erschwert. Trotzdem ist sie für Anwendungen wichtig und wird auch als Zugang in der Schule gewählt. Um sie korrekt zu machen, benötigen wir einen allgemeineren Begriff der Vereinigung.

Definition 18. *Es sei \mathcal{M} eine Menge von Mengen. Die Vereinigung der Elemente von \mathcal{M} ist die Menge aller Objekte x , für die es eine Menge $X \in \mathcal{M}$ gibt, so dass $x \in X$. Ist \mathcal{M} nicht leer, so ist der Durchschnitt der Elemente von \mathcal{M} ist die Menge aller Objekte x derart, dass für jede Menge $X \in \mathcal{M}$ gilt $x \in X$.*

So ist z. B. die Vereinigung der Elemente von

$$\mathcal{M} = \{ \{a, d, u\}, \{d, h\}, \{b, d, s\} \}$$

gleich der Menge $\{a, b, d, h, s, u\}$, und der Durchschnitt der Elemente von \mathcal{M} ist $\{d\}$.

Satz 16. *Es sei \mathcal{M} eine Menge von paarweise disjunkten Mengen, und für jede Menge $X \in \mathcal{M}$ gelte $|X| = n$. Wir bezeichnen die Vereinigung der Elemente von \mathcal{M} mit P . Ist $|\mathcal{M}| = m$, so gilt $|P| = m \cdot n$.*

Beweis. Wir wählen einen Repräsentanten N für die Kardinalzahl n . Für jede Menge $X \in \mathcal{M}$ können wir nach Voraussetzung eine bijektive Abbildung $f : N \rightarrow X$ wählen. Um die Abhängigkeit der Abbildung f von der Menge X auszudrücken, schreiben wir $f(n) = g(X, n)$. (Wir sind wie im Beweis von Satz 15 von $(P^N)^{\mathcal{M}}$ zu $P^{\mathcal{M} \times N}$ übergegangen.) Es genügt zu zeigen, dass $g : \mathcal{M} \times N \rightarrow P$ bijektiv ist.

Gilt $g(X, n) = g(X', n')$, so ist die linke wie auch die rechte Seite der Gleichung ein gemeinsames Element von X und X' , und wegen der paarweisen Disjunktheit folgt $X = X'$. Aus der Injektivität der für X gewählten Abbildung f folgt nun $n = n'$. Somit ist g injektiv.

Ist $y \in P$, so gibt es nach Definition der Vereinigung ein $X \in \mathcal{M}$, so dass $y \in X$, und wegen der Surjektivität der zu X gehörigen Abbildung f gibt es ein $n \in N$, so dass $f(n) = y$, das heißt $g(X, n) = y$. Somit ist g surjektiv. \square

2.3 Vergleich von Kardinalzahlen

Zunächst einige Vorbemerkungen. Wir erinnern uns daran, dass man eine Menge durch eine Eigenschaft definieren kann, die ihre Elemente charakterisiert, wie z. B.

$$\{x \mid x \text{ ist ehrlich}\}.$$

Mitunter ist eine Aussageform, die eine Variable x enthält, nicht für alle Objekte definiert, die man an Stelle von x einsetzen könnte. So ist z. B. unklar, ob die Aussageform „ x ist ehrlich“ beim Ersetzen von x durch einen Apfel zu einer wahren oder falschen Aussage wird. Oft ist eine Aussageform nur für die Elemente einer gewissen Menge definiert, wie im gegebenen Fall für die Menge M der Menschen. Diejenigen Elemente von M , die ehrlich sind, bilden dann eine Teilmenge, die wir so bezeichnen:

$$\{x \in M \mid x \text{ ist ehrlich}\}$$

(gelesen: Menge aller x in M mit der Eigenschaft „ x ist ehrlich“).

Nun wenden wir uns dem eigentlichen Thema zu. Bisher haben wir nur definiert, was es heißt, dass zwei Mengen gleichmächtig sind. Sind sie es nicht, so fragt man sich, welche von beiden mehr Elemente enthält. Bisher haben wir aber nicht definiert, was es heißt, dass eine Kardinalzahl größer als eine andere ist.

Definition 19. *Wir sagen, dass eine Menge N mächtiger oder gleichmächtig zur Menge M ist, wenn es eine injektive Abbildung von M in N gibt.*

Man kann das selbe im Wesentlichen auch über den Begriff der Surjektivität ausdrücken.

Satz 17. *Gibt es eine surjektive Abbildung von $g : N \rightarrow M$, so gibt es eine injektive Abbildung von $f : M \rightarrow N$, die außerdem die Eigenschaft $g \circ f = \text{id}_M$ hat. Ist M nicht leer, so gilt auch die Umkehrung.*

Beweis. Angenommen, eine surjektive Abbildung $g : N \rightarrow M$ ist gegeben. Dann müssen wir für jedes $x \in M$ einen Wert $f(x)$ aus der Menge

$$\{y \in N \mid g(y) = x\}$$

wählen. Wegen der Surjektivität von g sind diese Mengen nicht leer, man kann also für jedes x einzeln einen Wert $f(x)$ wählen. Dass dies aber gleichzeitig für alle x möglich ist, kann nicht aus den offensichtlichen Mengenaxiomen hergeleitet werden, sondern muss als zusätzliches Axiom (das sogenannte Auswahlaxiom) vorausgesetzt werden. Wir haben es bereits im Beweis von Satz 16 benutzt.

Die Umkehrung ist Gegenstand der Übungsaufgabe 19. Ist M leer und N nicht, so gibt es natürlich keine Abbildung von N in M . \square

Um zu einer Aussage über Kardinalzahlen zu kommen, müssen wir zeigen, dass sich nichts ändert, wenn wir die vorkommenden Mengen durch gleichmächtige Mengen ersetzen.

Satz 18. *Gilt für die Mengen K, L, M und N , dass*

$$K \sim M, \quad \text{und} \quad L \sim N,$$

so ist N genau dann mächtiger oder gleichmächtig zu M , wenn L mächtiger oder gleichmächtig zu K ist.

Beweis. Aufgrund unserer Voraussetzungen gibt es bijektive Abbildungen

$$p : K \rightarrow M, \quad q : N \rightarrow L.$$

Ist N mächtiger oder gleichmächtig zu M , so gibt es eine injektive Abbildung $f : M \rightarrow N$. Die Abbildung $q \circ f \circ p : K \rightarrow L$ ist dann nach Satz 5 ebenfalls injektiv, also ist L mächtiger oder gleichmächtig zu K . Die Umkehrung beweist man analog mit Hilfe der Umkehrabbildungen von p und q . \square

Damit ist die folgende Definition gerechtfertigt.

Definition 20. *Wir sagen, dass die Kardinalzahl m kleiner oder gleich der Kardinalzahl n ist (abgekürzt $m \leq n$), wenn eine Menge N der Mächtigkeit n mächtiger oder gleichmächtig zu einer Menge M der Mächtigkeit m ist.*

Man kann „ $m \leq n$ “ als Aussageform betrachten, die zwei Variablen m und n enthält, an deren Stelle man Kardinalzahlen einsetzen kann. Eine Aussageform mit zwei Variablen nennt man auch *Relation*. So gibt es z. B. die Enthaltenseinsrelation \subseteq sowie die Relation \sim der Gleichmächtigkeit für Mengen. Bei \leq spricht man von der Kleiner-Gleich-Relation für Kardinalzahlen. Folgende Eigenschaften ergeben sich sofort aus früheren Betrachtungen.

Folgerung 1. (i) Für beliebige Kardinalzahlen m gilt $m \leq m$. (Reflexivität)

(ii) Für beliebige Kardinalzahlen l , m und n gilt: Wenn $l \leq m$ und $m \leq n$, dann ist $l \leq n$. (Transitivität)

Aussage (i) ist klar, weil es für einen beliebigen Repräsentanten M von m die identische Abbildung id_M gibt. Aussage (ii) folgt leicht aus Satz 5(i). *Beispiel.* Wir können jetzt leicht nachprüfen, dass z. B. $3 \leq 4$ gilt. Dazu wählen wir Repräsentanten, sagen wir $M = \{\text{Caesar}, \text{Pompeius}, \text{Crassus}\}$ und $N = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$, und definieren eine injektive Abbildung $f : M \rightarrow N$ etwa durch folgende Wertetabelle:

x	Caesar	Pompeius	Crassus
$f(x)$	♠	♣	◇

Die Aussage $4 \leq 3$ ist hingegen falsch. Um das zu beweisen, müssen wir zeigen, dass es keine injektive Abbildung $N \rightarrow M$ gibt. Im Wesentlichen muss man dazu alle möglichen Abbildungen durchprobieren. Wir werden später eine einfachere Begründung kennenlernen.

Definition 21. Wir sagen, dass eine Kardinalzahl m kleiner als eine Kardinalzahl n ist (abgekürzt $m < n$), wenn $m \leq n$, aber $m \neq n$ ist.

Es gibt eine analoge Relation zwischen Mengen:

Definition 22. Eine Menge L heißt echte Teilmenge der Menge M (abgekürzt $L \subset M$), wenn L eine Teilmenge von M , aber nicht die Menge M selbst ist.

Auf den ersten Blick könnte man meinen, dass für eine echte Teilmenge L von M auch $|L| < |M|$ gelten müsste, aber das ist falsch! Es kann vorkommen, dass eine Menge M gleichmächtig zu einer echten Teilmenge L ist, mit anderen Worten, dass es eine injektive Abbildung $f : M \rightarrow M$ gibt, die nicht surjektiv ist. Stellen wir uns ein gespanntes Gummiband als eine Strecke vor und bewegen die Endpunkte aufeinander zu, bis das Band gerade noch straff ist, so hat sich jeder Punkt der Strecke an einen neuen Ort bewegt. Die dadurch gegebene Abbildung der Strecke in sich selbst ist injektiv, aber nicht surjektiv. Das ist allerdings kein Existenzbeweis auf streng logischer Ebene. Die Existenz einer solchen Abbildung ist vielmehr ein Axiom der Mengenlehre.

Um für zwei Mengen M und N nachzuprüfen, ob $|M| < |N|$ gilt, genügt es also nicht, eine injektive nichtsurjektive Abbildung $M \rightarrow N$ oder eine surjektive nichtinjektive Abbildung $N \rightarrow M$ zu finden, sondern man muss

u.a. zeigen, dass es keine injektive Abbildung $N \rightarrow M$ geben kann oder dass es keine surjektive Abbildung $M \rightarrow N$ geben kann. Wenn man alle Abbildungen auflisten kann, ist das leicht.

Beispiel. Betrachten wir die Menge

$$M = \{a, b, c\}.$$

Die Menge ihrer Teilmengen ist

$$\mathcal{P} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Man kann nachprüfen, dass \mathcal{P} mächtiger ist als M , d. h. $|M| < |\mathcal{P}|$. Ist das bei allen Mengen so?

Satz 19 (Cantor). *Ist M eine beliebige Menge und \mathcal{P} die Menge ihrer Teilmengen, so ist $|M| < |\mathcal{P}|$.*

Beweis. Wir können eine Abbildung $F : M \rightarrow \mathcal{P}$ durch die Festlegung

$$F(x) = \{x\} \quad \text{für alle } x \in M$$

definieren. Diese ist offensichtlich injektiv, also $|M| \leq |\mathcal{P}|$.

Nun sei F eine beliebige Abbildung von M in \mathcal{P} . Für jedes $x \in M$ hat die Aussage $x \in F(x)$ einen Wahrheitswert, da $F(x)$ eine Teilmenge von M ist. Wir können also die Teilmenge

$$L = \{x \in M \mid x \notin F(x)\}$$

von M bilden, das heißt $L \in \mathcal{P}$. Nun sei u irgend ein Element von M . Wenn $u \in F(u)$ ist, so ist laut Definition $u \notin L$, ist hingegen $u \notin F(u)$, so gilt $u \in L$. Auf jeden Fall können die Mengen $F(u)$ und L nicht übereinstimmen, das heißt, es gibt kein $u \in M$ mit der Eigenschaft $F(u) = L$, und somit ist F nicht surjektiv. Da $F : M \rightarrow \mathcal{P}$ beliebig war, ist $|M| \neq |\mathcal{P}|$. \square

Die Idee für diesen Beweis stammt aus der seit dem griechischen Altertum bekannten Antinomie vom lügenden Kreter.

Die Kleiner-Gleich-Relation hängt eng mit der Addition zusammen:

Satz 20. *Für Kardinalzahlen m und n gilt $m \leq n$ genau dann, wenn es eine Kardinalzahl l gibt, so dass $m + l = n$.*

Beweis. Wir wählen Repräsentanten M und N der Kardinalzahlen m und n . Ist $m \leq n$, so gibt es eine injektive Abbildung $f : M \rightarrow N$. Wir bezeichnen den Wertebereich von f mit K und setzen $L = N \setminus K$. Wegen der Injektivität

von f ist $M \sim K$. Außerdem gilt $N = K \cup L$, und wegen der Disjunktheit von K und L folgt

$$|K| + |L| = |N|.$$

Hier ist $|K| = m$ und $|N| = n$, und wir brauchen nur $l = |L|$ zu setzen.

Umgekehrt folgt aus der Existenz einer Kardinalzahl l mit der Eigenschaft $m + l = n$, dass es disjunkte Mengen M und L gibt, so dass $|M| = m$, $|L| = l$ und $|M \cup L| = n$. Die durch $g(x) = x$ gegebene Abbildung $g : M \rightarrow M \cup L$ ist injektiv, und die Ungleichung $m \leq n$ folgt. \square

Für die Kleiner-Gleich-Relation gelten die folgenden **Monotoniegesetze**.

Satz 21. *Für alle Kardinalzahlen k, l, m und n gilt:*

(i) *Wenn $k \leq l$ und $m \leq n$, dann $k + m \leq l + n$.*

(ii) *Wenn $k \leq l$ und $m \leq n$, dann $k \cdot m \leq l \cdot n$.*

Beweis. Der Beweis im Fall der Addition ist eine Übungsaufgabe.

Für den Fall der Multiplikation wählen wir Mengen K, L, M und N , so dass $|K| = k$, $|L| = l$, $|M| = m$ und $|N| = n$. Nach unseren Voraussetzungen gibt es injektive Abbildungen $f : K \rightarrow L$ und $g : M \rightarrow N$. Wir definieren eine Abbildung $h : K \times M \rightarrow L \times N$ durch

$$h((x, y)) = (f(x), g(y)).$$

Wir behaupten, dass h injektiv ist. Angenommen, die geordneten Paare (r, s) und (t, u) aus dem Kreuzprodukt $K \times L$ werden von h auf das selbe Element von $M \times N$ abgebildet, d. h.

$$h((r, s)) = h((t, u)).$$

Nach unserer Definition bedeutet dies, dass

$$(f(r), g(s)) = (f(t), g(u)).$$

Zwei geordnete Paare gelten dann als gleich, wenn sie in ihren vorderen und ihre hinteren Einträgen übereinstimmen, also ist die letzte Gleichung äquivalent zu

$$f(r) = f(t) \quad \text{und} \quad g(s) = g(u).$$

Wegen der Injektivität von f und g folgt hieraus, dass $r = t$ und $s = u$ ist, das heißt

$$(r, s) = (t, u).$$

Somit ist h injektiv. \square

Satz 22 (Schröder-Bernstein). *Gibt es eine injektive Abbildung von M in N und eine injektive Abbildung von N in M , so ist M gleichmächtig zu N .*

Bevor wir zum Beweis kommen, vermerken wir:

Folgerung 2. *Gelten für Kardinalzahlen m und n die beiden Aussagen*

$$m \leq n \quad \text{und} \quad n \leq m,$$

so ist $m = n$.

Diese Eigenschaft der Kleiner-Gleich-Relation nennt man auch *Antisymmetrie*.

Eine weitere Eigenschaft ist die *Totalität* – Für beliebige Kardinalzahlen m und n gilt

$$m \leq n \quad \text{oder} \quad n \leq m.$$

Letzteres mag offensichtlich erscheinen, aber der Beweis ist sehr schwer. Üblicherweise führt man ihn erst, nachdem man Ordinalzahlen eingeführt hat, und das Auswahlaxiom spielt dabei eine wichtige Rolle. Erst aus der Antisymmetrie und der Totalität folgt, dass die Aussage $m < n$ die Negation der Aussage $n \leq m$ ist (vgl. Aufgabe 22(a))!

Um Satz 22 logisch korrekt zu beweisen, müssen wir Abbildungen f einer Menge M in sich selbst etwas näher betrachten.

Definition 23. *Es sei f eine Abbildung der Menge M in sich selbst und L eine Teilmenge von M . Wir sagen, L sei abgeschlossen unter der Abbildung f , wenn für jedes Element x von L auch $f(x) \in L$ ist. Zur Abkürzung sagen wir auch, L sei f -abgeschlossen.*

Natürlich ist M selbst f -abgeschlossen. Der Durchschnitt von f -abgeschlossenen Teilmengen K und L ist ebenfalls f -abgeschlossen. Für jedes Element x dieses Durchschnitts gilt nämlich $x \in K$ und $x \in L$, also wegen der f -Abgeschlossenheit von K und L auch $f(x) \in K$ und $f(x) \in L$, und das bedeutet $f(x) \in K \cap L$. Das Gleiche gilt für den Durchschnitt einer beliebigen nichtleeren Menge von Teilmengen von M .

Satz 23. *Ist $f : M \rightarrow M$ und ist $K \subseteq M$, so gibt es unter allen f -abgeschlossenen Teilmengen von M , die K enthalten, eine kleinste (genannt der f -Abschluss von K).*

Wenn wir sagen, dass L die kleinste solche Menge ist, dann meinen wir, dass L in jeder anderen f -abgeschlossenen Teilmenge, die K enthält, enthalten sein muss. Es ist nicht offensichtlich, dass es eine solche Menge gibt. Ist z. B. $|M| \neq 1$, so gibt es unter den nichtleeren Teilmengen von M keine kleinste.

Beweis von Satz 23. Es sei L der Durchschnitt aller f -abgeschlossenen Teilmengen von M , die K enthalten. Dieser Durchschnitt existiert, weil M selbst eine von diesen Mengen ist, und er ist in jeder dieser Mengen enthalten. Er ist, wie wir gesehen haben, f -abgeschlossen, und offensichtlich enthält er die Menge K . \square

Mitunter kann man den f -Abschluss einer Teilmenge K praktisch auf die folgende Weise bestimmen. Für jedes $x \in K$ muss $f(x)$ zum f -Abschluss gehören, also fügt man diese Elemente zu K hinzu. Ist die entstehende Menge noch nicht f -abgeschlossen, so muss man das Verfahren wiederholen. Kommt man nach mehreren Wiederholungen zu einer f -abgeschlossenen Teilmenge, so hat man den f -Abschluss gefunden. Es kann allerdings vorkommen, dass dieses Verfahren nie zum Ende kommt.

Für den Beweis des Satzes von Schröder-Bernstein benötigen wir noch einen Hilfssatz.¹⁵

Lemma 1. *Ist $f : M \rightarrow M$ eine injektive Abbildung, K eine Teilmenge von M und L ihr f -Abschluss, so gibt es für jedes $y \in L \setminus K$ ein $x \in L$, so dass $f(x) = y$.*

Beweis. Angenommen, zu einem gegebenen y gibt es kein solches x . Dann ist auch $L \setminus \{y\}$ eine f -abgeschlossene Teilmenge, und wegen $y \notin K$ enthält sie die Menge K . Dann ist aber L nicht mehr die kleinste derartige Menge. Dies widerspricht der Voraussetzung, dass L der f -Abschluss von K sein soll. Somit war unsere Annahme falsch. \square

Beweis von Satz 22. Wir nehmen zunächst an, dass M und N disjunkt sind, und definieren eine Abbildung h der Menge $M \cup N$ in sich selbst durch die Festlegung

$$\begin{aligned} h(x) &= f(x), & \text{falls } x \in M, \\ h(x) &= g(x), & \text{falls } x \in N. \end{aligned}$$

Wegen der Injektivität von f und g und der Disjunktheit von M und N ist auch h injektiv. Wir bezeichnen das Komplement des Wertebereiches von f in N mit K und den h -Abschluss von K mit L . Nun definieren wir eine Abbildung $i : M \rightarrow N$ wie folgt.

- (a) Ist $x \in M \setminus L$, so setzen wir $i(x) = f(x)$.
- (b) Ist hingegen $x \in M \cap L$, so ist $x \in L \setminus K$, und nach Lemma 1 gibt es ein $y \in L$, so dass $h(y) = x$. Aus der Definition von h folgt, dass dann $y \in N$ und $g(y) = x$. Wegen der Injektivität von g ist y eindeutig bestimmt, und wir setzen $i(x) = y$.

Dies ist korrekt, weil M die Vereinigung der disjunkten Mengen $M \setminus L$ und $M \cap L$ ist.

Nehmen wir an, dass es Elemente $u \neq v$ von M gibt, die von i beide auf das selbe Element $y \in N$ abgebildet werden. Es können nicht beide zu L gehören, denn dann wäre $f(u) = f(v)$ im Widerspruch zur Injektivität von f . Es ist auch nicht möglich, dass keines von beiden zu L gehört, denn dann wäre $g(y) = u$ und $g(y) = v$. Es bleibt nur der Fall, dass eines von ihnen zu L gehört, sagen wir $u \notin L$, $v \in L$. Dann ist einerseits $f(u) = y$ und deshalb $y \notin K$, andererseits ist $g(y) = v$, wobei $y \in L$. Nach Lemma 1 gibt es ein $x \in L$, so dass $h(x) = y$, und aus der Definition von h folgt, dass $x \in M$ und $f(x) = y$. Wegen der Injektivität von f ist dann $x = u$, also $u \in L$. Das ist ein Widerspruch, also war unsere Annahme falsch, und i ist injektiv.

Zum Beweis der Surjektivität betrachten wir ein beliebiges Element y von N . Ist $y \in L$, so wird das Element $g(y)$ durch i auf y abgebildet. Ist hingegen $y \notin L$, so ist auch $y \notin K$, also gibt es ein $x \in M$, so dass $f(x) = y$. Wäre $x \in L$, so wäre wegen der h -Abgeschlossenheit von L auch $y \in L$. Das ist ein Widerspruch, also ist $x \notin L$ und $i(x) = y$. Somit ist i surjektiv.

¹⁵In der Tradition von Euklids „Elementen“ bezeichnet man einen Hilfssatz als *Lemma* (Mehrzahl *Lemmata*).

Unter der Voraussetzung, dass M und N disjunkt sind, haben wir also bewiesen, dass i bijektiv ist und somit die Mengen M und N gleichmächtig sind.

Sind M und N nicht disjunkt, dann können wir disjunkte Mengen P und Q finden, so dass $P \sim M$ und $Q \sim N$. Wie im Beweis von Satz 18 erhalten wir aus f und g injektive Abbildungen $P \rightarrow Q$ sowie $Q \rightarrow P$. Nach dem bereits Bewiesenen ist $P \sim Q$, und mit Satz 7 folgt $M \sim N$. \square

3 Natürliche Zahlen

3.1 Endliche Mengen

Wir wollen die Eigenschaft, endlich zu sein, definieren. Die hier gewählte Herangehensweise geht von der Vorstellung aus, dass man eine endliche Menge erhält, wenn man zur leeren Menge mehrmals je ein Element hinzufügt. Das darf man aber nur endlich oft tun. Leider ist dies keine Definition, denn in einer solchen darf der zu definierende Begriff nicht verwendet werden. Wir führen zunächst einen Hilfsbegriff ein.

Definition 24. *Es sei M eine Menge und \mathcal{P} die Menge ihrer Teilmengen. Eine Teilmenge \mathcal{I} von \mathcal{P} heißt induktive Menge von Teilmengen in M , wenn sie folgende Eigenschaften hat:*

- (i) $\emptyset \in \mathcal{I}$.
- (ii) Für jedes $K \in \mathcal{I}$ und $a \in M$ ist $K \cup \{a\} \in \mathcal{I}$.

Wenn wir schon wüssten, was endlich heißt, so müsste die Menge der endlichen Teilmengen von M induktiv sein. Leider ist dies im Allgemeinen nicht die einzige induktive Menge von Teilmengen in M , denn auch die Menge \mathcal{P} ist induktiv. Ist aber die Menge M endlich (was immer das auch heißen möge), dann sollte auch jede Teilmenge endlich sein.

Definition 25. *Die Menge M heißt endlich, wenn \mathcal{P} die einzige induktive Menge von Teilmengen in M ist.*

Eine endliche Menge ist also dadurch charakterisiert, dass eine beliebige induktive Menge von Teilmengen aus sämtlichen Teilmengen besteht.

Satz 24. *Es sei $f : M \rightarrow N$ eine Abbildung.*

- (i) *Ist N endlich und f injektiv, so ist M endlich.*
- (ii) *Ist M endlich und f surjektiv, so ist N endlich.*

Bevor wir diesen Satz beweisen, ziehen wir eine Folgerung.

Folgerung 3. *Eine Teilmenge einer endlichen Menge ist endlich.*

Ist nämlich M eine Teilmenge von N , so ist die durch $f(x) = x$ für alle $x \in M$ definierte Abbildung injektiv.

Beweis von Satz 24. (i) Wir beweisen zunächst die Folgerung, die ja einen Spezialfall darstellt. Es sei \mathcal{I} induktiv in M . Wir definieren eine Menge \mathcal{J} von Teilmengen von N wie folgt. Sie umfasst alle Elemente von \mathcal{I} sowie alle Teilmengen von N , die nicht in M enthalten sind, d. h.

$$\mathcal{J} = \mathcal{I} \cup \{L \subseteq N \mid L \not\subseteq M\}.$$

Wir wollen zeigen, dass \mathcal{J} induktiv in N ist. Zunächst ist offenbar $\emptyset \in \mathcal{J}$. Nun sei $L \in \mathcal{J}$ und $b \in N$. Ist $b \notin M$ oder $L \not\subseteq M$, so ist $L \cup \{b\}$ nicht in M enthalten, gehört also zu \mathcal{J} . Ist hingegen $L \subseteq M$ und $b \in M$, so ist $L \cup \{b\}$ ein Element der induktiven Menge \mathcal{I} , also auch von \mathcal{J} .

Damit ist \mathcal{J} induktiv in der endlichen Menge N und besteht folglich aus allen Teilmengen von N . Ist nun $K \subseteq M$, so ist auch $K \subseteq N$, also $K \in \mathcal{J}$, und aus der Definition von \mathcal{J} folgt $K \in \mathcal{I}$. Also besteht \mathcal{I} aus allen Teilmengen von M . Da \mathcal{I} beliebig war, ist M endlich.

Nun kommen wir zum allgemeinen Fall einer injektiven Abbildung $f : M \rightarrow N$. Wir bezeichnen den Wertebereich von f mit M' . Ist nun \mathcal{I} eine induktive Teilmenge von Mengen in M , so erhalten wir für jedes $K \in \mathcal{I}$ eine Teilmenge

$$K' = \{f(x) \mid x \in K\}$$

von M' , und diese Teilmengen bilden, weil jedes Element von M' von der Form $f(x)$ ist, eine induktive Menge \mathcal{I}' von Teilmengen in M' . Da M' nach dem Bewiesenen endlich ist, gehört jede Teilmenge von M' zu \mathcal{I}' , und wegen der Injektivität von f gehört jede Teilmenge von M zu \mathcal{I} .

(ii) Nach Satz 17 gibt es eine injektive Abbildung $N \rightarrow M$, und die Behauptung folgt aus (i). \square

Zwischen gleichmächtigen Mengen gibt es bijektive Abbildungen in beiden Richtungen, und Behauptung (i) zeigt:

Folgerung 4. *Ist von zwei gleichmächtigen Mengen die eine endlich, so auch die andere.*

Nun können wir die Objekte unseres ersten Zahlbereichs einführen.

Definition 26. *Unter einer natürlichen Zahl verstehen wir eine Kardinalzahl, die die Mächtigkeit einer endlichen Menge ist.*

Für uns sind Kardinalzahlen ja Mächtigkeitsklassen, und die Folgerung sagt uns, dass eine natürliche Zahl als Klasse betrachtet ausschließlich aus endlichen Mengen besteht.

Bezeichnen wir die Mächtigkeiten der Mengen M und N in Satz 24 mit m und n , so erhalten wir:

Folgerung 5. Gilt für eine Kardinalzahl m und eine natürliche Zahl n die Ungleichung $m \leq n$, so ist auch m eine natürliche Zahl.

Wir können nun Satz 20 für natürliche Zahlen konkretisieren.

Satz 25. Für natürliche Zahlen m und n gilt $m \leq n$ genau dann, wenn es eine natürliche Zahl l gibt, so dass $m + l = n$.

Beweis. Gilt $m \leq n$, so gibt es nach Satz 20 eine Kardinalzahl l , so dass $m + l = n$ ist. Nach Satz 10 ist dann aber auch $l + m = n$, und wiederum mit Satz 20 folgt $l \leq n$. Nun schließen wir mit Satz 24, dass l eine natürliche Zahl ist.

Die Umkehrung folgt direkt aus Satz 20. □

Für den nächsten Satz benötigen wir einen Hilfssatz.¹⁶

Lemma 2. Ist M eine endliche Menge und a ein Objekt, so ist $M \cup \{a\}$ endlich.

Beweis. Wir brauchen nur den Fall zu behandeln, dass $a \notin M$ ist. Es sei \mathcal{J} eine induktive Menge von Teilmengen in $M \cup \{a\}$. Wir betrachten

$$\mathcal{I} = \{L \in \mathcal{J} \mid a \notin L\}.$$

Dies ist offensichtlich eine induktive Menge von Teilmengen in der endlichen Menge M , also die Menge aller Teilmengen von M . Es genügt zu zeigen, dass \mathcal{J} die Menge aller Teilmengen von $M \cup \{a\}$ ist.

Ist irgendeine Teilmenge L von $M \cup \{a\}$ gegeben, so betrachten wir die Teilmenge $K = L \setminus \{a\}$ von M . Nach dem Bewiesenen gilt $K \in \mathcal{I}$, also $K \in \mathcal{J}$. Nun gibt es zwei Fälle. Ist $a \notin L$, so ist $L = K$ also $L \in \mathcal{J}$. Ist hingegen $a \in L$, so ist $L = K \cup \{a\}$, und da \mathcal{J} induktiv ist, folgt auch in diesem Fall $L \in \mathcal{J}$. □

Satz 26. Sind M und N endliche Mengen, so sind auch $M \cup N$ und $M \times N$ endlich.

Beweis. Wir widmen uns zunächst der Vereinigung. Es sei \mathcal{J} die Menge derjenigen Teilmengen L von N , für die $M \cup L$ endlich ist. Da M endlich ist, gilt $\emptyset \in \mathcal{J}$. Ist nun $L \in \mathcal{J}$ und $b \in N$, so ist nach Satz 2

$$M \cup (L \cup \{b\}) = (M \cup L) \cup \{b\},$$

und mit Lemma 2 folgt, dass diese Menge endlich ist, d. h. $L \cup \{b\} \in \mathcal{J}$. Wir haben gezeigt, dass \mathcal{J} induktiv in N ist, und da N endlich ist, folgt insbesondere $N \in \mathcal{J}$.

Der Beweis für das Produkt ist ähnlich (Aufgabe 23). □

¹⁶Siehe Fußnote auf S. 37.

Folgerung 6. *Die Summe und das Produkt von natürlichen Zahlen sind natürliche Zahlen.*

Bevor wir ein weiteres Resultat anführen, führen wir einen leicht verständlichen Begriff ein.

Definition 27. *Es seien a und b Elemente einer Menge M . Die Transposition von a und b in der Menge M ist die Abbildung $t : M \rightarrow M$, die gegeben ist durch die Vorschrift*

$$t(a) = b, \quad t(b) = a, \quad t(x) = x \quad \text{für alle } x \in M \setminus \{a, b\}.$$

Es ist offensichtlich, dass eine Transposition t in einer Menge M die Eigenschaft

$$t \circ t = \text{id}_M$$

hat und bijektiv ist.

Wir haben eben einige Sätze kennengelernt, mit denen man zeigen kann, dass gewisse Mengen endlich sind. Den folgenden Satz kann man u. a. für den Nachweis benutzen, dass gewisse Mengen unendlich sind.

Satz 27. *Es sei M eine endliche Menge. Eine Abbildung $f : M \rightarrow M$ ist genau dann injektiv, wenn sie surjektiv ist.*

Beweis. Es sei \mathcal{I} die Menge derjenigen Teilmengen K von M , für die jede injektive Abbildung $h : K \rightarrow K$ auch surjektiv ist. Offensichtlich ist $\emptyset \in \mathcal{I}$. Nun sei $K \in \mathcal{I}$ und $a \in M$. Um zu zeigen, dass auch $K \cup \{a\} \in \mathcal{I}$ ist, genügt es den Fall $a \notin K$ zu betrachten.

Sei also g eine injektive Abbildung von $K \cup \{a\}$ in sich selbst. Angenommen g ist nicht surjektiv. Dann gibt es ein Element b , das nicht im Wertebereich von g liegt. Wir betrachten zunächst den Spezialfall, dass $a = b$ ist. Dann können wir eine injektive Abbildung $h : K \rightarrow K$ durch die Festlegung $h(x) = g(x)$ definieren. Wegen $K \in \mathcal{I}$ ist h surjektiv. Aufgrund der Injektivität von g liegt aber $g(a)$ nicht im Wertebereich von h . Dieser Widerspruch zeigt, dass unsere Annahme falsch war, also muss g surjektiv sein.

Nun kommen wir zum Fall $a \neq b$. Wir bezeichnen die Transposition von a und b in $K \cup \{a\}$ mit t . Da t bijektiv ist, ist $t \circ g$ nach Satz 5 ebenfalls injektiv, aber wegen $g = t \circ (t \circ g)$ nicht surjektiv. Das Element a gehört nicht zum Wertebereich von $t \circ g$, denn aus $a = t(g(x))$ würde bei Anwendung von t auf beiden Seiten $b = g(x)$ folgen. Wir können also im vorangehenden Argument g durch $t \circ g$ ersetzen und stoßen wieder auf den erwünschten Widerspruch.¹⁷

¹⁷Für fortgeschrittene Leser lässt man den allgemeinen Fall weg und merkt stattdessen nur an, dass man ohne Beschränkung der Allgemeinheit (abgekürzt o.B.d.A.) $a = b$ annehmen kann.

Zum Beweis der Umkehrung betrachten wir eine surjektive Abbildung $f : M \rightarrow M$. Nach Satz 17 gibt es eine injektive Abbildung $g : M \rightarrow M$, so dass $f \circ g = \text{id}_M$. Nach dem bereits Bewiesenen ist g bijektiv, hat also nach Satz 6 eine Umkehrabbildung k , die ebenfalls bijektiv ist. Nun gilt nach Satz 4

$$f = f \circ (g \circ k) = (f \circ g) \circ k = k,$$

und f ist folglich injektiv. \square

Folgerung 7. *Ist N eine echte Teilmenge einer endlichen Menge M , so ist $|N| < |M|$.*

Wäre nämlich $|N| = |M|$, so gäbe es eine bijektive Abbildung $h : M \rightarrow N$, und wir erhielten eine Abbildung $f : M \rightarrow M$ mit dem Wertebereich N durch die Festlegung $f(x) = h(x)$ für alle $x \in M$.

Satz 28. *Sind M und N endliche Mengen, so gibt es eine injektive Abbildung $M \rightarrow N$ oder eine injektive Abbildung $N \rightarrow M$.*

Beweis. Es sei \mathcal{I} die Menge derjenigen Teilmengen K von M mit der Eigenschaft, dass es eine injektive Abbildung $K \rightarrow N$ oder eine injektive Abbildung $N \rightarrow K$ gibt. Wir wollen zeigen, dass \mathcal{I} induktiv in M ist.

Da es immer eine injektive Abbildung $\emptyset \rightarrow N$ gibt, ist $\emptyset \in \mathcal{I}$. Angenommen, $K \in \mathcal{I}$ und $a \in M$. Um zu zeigen, dass $K \cup \{a\} \in \mathcal{I}$ ist, können wir wieder $a \notin K$ annehmen. Gibt es eine injektive Abbildung $N \rightarrow K$, so gibt es offensichtlich auch eine injektive Abbildung $N \rightarrow K \cup \{a\}$. Nun betrachten wir den Fall, dass es eine injektive Abbildung $f : K \rightarrow N$ gibt. Ist diese auch surjektiv, so hat sie nach Satz 6 eine injektive Umkehrabbildung $N \rightarrow K$, und wir sind wieder im ersten Fall. Gibt es hingegen ein Element b von N , das nicht im Wertebereich von f liegt, so definieren wir eine Abbildung $g : K \cup \{a\} \rightarrow N$ durch die Festlegung $g(a) = b$ und $g(x) = f(x)$ für $x \in K$. Dann ist g injektiv.

In jedem Fall erhalten wir also $K \cup \{a\} \in \mathcal{I}$. Damit ist \mathcal{I} induktiv in M , und da M endlich ist, gilt auch $M \in \mathcal{I}$. \square

Aus diesem Satz folgt die Totalität der Kleiner-Gleich-Relation für natürliche Zahlen:

Folgerung 8. *Für beliebige natürliche Zahlen m und n gilt $m \leq n$ oder $n \leq m$.*

Wie wir auf S. 36 erwähnt haben, gilt dies auch für die Kleiner-Gleich-Relation auf den Kardinalzahlen, was wir aber in dieser Vorlesung nicht beweisen werden. Immerhin haben wir im Beweis von Satz 28 die Endlichkeit von N nicht benutzt.

Die Gesamtheit aller Mengen kann keine Menge sein, sonst könnte man die Menge aller Mengen bilden, die nicht Element von sich selbst sind, was ähnlich wie im Beweis von Satz 19 zu einem Widerspruch führen würde. Darum ist zunächst unklar, ob die Gesamtheit aller Kardinalzahlen bzw. aller natürlichen Zahlen eine Menge ist. Man kann aber die Mengenlehre so entwickeln (was wir hier nicht ausführen wollen), dass die natürlichen Zahlen tatsächlich eine Menge bilden, für die sich die von N. Bourbaki eingeführte Abkürzung \mathbf{N} durchgesetzt hat.¹⁸

3.2 Vollständige Induktion

Enthält eine Aussageform eine Variable n , so wird sie beim Ersetzen von n durch ein Objekt zu einer Aussage, nimmt also einen der Werte w oder f an. Deshalb betrachtet man sie in der Informatik als Funktion mit der Zielmenge $\{w, f\}$ und kürzt sie z. B. durch $A(n)$ ab. Diese Schreibweise ist auch in der Mathematik üblich.

In der Logik unterscheidet man zwischen Deduktion (Ableitung einer speziellen Aussage aus einem allgemeingültigen Gesetz) und Induktion (Rückschluss auf ein allgemeingültiges Gesetz aus bekannten Spezialfällen). Die Induktion stellt zwar den Hauptkenntnisweg in den Experimentalwissenschaften dar (auch wenn sie dort nicht unter diesem Namen erwähnt wird), aber für die Mathematik ist sie wertlos. Trotzdem gibt es eine Beweismethode, bei der die Gültigkeit einer Aussage, beginnend mit einem Spezialfall, auf immer mehr Fälle (nämlich natürliche Zahlen) ausgeweitet wird. Kann man sie auf diesem Wege für alle natürlichen Zahlen beweisen, so spricht man von vollständiger Induktion. Die Methode wird durch folgenden Satz gerechtfertigt.

Satz 29. *Es sei N eine Teilmenge von \mathbf{N} mit folgenden Eigenschaften:*

- (i) $0 \in N$.
- (ii) Wenn $n \in N$ ist, so ist auch $n + 1 \in N$.

Dann ist $N = \mathbf{N}$.

(Die Zahl $n + 1$ nennt man bekanntlich den *Nachfolger* der Zahl n .)

Beweis. Es sei m eine beliebige natürliche Zahl. Das bedeutet, dass es eine endliche Menge M gibt, so dass $|M| = m$. Es sei \mathcal{I} die Menge der Teilmengen K von M mit der Eigenschaft $|K| \in N$. Wegen der Eigenschaft (i) von N ist $\emptyset \in \mathcal{I}$.

¹⁸An der Tafel wird das fettgedruckte \mathbf{N} meist als \mathbf{N} wiedergegeben.

Nun sei $K \in \mathcal{I}$ und $a \in M$. Dann gibt es zwei Fälle. Ist $a \in K$, so ist $K \cup \{a\} = K \in \mathcal{I}$. Ist $a \notin K$, so sind K und $\{a\}$ disjunkt, also

$$|K \cup \{a\}| = |K| + |\{a\}| = |K| + 1.$$

Wegen $|K| \in N$ folgt aus der Eigenschaft (ii), dass $|K \cup \{a\}| \in N$, also auch in diesem Fall $K \cup \{a\} \in \mathcal{I}$ ist.

Wir haben bewiesen, dass \mathcal{I} induktiv ist. Da M endlich ist, ist insbesondere $M \in \mathcal{I}$, also $m \in N$. \square

Folgerung 9. *Eine Aussageform $A(n)$ sei für alle natürlichen Zahlen n definiert. Gilt die Aussage $A(0)$ und gilt für jede natürliche Zahl „wenn $A(n)$, dann $A(n+1)$ “, so gilt $A(n)$ für alle natürlichen Zahlen n .*

Diese Folgerung kann den Beweis von Aussagen über alle natürlichen Zahlen erheblich vereinfachen oder überhaupt erst ermöglichen, denn beim Beweis der Aussage für eine bestimmte natürliche Zahl darf man nun annehmen, dass die Aussage bereits für den Vorgänger dieser Zahl gilt (wenn es einen gibt).

Den Beweis der Aussage $A(0)$ nennt man den *Induktionsanfang*, den Beweis der Aussage „wenn $A(n)$, dann $A(n+1)$ “ nennt man den *Induktionsschritt*. Diesen führt man für jede einzelne natürliche Zahl n . Da es unendlich viele solche Zahlen gibt, muss man ein Argument finden, dass für jede dieser Zahlen funktioniert. Nichtsdestotrotz hält man während des Induktionsschritts die Zahl n fest. Die Aussage $A(n)$ nennt man in diesem Zusammenhang die *Induktionsvoraussetzung* und die Aussage $A(n+1)$ die *Induktionsbehauptung*.

Mit dieser Methode kann man zahlreiche Aussagen über natürliche Zahlen beweisen, wie z. B. den folgenden Satz.

Satz 30. *Sind m und $n \neq 0$ natürliche Zahlen, dann gibt es natürliche Zahlen q und r , so dass*

$$m = q \cdot n + r \quad \text{und} \quad r < n.$$

Beweis. Wir halten eine beliebige natürliche Zahl n fest und führen den Beweis durch vollständige Induktion nach m .

Ist $m = 0$, so können wir $q = 0$ und $r = 0$ setzen, denn es gilt

$$0 = 0 \cdot n + 0 \quad \text{und} \quad 0 < n,$$

weil wir $n \neq 0$ vorausgesetzt haben. Damit ist der Induktionsanfang abgeschlossen.

Nun nehmen wir an, dass es für gegebene natürliche Zahlen m und $n \neq 0$ natürliche Zahlen q und r gibt, so dass

$$m = q \cdot n + r \quad \text{und} \quad r < n.$$

(Dies ist die Induktionsvoraussetzung.) Wir müssen beweisen, dass dann auch die Aussage gilt, die man daraus durch Ersetzung von n durch $n + 1$ gewinnt, also im vorliegenden Fall die Aussage

Es gibt natürliche Zahlen q' und r' , so dass

$$m + 1 = q' \cdot n + r' \quad \text{und} \quad r' < n.$$

(Dies ist die Induktionsbehauptung.) Wenn uns das gelingt, dann ist der Beweis auf Grund von Folgerung 9 abgeschlossen.¹⁹

Laut Induktionsvoraussetzung und Assoziativgesetz (Satz 10) gilt

$$m + 1 = (q \cdot n + r) + 1 = q \cdot n + (r + 1).$$

Aus $r < n$ folgt laut Aufgabe 26, dass $r + 1 \leq n$. Nun unterscheiden wir zwei Fälle.

- Ist $r + 1 \neq n$, so ist $r + 1 < n$. Also gilt die Behauptung für $m + 1$, wenn wir $q' = q$ und $r' = r + 1$ setzen.
- Ist $r + 1 = n$, so ist

$$m + 1 = q \cdot n + 1 \cdot n = (q + 1) \cdot n.$$

Also gilt die Behauptung für $m + 1$, wenn wir $q' = q + 1$ und $r' = 0$ setzen.

Damit ist der Induktionsschritt abgeschlossen. □

Man beachte, dass Induktionsvoraussetzung und Induktionsbehauptung keine Beweisschritte sind. Es ist allenfalls sinnvoll, sich zu Beginn des Induktionsschrittes klarzumachen, was man benutzen darf und was man zu beweisen hat. Besonders die Gewinnung der Induktionsbehauptung aus der Induktionsvoraussetzung mittels Ersetzung von n durch $n + 1$ an allen Stellen ist nämlich eine häufige Fehlerquelle.

¹⁹Mehr Hilfe kann die Methode der vollständigen Induktion nicht leisten. Von hier an muss man wie in jedem Beweis weitere Ideen einbringen.

3.3 Ordnungen

Ordnungen kommen in vielen praktischen Situationen vor. So gibt es auf jedem Hühnerhof eine Hackordnung, und man hat die Buchstaben des Alphabets geordnet. Die Aussage „ a (kommt) vor b “ kürzen wir durch $a \prec b$ ab. Ähnlich wie bei der Kleiner-Gleich-Relation ist es nützlich, auch hier Gleichheit zuzulassen. So ist z. B. $a \preceq a$.

Definition 28. Die Aussage $x \preceq y$ sei für alle Objekte x und y einer Menge M definiert. Man nennt \preceq eine Ordnung auf M , wenn für alle Elemente x , y und z von M gilt:

- (i) $x \preceq y$ oder $y \preceq x$. (Totalität)
- (ii) Wenn $x \preceq y$ und $y \preceq z$, dann $x \preceq z$. (Transitivität)
- (iii) Wenn $x \preceq y$ und $y \preceq x$, dann $x = y$. (Antisymmetrie)

Zu jeder Relation gibt es die umgekehrte Relation, die man mit dem gespiegelten Symbol bezeichnet:

$$x \succeq y \quad \text{bedeutet, dass} \quad y \preceq x.$$

Die umgekehrte Relation einer Ordnung ist wieder eine Ordnung. So ist die Größer-Gleich-Relation die umgekehrte Relation zur Kleiner-Gleich-Relation.

Verlangt man an Stelle der Totalität nur die Eigenschaft

$$x \preceq x \text{ für alle } x \text{ (Reflexivität),}$$

so erhält man den Begriff der *Halbordnung*. Die Enthaltenseinsrelation \subseteq ist z. B. eine Halbordnung auf der Menge aller Teilmengen einer gegebenen Menge.

Für verschiedene Ordnungen, die in dem selben Kontext auftauchen, sollte man verschiedene Symbole verwenden. In der Mathematik kommen u. a. \leq , \preceq und \trianglelefteq als Symbole für Ordnungen vor.

Die Ordnung auf dem Alphabet dient bekanntlich zur Ordnung von Einträgen im Wörterbuch oder Lexikon. Wir wollen den mathematischen Gehalt zunächst im Fall von Hausnummern wie 1, 2, 2a, 2b, 3, ... verstehen. Es handelt sich dabei um geordnete Paare aus dem Kreuzprodukt

$$\mathbf{N} \times \{-, a, b, c, \dots, z\}.$$

(Zwar kommt die Null als Hausnummer nicht vor, aber es schadet nicht, sie vorsorglich mit einzubeziehen.) Die Menge \mathbf{N} und das Alphabet (in das wir das Leerzeichen vor allen Buchstaben aufnehmen) haben offensichtliche Ordnungen.

Definition 29. Es sei \leq eine Ordnung auf der Menge M und \preceq eine Ordnung auf der Menge N . Wir definieren eine Relation \trianglelefteq auf der Menge $M \times N$ (genannt lexikographische Ordnung) wie folgt.

Die Aussage $(v, w) \trianglelefteq (x, y)$ bedeutet:

$$v \leq x, \text{ und wenn } v = x, \text{ dann } w \preceq y.$$

Man prüft nach (siehe Aufgabe 29) dass dies tatsächlich eine Ordnung ist. Die Aussage $(v, w) \trianglelefteq (x, y)$ könnte man auch so formulieren:

$$v < x \text{ oder } (v = x \text{ und } w \preceq y).$$

Dabei tritt allerdings zusätzlich die Relation $<$ auf, wobei $v < x$ bedeutet, dass $v \leq x$ und $v \neq x$.

Definition 30. Eine Ordnung auf einer Menge M wird Wohlordnung genannt, wenn jede nichtleere Teilmenge von M ein kleinstes Element bezüglich dieser Ordnung hat.

Satz 31. Die Kleiner-Gleich-Relation auf der Menge der natürlichen Zahlen ist eine Wohlordnung.

Die Wohlordnung der natürlichen Zahlen erlaubt eine allgemeinere Art der vollständigen Induktion, bei der man im Induktionsschritt die Gültigkeit der Behauptung nicht nur für den Vorgänger, sondern für alle kleineren natürlichen Zahlen benutzen darf. Dazu betrachtet man einfach die Menge der natürlichen Zahlen, für die die zu beweisende Behauptung *nicht* gilt. Ihr kleinstes Element hat nämlich die Eigenschaft, dass die fragliche Behauptung für alle kleineren Zahlen gilt.

Beweis. Es sei M eine Teilmenge von \mathbf{N} ohne kleinstes Element. Wir wollen durch vollständige Induktion beweisen, dass für jede natürliche Zahl n folgende Aussage gilt:

$$\text{Für jedes Element } m \text{ von } M \text{ ist } n < m.$$

Zunächst betrachten wir $n = 0$. Laut Definition der Kleiner-Gleich-Relation gilt $0 \leq m$ für alle $m \in M$, und es kann nicht $0 = m$ gelten, weil 0 dann das kleinste Element von M wäre. Damit ist der Induktionsanfang abgeschlossen.

Nun kommen wir zum Induktionsschritt. Betrachten wir also eine natürliche Zahl n , für die die obige Aussage gilt. Für jedes $m \in M$ gilt dann nach Aufgabe 26, dass $n + 1 \leq m$. Wäre $n + 1$ ein Element von M , so wäre es das kleinste. Da es dieses nicht gibt, gilt für alle $m \in M$ außerdem $n + 1 \neq m$, zusammengefasst also $n + 1 < m$. Damit ist der Induktionsschritt beendet und unsere Behauptung für alle $n \in \mathbf{N}$ bewiesen.

Sie muss insbesondere auch gelten, wenn $n \in M$ ist, aber es gibt keine Zahl m mit der Eigenschaft $m < m$. Wir haben somit bewiesen, dass eine Teilmenge von \mathbf{N} ohne kleinstes Element leer sein muss. Die Kontraposition dieser Aussage ist die Behauptung des Satzes. \square

Man kann auch auf der Menge M^N eine lexikographische Ordnung \preceq definieren, wenn eine Ordnung \preceq auf M und eine Wohlordnung \leq auf N gegeben sind. Und zwar bedeutet die Aussage $f \preceq g$ für Abbildungen $f, g : N \rightarrow M$ das Folgende: Es ist $f = g$ oder für das kleinste Element x von M mit der Eigenschaft $f(x) \neq g(x)$ gilt $f(x) \preceq g(x)$. Es lässt sich beweisen, dass dies eine Ordnung ist. Sie gibt das Ordnungsprinzip im Lexikon wieder, wenn wir Wörter wie in der Präsenzaufgabe 6 als Abbildungen von \mathbf{N} in ein Alphabet M interpretieren (bei denen ab einer bestimmten Stelle nur noch Leerzeichen kommen). Wenn auch \preceq eine Wohlordnung ist, braucht \preceq trotzdem keine Wohlordnung zu sein. Unter allen Zeichenketten, die nicht nur aus Leerzeichen bestehen, gibt es keine früheste, weil man immer noch Leerzeichen voranstellen kann. Auch im Branchentelefonbuch, wo Sonderzeichen vor Buchstaben kommen, aber Sonderzeichen am Wortanfang oder direkt hintereinander nicht zugelassen sind, kann man immer weiter nach vorn rutschen, indem man seinem Firmennamen ein A, gefolgt von dem ersten Sonderzeichen, voranstellt.

Wir wollen noch einen Ausblick auf *Ordinalzahlen* geben, obwohl sie in dieser Vorlesung nicht benutzt werden. Eine Menge M zusammen mit einer Wohlordnung \leq nennt man wohlgeordnete Menge. Genaugenommen ist eine wohlgeordnete Menge ein geordnetes Paar (M, \leq) . Zwei wohlgeordnete Mengen (M, \leq) und (N, \preceq) heißen ähnlich, wenn es eine ordnungstreu bijektive Abbildung $f : M \rightarrow N$ gibt. (Dabei heißt f ordnungstreu, wenn für beliebige Elemente $x, y \in M$ genau dann $f(x) \preceq f(y)$ gilt, wenn $x \leq y$.) Wie schon bei der Gleichmächtigkeit fassen wir wohlgeordnete Mengen in Ähnlichkeitsklassen zusammen, und diese Klassen nennt man Ordinalzahlen. So ist z. B. „nulltens“ die Klasse der leeren Menge mit ihrer offensichtlichen Ordnung, und die Ordinalzahl „drittens“ ist z. B. die Klasse der Dreiermenge $\{a, b, c\}$ mit der Ordnung $a \preceq b, b \preceq c$ und (somit) $a \preceq c$. Die endlichen Ordinalzahlen entsprechen eineindeutig den endlichen Kardinalzahlen, das heißt den natürlichen Zahlen.

Man addiert Ordinalzahlen, indem man disjunkte Repräsentanten M und N vereinigt und auf $M \cup N$ eine Ordnung festlegt, bei der jedes Element von M vor jedem Element von N kommt, während innerhalb von M und N die ursprünglichen Ordnungen beibehalten werden. Diese Addition ist nicht kommutativ, wie man am Beispiel $M = \{*\}$, $N = \mathbf{N}$ sieht. Des Weiteren definiert man die Multiplikation von Ordinalzahlen mit Hilfe der lexikographischen Ordnung, während man für die Potenz eine abgewandelte lexikographische Ordnung auf der Teilmenge von M^N betrachtet, die aus denjenigen $f : N \rightarrow M$ besteht, bei denen für alle x außer endlich vielen der Wert $f(x)$ gleich dem Anfangselement von M ist. Damit eine Wohlordnung entsteht, benutzt man die umgekehrte Ordnung auf N .

Ein Abschnitt einer wohlgeordneten Menge (M, \leq) ist eine Teilmenge der Form $\{x \in M \mid x < y\}$ für ein $y \in M$; dieser wird wieder zu einer wohlgeordneten Menge. Die Klassen der Abschnitte von (M, \leq) bezeichnet man dann als kleinere Ordinalzahlen als die Klasse von (M, \leq) . Die so definierte Kleiner-Gleich-Relation für Ordinalzahlen ist total, transitiv und antisymmetrisch.

3.4 Umkehroperationen

In der Schule wird die Subtraktion eingeführt, indem man das Wegnehmen von Elementen einer Menge betrachtet, was auf den Begriff der Differenzmenge hinausläuft. Leider lässt sich auf diese Weise die Differenz beliebiger Kardinalzahlen nicht definieren. Wie wir auf S. 33 gesehen haben, gibt es eine Menge M , die gleichmächtig zu einer echten Teilmenge N ist. Nun haben wir

$$M \setminus N \neq \emptyset, \quad M \setminus M = \emptyset.$$

Bezeichnen wir $|M| = |N| = m$, so gibt es also verschiedene Kardinalzahlen, die als Differenz $m - m$ in Frage kommen!

Für natürliche Zahlen kann so etwas wegen der folgenden *Kürzungsregeln* nicht passieren.

Satz 32. *Es seien k, l und n natürliche Zahlen. Ist*

$$k + n = l + n,$$

so ist $k = l$. Ist

$$k \cdot n = l \cdot n \quad \text{und} \quad n \neq 0,$$

so ist ebenfalls $k = l$.

Für den Beweis benötigen wir

Lemma 3. *Ist n eine Kardinalzahl und M eine Menge, so dass $|M| = n + 1$, dann ist M nicht leer, und für jedes Element a von M gilt $|M \setminus \{a\}| = n$.*

Beweis. Wir wählen eine Menge N der Mächtigkeit n und ein Objekt $b \notin N$. Dann ist $|N \cup \{b\}| = n + 1$. Somit gibt es eine bijektive Abbildung $f : N \cup \{b\} \rightarrow M$. Wegen $f(b) \in M$ ist $M \neq \emptyset$. Nun gibt es zwei Fälle.

Ist $f(b) = a$, so ist wegen der Injektivität $f(x) \neq a$ für alle $x \in N$, und wir können eine Abbildung $g : N \rightarrow M \setminus \{a\}$ durch $g(x) = f(x)$ definieren. Diese ist offensichtlich bijektiv, und es folgt $|N| = |M \setminus \{a\}|$, was zu beweisen war.

Ist hingegen $f(b) \neq a$, so bezeichnen wir die Transposition von a und $f(b)$ mit t . Dann ist $t \circ f$ eine bijektive Abbildung, die b auf a abbildet, und die Behauptung folgt wie im ersten Fall. \square

Beweis von Satz 32. Wir beweisen die erste Behauptung durch vollständige Induktion nach n . Sie gilt offensichtlich für $n = 0$, weil $k + 0 = k$ und $l + 0 = l$ ist. Damit ist der Induktionsanfang abgeschlossen.

Nun kommen wir zum Induktionsschritt. Nehmen wir also an, dass die Behauptung des Satzes für eine gewisse Zahl n richtig ist. Gilt nun

$$k + (n + 1) = l + (n + 1),$$

also laut Assoziativgesetz

$$(k + n) + 1 = (l + n) + 1,$$

so wählen wir eine Menge M , so dass $|M| = (k + n) + 1$. Für ein Element $a \in M$ folgt aus Lemma 3 sowohl $|M \setminus \{a\}| = k + n$ als auch $|M \setminus \{a\}| = l + n$, das heißt

$$k + n = l + n.$$

Nun folgt aus der Induktionsvoraussetzung, dass $k = l$.

Der Beweis der Kürzungsregel für die Multiplikation ist Gegenstand einer Übungsaufgabe. \square

Der Satz rechtfertigt folgende Definition.

Definition 31. *Es seien m und n natürliche Zahlen. Gibt es eine natürliche Zahl k , so dass $n + k = m$, so nennt man k die Differenz von m und n , abgekürzt $m - n$. Ist $n \neq 0$ und gibt es eine natürliche Zahl k , so dass $n \cdot k = m$, so nennt man k den Quotienten von m und n , abgekürzt²⁰ $m : n$.*

Die Rechenoperationen zur Ermittlung der Differenz bzw. des Quotienten nennt man bekanntlich *Subtraktion* bzw. *Division*. Aus Satz 25 erhalten wir:

Folgerung 10. *Die Differenz von natürlichen Zahlen m und n existiert genau dann, wenn $m \geq n$ ist, und dann gilt $m - n \leq m$.*

Für die Existenz des Quotienten gibt es keine unabhängige Charakterisierung. Man setzt fest:

Definition 32. *Es seien m und n natürliche Zahlen. Man nennt m ein Vielfaches von n , wenn es eine natürliche Zahl k gibt, so dass $n \cdot k = m$. Man nennt n einen Teiler von m und sagt, m sei durch n teilbar, wenn m ein Vielfaches von n und außerdem $n \neq 0$ ist. Als Abkürzung schreibt man $n \mid m$ (gelesen „ n teilt m “).*

²⁰In englischsprachigen Ländern schreibt man den Quotienten als $m \div n$, und das entsprechende Zeichen findet man auch auf den meisten Taschenrechnern.

Der Quotient $m : n$ existiert also genau dann, wenn $n \mid m$. Zahlen, die durch 2 teilbar sind, nennt man auch gerade Zahlen, alle anderen natürlichen Zahlen heißen ungerade.

Für die Subtraktion und die Division gelten neben den offensichtlichen Folgerungen aus der Definition

$$m - 0 = m, \quad m - m = 0, \quad m : 1 = m, \quad m : m = 1$$

weitere Rechengesetze, z. B. die Assoziativgesetze der Subtraktion und der Division sowie weitere Distributivgesetze.

Satz 33. *Es seien l, m und n natürliche Zahlen. Ist $n \geq l$, so gilt*

$$(m + n) - l = m + (n - l), \quad m \cdot (n - l) = m \cdot n - m \cdot l.$$

Ist n durch l teilbar, so gilt

$$(m \cdot n) : l = m \cdot (n : l).$$

Sind m und n durch l teilbar, so gilt

$$(m + n) : l = m : l + n : l.$$

Beweis. Wir beweisen das erste dieser Gesetze. Ist $n \geq l$, so gibt es nach Satz 25 eine natürliche Zahl k , so dass $l + k = n$. Nach Definition der Differenz ist nun $k = n - l$, und wegen der Kommutativität und Distributivität der Addition gilt

$$(m + k) + l = m + (k + l) = m + (l + k) = m + n.$$

Daraus folgt nach Definition der Differenz, dass

$$(m + n) - l = m + k.$$

Setzen wir hier den Ausdruck für k ein, so folgt das Assoziativgesetz der Subtraktion.

Ersetzt man im obigen Beweis überall „+“ durch „·“ und „-“ durch „:“, so erhält man den Beweis des Gesetzes $(m \cdot n) : l = m \cdot (n : l)$.

Die anderen Gesetze sind in einer Übungsaufgabe zu beweisen. □

Um für gegebene natürliche Zahlen m und $n \neq 0$ anhand der Definition festzustellen, ob m durch n teilbar ist, müsste man theoretisch alle natürlichen Zahlen k daraufhin prüfen, ob $k \cdot n = m$ ist. Das ist praktisch unmöglich. Zum Glück folgt aus $n \geq 1$ nach Satz 21, dass $k \cdot n \geq k$, also

kommen für k sowieso nur die natürlichen Zahlen in Frage, die nicht größer als m sind.

Man kann sich die Arbeit weiter erleichtern, indem man die *Division mit Rest* benutzt. Man subtrahiert dazu die Zahl n so oft von m , wie es geht. Bleibt kein Rest, so „geht die Division auf“. Dass dieses Verfahren immer zum Ende kommt, wird durch Satz 30 begründet, den wir jetzt noch verfeinern.

Satz 34. *Sind m und $n \neq 0$ beliebige natürliche Zahlen, dann gibt es eindeutig bestimmte natürliche Zahlen q und r , so dass*

$$m = q \cdot n + r \quad \text{und} \quad r < n.$$

(Man nennt q den abgerundeten Quotienten und r den Rest bei der Division von m durch n .)

Beweis. Die Existenz von q und r wurde bereits in Satz 30 bewiesen. Nun zur Eindeutigkeit. Angenommen, die natürlichen Zahlen q' und r' haben ebenfalls die Eigenschaften

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

Dann ist

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

bzw. aufgrund der Kommutativität

$$r + q \cdot n = r' + q' \cdot n.$$

Wegen der Totalität muss $q \leq q'$ oder $q' \leq q$ sein²¹. Es genügt, den ersten Fall zu betrachten. Laut Definition der Differenz ist

$$r = (r' + q' \cdot n) - q \cdot n,$$

und nach Satz 33 und Kommutativgesetz

$$r = r' + (q' \cdot n - q \cdot n) = r' + (q' - q) \cdot n.$$

Angenommen, es ist $q' - q \neq 0$. Dann wäre $q' - q \geq 1$, also nach Satz 21

$$(q' - q) \cdot n \geq 1 \cdot n, \quad r' + (q' - q) \cdot n \geq r' + n.$$

Nach Satz 20 ist $r' + n \geq n$, und wegen der Transitivität würde $r \geq n$ folgen, was den Voraussetzungen widerspricht. Also ist die Annahme falsch, und es muss $q' - q = 0$ sein. Durch Einsetzen folgt $r = r'$, und nach Definition der Differenz ist $q' = q$. \square

²¹Diese Fallunterscheidung ist geschickter als die nach r und r' .

3.5 Rekursive Definition

Beispiel. In der Schule wird die Potenz nicht wie in Definition 17 als Anzahl von Abbildungen eingeführt, weil das die Schüler überfordern würde. Statt dessen schreibt man etwa

$$m^k \stackrel{\text{def}}{=} \underbrace{m \cdot m \cdot \dots \cdot m}_{k \text{ Faktoren}},$$

wobei m und k natürliche Zahlen bezeichnen. Die Abkürzung „def“ über oder unter dem Gleichheitszeichen soll besagen, dass links ein noch undefinierter Ausdruck steht und rechts, was damit gemeint ist.²² Wir werden diese Schreibweise nicht benutzen, sondern im Text vermerken, wenn es sich um eine Definition handelt.

Dass die obige Definition der Potenz unbefriedigend ist, merkt man spätestens, wenn man ein Computerprogramm schreiben will, das nach jeder Eingabe von Zahlen m und k die Potenz m^k berechnet. Dann muss man die Rechenschritte vorgeben, deren Anzahl aber vorher nicht bekannt ist. Zum Glück sehen diese Schritte alle gleich aus: Man beginnt mit

$$m^0 = 1$$

und schreitet von einer Potenz zur nächsten immer mit Hilfe der selben Formel fort:

$$m^{n+1} = m^n \cdot m$$

Diese beiden Gleichungen bilden eine sogenannte rekursive Definition.

Beispiel. Mit der Zahl $n!$ (gelesen „ n Fakultät“, auf Englisch „ n factorial“) ist Folgendes gemeint:

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n.$$

Auch hier ist die Formel unbefriedigend, weil sie für $n \leq 3$ nicht stimmt und weil man genauer sagen müsste, was mit den Auslassungspunkten gemeint ist. Legt man aber fest, dass

$$0! = 1, \quad (n+1)! = n! \cdot (n+1) \quad \text{für alle } n \in \mathbf{N},$$

so hat man alle Informationen zur Berechnung für beliebig große n .

Beispiel. Haben sich Kinder im Kreis aufgestellt, so wird beim Aufsagen eines Abzählreims bei einem Kind a begonnen und bei jeder folgende Silbe zum linken Nachbarn übergegangen. Nummeriert man die Silben durch, so wird jeder natürlichen Zahl n ein Kind zugeordnet.

²²Anstelle von $\stackrel{\text{def}}{=}$ wird unter dem Einfluss der Informatik auch $:=$ geschrieben.

In den drei betrachteten Beispielen wird jeweils einer natürlichen Zahl nach der anderen ein Element einer gegebenen Menge M zugeordnet. Um von einer Abbildung $g : \mathbf{N} \rightarrow M$ zu sprechen, muss aber die gesamte Zuordnung gewissermaßen sofort gegeben sein. Dass diese Abbildung g existiert, folgt aus

Satz 35 (Rekursionssatz). *Es sei $f : M \rightarrow M$ eine Abbildung einer Menge in sich selbst. Ist a ein Element von M , so gibt es genau eine Abbildung $g : \mathbf{N} \rightarrow M$, so dass $g(0) = a$ ist und für alle $n \in \mathbf{N}$ gilt*

$$g(n+1) = f(g(n)). \quad (2)$$

Beweis. Es genügt, den Graphen der Abbildung g zu finden. Dazu betrachten wir die Abbildung h der Menge $\mathbf{N} \times M$ in sich selbst, die durch

$$h((n, y)) = (n+1, f(y))$$

gegeben ist, und bezeichnen den h -Abschluss der Einermenge $\{(0, a)\}$ mit G .

Es sei K die Menge aller $n \in \mathbf{N}$, für die es ein $y \in M$ gibt, so dass $(n, y) \in G$. Wegen $(0, a) \in G$ ist $0 \in K$. Wegen der Abgeschlossenheit von G unter h ist mit (n, y) auch $h((n, y)) \in G$, das heißt $(n+1, f(y)) \in G$ und somit $n+1 \in K$. Also hat K die beiden Eigenschaften aus Satz 29, und es folgt $K = \mathbf{N}$.

Es sei L die Menge aller $n \in \mathbf{N}$, für die es nur ein $y \in M$ mit der Eigenschaft $(n, y) \in G$ gibt. Ist $(0, y) \in G \setminus \{(0, a)\}$, dann gibt es nach Lemma 1 ein $(m, z) \in G$, so dass $h((m, z)) = (0, y)$, also $m+1 = 0$, was unmöglich ist. Somit ist $0 \in L$. Wir wollen zeigen, dass für $n \in L$ auch $n+1 \in L$ ist. Angenommen, es gibt $t \in M$ und $u \in M$, so dass $(n+1, t) \in G$ und $(n+1, u) \in G$. Nach Lemma 1 muss es wegen $n+1 \neq 0$ Paare $(k, v) \in G$ und $(l, w) \in G$ geben, so dass

$$(n+1, t) = h((k, v)), \quad (n+1, u) = h((l, w)),$$

mit anderen Worten,

$$n+1 = k+1, \quad t = f(v), \quad n+1 = l+1, \quad u = f(w).$$

Nach Satz 32 ist $n = k$ und $n = l$, und wegen $n \in L$ ist $v = w$, also $t = u$. Damit haben wir bewiesen, dass auch $n+1 \in L$ ist. Somit hat L die beiden Eigenschaften aus Satz 29, so dass $L = \mathbf{N}$ ist.

Die Menge G hat also alle charakteristischen Eigenschaften eines Graphen und definiert somit eine Abbildung $g : \mathbf{N} \rightarrow M$. Wegen $(0, a) \in G$ ist $g(0) = a$. Ist nun $(n, y) \in G$, also

$$y = g(n),$$

so ist auch $(n+1, f(y)) \in G$, also

$$f(y) = g(f(n)).$$

Setzen wir die eine Gleichung in die andere ein, so folgt die im Satz geforderte Eigenschaft von g .

Durch Umkehrung des letzten Schlusses sieht man, dass der Graph einer Abbildung g mit den geforderten Eigenschaften das Paar $(0, a)$ enthalten und abgeschlossen unter h sein muss. Er muss also G enthalten, kann aber als Graph keine weiteren Punkte enthalten. \square

Will man aus der sogenannten Rekursionsformel (2) eine Formel für, sagen wir, $g(100)$ gewinnen, so muss man schreiben

$$g(100) = f(g(99)).$$

Auf der rechten Seite kommt aber wieder die unbekannte Abbildung g vor, und setzt man dafür die gegebene Definition ein, so erhält man

$$g(100) = f(f(g(98))).$$

Fährt man so fort, dann gelangt man schließlich zu $g(0)$, wofür man den vorgegebenen Wert a einsetzen kann. Aus diesem Grund spricht man von einer *rekursiven* (lat. rückläufigen) Definition.

Nun wollen wir den Satz auf die eingangs angeführten Beispiele anwenden. Im ersten Beispiel hält man m fest und betrachtet $f(x) = x \cdot m$, im dritten Beispiel ist $f(x)$ der linke Nachbar von x . Im zweiten Beispiel ist der Satz nicht unmittelbar anwendbar. Man kann aber eine Abbildung f der Menge $\mathbf{N} \times \mathbf{N}$ in sich selbst durch

$$f(x, n) = (x \cdot (n + 1), n + 1)$$

definieren. Der Satz liefert dann die Abbildung $g(n) = (n!, n)$, und man braucht sie nur noch mit der Abbildung $h(x, n) = x$ zu verketteten.

Wenn man wie in der Schule die Potenz rekursiv definiert, muss man auch die Potenzgesetze unter Benutzung dieser Definition beweisen. Aussagen über rekursiv definierte Objekte werden meist durch vollständige Induktion bewiesen.

Beispiel. Wir beweisen das erste Potenzgesetz

$$(l \cdot m)^n = l^n \cdot m^n$$

für natürliche Zahlen l , m und n durch vollständige Induktion nach n . Es gilt für $n = 0$, weil alle nullten Potenzen gleich 1 sind. Angenommen, das Potenzgesetz gilt für eine natürliche Zahl n . Nach Definition ist

$$(l \cdot m)^{n+1} = (l \cdot m)^n \cdot (l \cdot m).$$

Nach Induktionsvoraussetzung ist hier die rechte Seite gleich

$$l^n \cdot m^n \cdot l \cdot m,$$

wobei wir die Klammern wegen des Assoziativgesetzes weglassen. Dieser Ausdruck ist aufgrund des Kommutativgesetzes gleich

$$l^n \cdot l \cdot m^n \cdot m,$$

und laut Definition der Potenz ist dies gleich

$$l^{n+1} \cdot m^{n+1}.$$

Wir haben also die Induktionsbehauptung

$$(l \cdot m)^{n+1} = l^{n+1} \cdot m^{n+1}$$

bewiesen.

Man kann auch Potenzen von Abbildungen f einer Menge M in sich selbst rekursiv definieren:

$$f^0 = \text{id}_M, \quad f^{n+1} = f \circ f^n \quad \text{für alle } n \in \mathbf{N}. \quad (3)$$

Es gelten die Potenzgesetze, nämlich

$$f^{m+n} = f^m \circ f^n, \quad f^{m \cdot n} = (f^m)^n.$$

Wenn f und g miteinander kommutieren, d. h. wenn $f \circ g = g \circ f$, so gilt auch

$$(f \circ g)^n = f^n \circ g^n.$$

Die Beweise sind wörtliche Kopien der Beweise für natürliche Zahlen unter Benutzung von Satz 4.

Will man Potenzen einer Menge M definieren, so beginnt man üblicherweise²³ bei $n = 1$:

$$M^1 = M, \quad M^{n+1} = M^n \times M \quad \text{für alle } n \in \mathbf{N} \setminus \{0\}.$$

Auch hier gelten Potenzgesetze, nämlich

$$(M \times N)^n \sim M^n \times N^n, \quad M^{m+n} \sim M^m \times M^n, \quad M^{m \cdot n} \sim (M^m)^n.$$

Die Beweise sind wieder analog zu denen für natürliche Zahlen und verwenden Satz 12. Analog zu Tripeln (x, y, z) definiert man Quadrupel (w, x, y, z) , Quintupel, Sextupel, Septupel, Oktupel usw., deren Namen man mit lateinischen Ordnungszahlwörtern bildet, und allgemein spricht man von n -Tupeln.

Häufig reichen die Buchstaben des Alphabets nicht aus, um alle Objekte in einer mathematischen Argumentation zu bezeichnen. Dann verwendet man denselben Buchstaben mehrmals und fügt zur Unterscheidung Indizes²⁴ an. So könnte man ein n -Tupel z. B. mit (x_1, x_2, \dots, x_n) bezeichnen.

²³Man könnte mit M^0 eine Einermenge bezeichnen, z. B. $\{\emptyset\}$.

²⁴Die Mehrzahl des lateinischen Wortes *index* ist *indices*.

Angenommen, wir haben die Variablen x_i für gewisse Indizes i mit Werten belegt. Die besagten Indizes bilden eine Teilmenge M von \mathbf{N} , und die Werte gehören zu einer Menge N . Dann haben wir faktisch jedem Element i von M ein Element x_i von N zugeordnet, also eine Abbildung $g : M \rightarrow N$ definiert, nämlich $g(i) = x_i$. Ist insbesondere $M = \{m, m+1, m+2, \dots, n\}$ ein Abschnitt der natürlichen Zahlen, so bilden die Zahlen $x_m, x_{m+1}, x_{m+2}, \dots, x_n$ eine Folge. Wir sehen also, dass man eine Folge auch als Abbildung verstehen kann. So lässt sich eine unendliche Folge x_0, x_1, x_2, \dots auch als Abbildung $g : \mathbf{N} \rightarrow M$ interpretieren.

In diesem Sinne kann man Folgen rekursiv definieren (vgl. Aufgabe 35). Die Folge der Fibonaccizahlen ist wie folgt definiert:

$$x_0 = 1, \quad x_1 = 1, \quad x_{n+2} = x_n + x_{n+1} \quad \text{für alle } n \in \mathbf{N}.$$

Um auch dies durch Satz 35 zu rechtfertigen, müsste man z. B. die durch $f(x, y) = (y, x + y)$ definierte Abbildung der Menge $\mathbf{N} \times \mathbf{N}$ in sich selbst betrachten und die aus dem Anfangswert $(1, 1)$ resultierende Abbildung $g : \mathbf{N} \rightarrow \mathbf{N} \times \mathbf{N}$ mit der Abbildung $h(x, y) = x$ verketteten.

Wir wollen nun Summen- und Produktzeichen einführen. In einem Ausdruck wie $x + y + z$, in dem x, y und z natürliche Zahlen bedeuten, brauchen wir wegen des Assoziativgesetzes keine Klammern zu setzen. Es ist klar, was mit einem Ausdruck wie

$$x_7 + x_8 + x_9 + \dots + x_{235} + x_{236}$$

gemeint ist. Wegen der Mehrdeutigkeit der Auslassungspunkte und aus Platzgründen benutzt man die Abkürzung

$$\sum_{i=7}^{236} x_i,$$

gelesen „Summe der x_i für i von 7 bis 236“. Die Variable i nennt man Summationsindex; hier kann man jede Variable benutzen, die in dieser Summe nicht anderweitig belegt ist. Es gilt also z. B.

$$\sum_{i=7}^{236} x_i = \sum_{r=7}^{236} x_r.$$

Die Zahlen 7 und 236 nennt man die untere bzw. obere Summationsgrenze. Genauso kürzt man Produkte ab, z. B.

$$x_{17} \cdot x_{18} \cdot x_{19} \cdot \dots \cdot x_{83} \cdot x_{84} = \prod_{j=17}^{84} x_j.$$

Das Summenzeichen und das Produktzeichen sind die großen griechischen Buchstaben Sigma und Pi.

Ähnlich wie bei Potenz und Fakultät muss eine logisch einwandfreie Definition auch hier rekursiv sein. Man definiert also

$$\sum_{i=m}^m x_i = x_m, \quad \sum_{i=m}^{n+1} x_i = \left(\sum_{i=m}^n x_i \right) + x_{n+1} \quad \text{für } n \geq m,$$

$$\prod_{i=m}^m x_i = x_m, \quad \prod_{i=m}^{n+1} x_i = \left(\prod_{i=m}^n x_i \right) \cdot x_{n+1} \quad \text{für } n \geq m.$$

Mitunter verwendet man diese Bezeichnungen auch, wenn $m > n$ ist, in diesem Fall ist

$$\sum_{i=m}^n x_i = 0, \quad \prod_{i=m}^n x_i = 1.$$

Satz 36. Für alle natürlichen Zahlen $m \leq n < p$ und $k \geq 1$ gelten die Assoziativgesetze

$$\sum_{i=m}^n x_i + \sum_{i=m}^n y_i = \sum_{i=m}^n (x_i + y_i), \quad \sum_{i=m}^n x_i + \sum_{i=n+1}^p x_i = \sum_{i=m}^p x_i,$$

und die Substitutionsregeln

$$\sum_{i=m}^n x_{i+k} = \sum_{j=m+k}^{n+k} x_j, \quad \sum_{i=1}^k x_i = \sum_{j=0}^{k-1} x_{k-j}.$$

Wenn $x_i \leq y_i$ für alle i mit der Eigenschaft $m \leq i \leq n$ ist, dann gilt

$$\sum_{i=m}^n x_i \leq \sum_{i=m}^n y_i.$$

Es gelten die analogen Aussagen für das Produktzeichen sowie das Distributivgesetz

$$a \cdot \sum_{i=m}^n x_i = \sum_{i=m}^n a \cdot x_i.$$

Die hier vorkommenden Variablen x_i und a bezeichnen natürliche Zahlen.

Beweis. Wir beweisen das zweite Assoziativgesetz für das Summenzeichen durch vollständige Induktion nach n beginnend mit $n = m + 1$, also mit der Aussage

$$\sum_{i=l}^m x_i + \sum_{i=m+1}^{m+1} x_i = \sum_{i=l}^{m+1} x_i.$$

Dies ist nichts anderes als die rekursive Definition, denn die zweite Summe auf der linken Seite ist nach Definition gleich x_{m+1} .

Nun nehmen wir an, dass die Behauptung für eine Zahl n gilt, und formen die linke Seite der Induktionsbehauptung mit Hilfe der rekursiven Definition um:

$$\sum_{i=l}^m x_i + \sum_{i=m+1}^{n+1} x_i = \sum_{i=l}^m x_i + \left(\sum_{i=m+1}^n x_i + x_{n+1} \right).$$

Aufgrund des Assoziativgesetzes und der Induktionsvoraussetzung ist dies gleich

$$\left(\sum_{i=l}^m x_i + \sum_{i=m+1}^n x_i \right) + x_{n+1} = \sum_{i=l}^n x_i + x_{n+1},$$

und durch eine weitere Anwendung der rekursiven Definition wird dies zur rechten Seite der Induktionsbehauptung.

Nun beweisen wir die zweite Substitutionsregel. Für $k = 1$ wird sie zur Behauptung $x_1 = x_1$. Nun nehmen wir an, dass sie für eine Zahl $k \geq 1$ gilt. Nach der Definition des Summenzeichens und der Induktionsvoraussetzung ist

$$\sum_{i=1}^{k+1} x_i = \sum_{i=1}^k x_i + x_{k+1} = \sum_{j=0}^{k-1} x_{k-j} + x_{k+1}.$$

Wir behaupten, dass der Index $k - j$ gleich $(k + 1) - (j + 1)$ ist. In der Tat gilt nach dem Assoziativgesetz der Addition und der Definition der Differenz

$$(k - j) + (j + 1) = ((k - j) + j) + 1 = k + 1,$$

und nach der selben Definition folgt die Behauptung. Damit ergibt sich

$$\sum_{j=0}^{k-1} x_{k-j} = \sum_{j=0}^{k-1} x_{(k+1)-(j+1)},$$

und nach der ersten Substitutionsregel (die in einer Übungsaufgabe zu beweisen ist) ist dies gleich

$$\sum_{j=0+1}^{(k-1)+1} x_{(k+1)-j}.$$

(Zum besseren Verständnis könnte man hier die Bezeichnung $y_j = x_{(k+1)-j}$ verwenden.) Fassen wir zusammen, so erhalten wir

$$\sum_{i=1}^{k+1} x_i = x_{k+1} + \sum_{j=1}^k x_{(k+1)-j} = \sum_{j=0}^k x_{(k+1)-j},$$

wobei wir erst das Kommutativgesetz und im letzten Schritt das erste Assoziativgesetz für das Summenzeichen benutzt haben.

Die anderen Behauptungen sind in Übungsaufgaben zu beweisen. \square

3.6 Stellenwertsysteme

Natürliche Zahlen kann man einfach dadurch aufzuschreiben, dass man so viele Striche zeichnet, wie die Zahl angibt. Dies wird übersichtlicher, wenn man die Zeichen bündelt, wie es noch heute bei Strichlisten üblich ist, z. B.

‖‖‖ ‖‖‖ ‖‖‖

Eine platzsparendere Variante haben die Maya erfunden, die die selbe Zahl so notierten:

⋮

Die Wahl der Bündelgröße ist offenbar durch die Anzahl der Finger einer Hand motiviert. Nimmt man beide Hände, so kommt man auf Zehnerbündel, aber hier hat man aus Gründen der Übersichtlichkeit meist neue Zeichen erfunden, unter anderem in Indien und China. Hier findet man z. B. die chinesischen Zahlzeichen.

Bei großen Zahlen ist das Bündeln allein kaum eine Erleichterung, aber man kann die Bündel wiederum bündeln. Auf dem Rechenbrett wurde die Anzahl der Bündel durch die Anzahl der Steinchen (lat. *calculus*, Mz. *calculi*) in nebeneinanderliegenden Feldern wiedergegeben: Im rechten Feld die Anzahl der Einer, links daneben die Anzahl der Bündel, wieder links daneben die Anzahl der Bündel von Bündeln usw. Die Sumerer bildeten z. B. Zehnerbündel, fassten je sechs davon zu einem Bündel zusammen, von diesen wiederum zehn, davon wiederum sechs usw. Daher stammt die Einteilung der Stunde in 60 Minuten.

In allen Sprachen gibt es spezielle Wörter für die Bündel, z. B. zehn, hundert, tausend.²⁵ Im Chinesischen werden Wörter allgemein durch je ein Zeichen notiert, aber für diese Zeichen hat man vereinfachte Versionen eingeführt. Damit kann man problemlos alle Zahlen kleiner als einhunderttausend bezeichnen. Die Maya bildeten auf jeder Ebene Zwanzigerbündel, deren Anzahl sie mit Hilfe der Zeichen . bis \equiv notierten. Diese Zeichen werden mit etwas Abstand untereinander geschrieben, wobei die Einerstelle zuunterst steht.

²⁵Die Wörter Million (Vergrößerungsform von *mille*=tausend), Billion, Trillion, Quadrillion usw. haben wir aus dem Französischen übernommen, die dazwischengeschobenen Stufen Milliarde, Billiarde usw. sind übrigens in den USA unbekannt.

Manche Kulturen (z. B. die babylonische und die chinesische) ließen oft die Zeichen für die Bündel weg, was natürlich zu Verwechslungen führte. Nur drei Kulturen (die sumerisch-babylonische, die indische und die der Maya) hatten die durchschlagende Idee, ein spezielles Zeichen für ein leeres Feld einzuführen: In Babylon war dies ein bloßes Trennzeichen, aber in Indien bedeutete ein leerer Kreis bereits „śūnya“, das heißt „nichts“ bzw. auf lateinisch „nullum“. Die Maya benutzten für eine fehlende Stelle das stilisierte Bild einer leeren Muschel.

Die indischen Zahlen sind über Arabien nach Europa gekommen, wobei sich in der arabischen Welt letztlich die ostarabischen Ziffern durchgesetzt haben.

ostarabisch:	•	∖	ʿ	ʿ	ξ	Ϟ	ʿ	∧	ϙ	
westarabisch:	0	1	2	3	4	5	6	7	8	9

Aus der arabischen Übersetzung „sifr“ des Wortes „śūnya“ entstanden durch Missverständnisse die Worte „Ziffer“ und „Chiffre“.

In Zahlssystemen mit einer Null braucht man keine Zeichen für Bündel mehr, sondern der Wert eines Zeichens ergibt sich aus seiner Stellung. Darum spricht man von *Stellenwertsystemen*, und die Bündelgröße nennt man *Grundzahl*. Jede Grundzahl größer als 1 ist möglich, und dem Wort „System“ wird das entsprechende lateinische²⁶ oder griechische²⁷ Adjektiv vorangestellt:

<i>Grundzahl</i>	<i>lateinisch</i>	<i>griechisch</i>
2	binär, dual	dyadisch
3	ternär	triadisch
4	quaternär	tetradisch
5	quinär	pentadisch
6	senär	hexadisch
7	septenär	heptadisch
8	oktal	oktadisch
9	nonär	nonadisch
10	dezimal	dekadisch
16	sedezimal ²⁸	hexadekadisch
20	vigesimal	ikosadisch
60	sexagesimal	hexakontadisch
:		:
<i>g</i>		<i>g</i> -adisch

²⁶Die Endungen sind z. T. dem Französischen angeglichen.

²⁷Die Endungen sind dem Deutschen angeglichen.

Im g -adischen Zahlensystem benötigt man g verschiedene Zeichen, genannt Ziffern. Für Computer ist die Grundzahl zwei besonders geeignet. In Programmiersprachen benutzt man auch die Grundzahlen zwölf und (früher) acht.²⁹ Beim Hexadezimalsystem verwendet man zusätzlich zu den Dezimalziffern meist die Ziffern A = 10, B = 11, ..., F = 15.

Das System der Sumerer ist kein Stellenwertsystem im eigentlichen Sinne. Man kann es aber als Sexagesimalsystem interpretieren, indem man immer zwei benachbarte Ziffern zu einem Zeichen zusammenfasst. Ähnliche Systeme mit unterschiedlichen Bündelgrößen entstehen jedesmal, wenn Einheiten in eine Anzahl kleinerer Einheiten unterteilt werden, die nicht mit der Grundzahl verträglich ist.

- In heutigen Zeitangaben wie 2:17:48, z. B. im Sport, folgen wir den Sumerern und teilen die Stunde in sechzig Minuten und die Minute in sechzig Sekunden ein, wir haben also immer noch zwei Sechserziffern (in unserem Beispiel 1 und 4). Bei mehrstelligen Stundenangaben benutzen wir aber nur Dezimalziffern.
- Man kann das Zahlensystem der Maya als gemischtes Stellenwertsystem verstehen, in dem sich Fünferziffern (notiert durch Punkte) und Viererziffern (notiert durch Balken) abwechseln. In jeder Zweiergruppe ist allerdings die Reihenfolge vertauscht.
- Die Maya hatten Monate zu zwanzig Tagen, also achtzehn Monate im Jahr (plus fünf Unglückstage). Bei der Angabe eines Datums war dadurch die vorletzte Ziffer eine Achtzehnerziffer.
- Bis 1971 war das Britische Pfund in zwanzig Schillinge unterteilt und ein Schilling in zwölf Pfennige (pence, abgekürzt d für *denarius*).

Wir wollen nun untersuchen, wie und warum Stellenwertsysteme funktionieren. Dabei betrachten wir der Einfachheit halber nur reine und keine gemischten Stellenwertsysteme. Vorab eine Bemerkung. Es hat sich in der Mathematik eingebürgert, in Produkten die Zahlen vor den Variablen anzuordnen und das Multiplikationszeichen nur zwischen Zahlen zu schreiben. Letzteres hat zur Folge, dass (im Unterschied zur Informatik) Variablen nur aus einem Buchstaben bestehen dürfen. Auch wir werden diesem Brauch folgen.

²⁸In der Informatik hat sich das griechisch-lateinische Mischwort *hexadezimal* durchgesetzt.

²⁹Dort man macht solche Zahlen z. B. durch ein vorangestelltes 0x bzw. 0 kenntlich.

Satz 37. *Es sei $g > 1$ eine natürliche Zahl. Unter einer Ziffer zur Grundzahl g verstehen wir eine natürliche Zahl kleiner als g . Zu jeder natürlichen Zahl n gibt es eindeutig bestimmte Ziffern c_0, c_1, \dots , von denen nur endlich viele³⁰ nicht Null sind, so dass*

$$n = c_0 + c_1g + c_2g^2 + \dots$$

Man könnte die Summe an einer Stelle abbrechen, nach der nur noch Nullen folgen. Es ist aber bequemer, sich das Nachdenken darüber zu ersparen, an welcher Stelle das genau geschieht. Man notiert Zahlen in Stellenwertsystemen durch die Folge ihrer von Null verschiedenen Ziffern, beginnend mit der Stelle von höchstem Wert. Wenn man will, kann man links beliebig viele Nullen anfügen, was man mitunter wegen des einheitlichen Aussehens tut, z. B. bei Tagesdaten wie 04.12.2008 oder Listeneinträgen wie 007.

Beispiel. Um die im Dezimalsystem geschriebene Zahl 625 ins ternäre System umzuwandeln, dividieren wir entsprechend Satz 34 fortgesetzt durch 3:

$$\begin{aligned} 625 &= 208 \cdot 3 + 1 \\ 208 &= 69 \cdot 3 + 1 \\ 69 &= 23 \cdot 3 + 0 \\ 23 &= 7 \cdot 3 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 0 \cdot 3 + 2 \end{aligned}$$

Setzen wir jeweils eine Zeile in die vorhergehende ein, so erhalten wir³¹

$$\begin{aligned} 625 &= (((((2 \cdot 3 + 1) \cdot 3 + 2) \cdot 3 + 0) \cdot 3 + 1) \cdot 3 + 1) \cdot 3 + 1 \\ &= 2 \cdot 3^5 + 1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3 + 1. \end{aligned}$$

Die Reste ergeben also die Ternärziffern. Wenn man Zahlen in verschiedenen Systemen gleichzeitig betrachtet, so muss man sie kenntlich machen, z. B. durch Anfügen der tiefgestellten Grundzahl:

$$625_{10} = 212011_3$$

Beweis von Satz 37. Entsprechend den Bemerkungen nach Satz 31 können wir annehmen, dass die Behauptung gilt, wenn wir n durch eine beliebige

³⁰Besser wäre es zu sagen, dass es ein k gibt, so dass $c_i = 0$ für alle i mit der Eigenschaft $i \geq k$ gilt.

³¹Für praktische Berechnungen ist die erste Zeile zu empfehlen, da sie mit weniger Multiplikationen auskommt. Man kann sie mit dem **Hornerschema** übersichtlich gestalten.

kleinere natürliche Zahl ersetzen. Nach Satz 34 gibt es natürliche Zahlen q und $r < g$, so dass

$$n = qg + r.$$

Nach Satz 25 ist $n \geq qg$, und nach Satz 21 ist wegen $g > 1$ auch $qg > q$. Aus der Transitivität folgt $n > q$, und nach Induktionsvoraussetzung gibt es Ziffern d_0, d_1, \dots , von denen nur endlich viele nicht Null sind, so dass

$$q = d_0 + d_1g + d_2g^2 + \dots$$

Wir erhalten durch Einsetzen und mit Hilfe des Distributivgesetzes

$$n = r + (d_0 + d_1g + d_2g^2 + \dots)g = r + d_0g + d_1g^2 + d_2g^3 + \dots$$

Also gilt die Behauptung auch für die Zahl n mit den Ziffern

$$c_0 = r, \quad c_1 = d_0, \quad c_2 = d_1, \quad c_3 = d_2, \quad \dots$$

Zum Beweis der Eindeutigkeit betrachten wir eine weitere Zifferndarstellung

$$n = c'_0 + c'_1g + c'_2g^2 + c'_3g^3 + \dots$$

und setzen

$$q' = c'_1 + c'_2g + c'_3g^2 + \dots$$

Dann gilt $n = q'g + c'_0$, und nach der Eindeutigkeitsaussage von Satz 34 ist $c_0 = c'_0$ und $q = q'$. Nach Induktionsvoraussetzung sind die Ziffern von q eindeutig bestimmt, also gilt $c_1 = c'_1, c_2 = c'_2, c_3 = c'_3, \dots$ \square

Der Gebrauch von Auslassungspunkten in Rechenausdrücken ist nicht ganz einwandfrei. Strenggenommen hätte man die im Satz behauptete Zifferndarstellung unter Benutzung des Summenzeichens schreiben müssen:

$$n = \sum_{i=0}^k c_i g^i,$$

wobei k eine genügend große natürliche Zahl ist, so dass $c_i = 0$ ist für alle i , die größer als k sind. Im Beweis erhält man aus der Induktionsvoraussetzung zunächst die Zifferndarstellung

$$q = \sum_{j=0}^l d_j g^j,$$

wobei l genügend groß ist. Einsetzen ergibt

$$n = r + \left(\sum_{j=0}^l d_j g^j \right) g.$$

Mit dem Distributivgesetz und der Substitutionsregel aus Satz 36 folgt

$$n = r + \sum_{j=0}^l d_j g^{j+1} = r + \sum_{i=1}^{l+1} d_{i-1} g^i,$$

und mit dem Assoziativgesetz aus dem selben Satz erhalten wir schließlich die behauptete Zifferndarstellung von n .

Um in einem Stellenwertsystem schriftlich zu rechnen, braucht man eine Additions- und eine Multiplikationstabelle (letztere auch „kleines Einmal-eins“ genannt). Wir wollen beispielsweise diese Tabellen für das Ternärsystem aufstellen. Die Rechnungen führen wir entweder durch Abzählen aus (entsprechend den Definitionen 14 und 15), oder wir machen eine Nebenrechnung im Dezimalsystem, wie wir es in der Schule (wenn auch ohne strenge Begründung) gelernt haben. Dann wandeln das Ergebnis nach dem obigen Verfahren ins Ternärsystem um. So ist z. B.

$$1 + 2 = 3_{10} = 10_3, \quad 2 + 2 = 2 \cdot 2 = 4_{10} = 11_3.$$

Wir erhalten folgende Tabellen, wobei wir die Zeilen und Spalten für die Ziffer 0 weglassen haben:

+	1	2
1	2	10
2	10	11

·	1	2
1	1	2
2	2	11

Wir haben uns auch erspart, jede Ternärzahl durch eine tiefgestellte 3 zu kennzeichnen.

Mit Hilfe dieser Tabellen kann man im Ternärsystem schriftlich addieren und multiplizieren, wie in der Schule gelernt:

$$\begin{array}{r}
 2\ 2\ 1\ 1\ 0\ 1 \cdot 2\ 1\ 2 \\
 \hline
 1\ 2\ 1\ 2\ 2\ 0\ 2 \\
 2\ 2\ 1\ 1\ 0\ 1 \\
 2\ 1\ 2\ 1\ 1\ 2\ 0\ 2 \\
 \hline
 2\ 1\ 0\ 1\ 2\ 1\ 1\ 1\ 2
 \end{array}$$

(Eigentlich gibt es keine allgemeine Methode zur schriftlichen Addition von mehr als zwei Zahlen. Man kann aber eine Zahl nach der anderen hinzufügen.) Wir erhalten somit

$$221101_3 \cdot 212_3 = 210121112_3.$$

Durch Rückverwandlung ins Dezimalsystem kann man die Probe machen:

$$685 \cdot 23 = 15755.$$

Für die nächste Überlegung benötigen wir die dritte binomische Formel: Sie besagt, dass für natürliche Zahlen $a \geq b$ und n gilt

$$a^n - b^n = (a - b) \sum_{i=1}^n a^{n-i} b^{i-1}.$$

Der Beweis ist Gegenstand einer Übungsaufgabe.

Wie kann man an der Zifferndarstellung zweier natürlicher Zahlen in einem Stellenwertsystem erkennen, welche von beiden die kleinere ist?

Satz 38. *Es seien n und n' natürliche Zahlen mit den Ziffernfolgen c_0, c_1, c_2, \dots und c'_0, c'_1, c'_2, \dots im g -adischen System. Es gilt genau dann $n < n'$, wenn es eine natürliche Zahl j gibt, so dass $c_j \neq c'_j$, und wenn für die größte solche Zahl j gilt $c_j < c'_j$.*

Da wir die Ziffern links mit Nullen auffüllen, benötigen wir keine Fallunterscheidung in Abhängigkeit von der Stellenzahl. Wir erinnern daran, dass jeweils nur endlich viele Ziffern von Null verschieden sind. Somit ist die Menge der Stellen, an denen sich die Ziffern zweier Zahlen unterscheiden, endlich. Sind die Zahlen verschieden, so ist diese Menge nach Satz 37 nicht leer und hat nach Aufgabe 27 ein größtes Element.

Beweis. Es sei $n \neq n'$. Dann gibt es also eine größte natürliche Zahl j , so dass $c_j \neq c'_j$ ist. Nach dem Assoziativgesetz aus Satz 36 ist

$$\begin{aligned} n &= \sum_{i=0}^{j-1} c_i g^i + \sum_{i=j}^{\infty} c_i g^i, \\ n' &= \sum_{i=0}^{j-1} c'_i g^i + \sum_{i=j}^{\infty} c'_i g^i, \end{aligned}$$

wobei wir zwar den Summationsindex i formal bis ∞ (gelesen „unendlich“) laufen lassen, aber in Wirklichkeit nur endlich viele Summanden von Null verschieden sind. Für alle i gilt $c_i \leq g - 1$ und $c'_i \geq 0$, also $c_i g^i \leq (g - 1)g^i$ und $c'_i g^i \geq 0$. Mit Satz 36 folgt

$$\begin{aligned} n &\leq \sum_{i=0}^{j-1} (g - 1)g^i + \sum_{i=j}^{\infty} c_i g^i, \\ n' &\geq \sum_{i=j}^{\infty} c'_i g^i. \end{aligned}$$

Ersetzen wir in der dritten binomischen Formel die Zahlen a , b und n durch g , 1 und j , so erhalten wir

$$(g-1) \sum_{i=1}^j g^{j-i} = g^j - 1,$$

was wir nach der zweiten Substitutionsregel aus Satz 36 auch so schreiben können:

$$(g-1) \sum_{i=0}^{j-1} g^i = g^j - 1,$$

Mit dem Assoziativgesetz aus dem selben Satz folgt

$$\sum_{i=0}^{j-1} (g-1)g^i = g^j - 1,$$

und mit Satz 21 und dem Assoziativgesetz aus Satz 36 folgt

$$n < g^j + \sum_{i=j}^{\infty} c_i g^i = (c_j + 1)g^j + \sum_{i=j+1}^{\infty} c_i g^i.$$

Ist $c_j < c'_j$, nach Aufgabe 26 also $c_j + 1 \leq c'_j$, so folgt mit Satz 36

$$n < c'_j g^j + \sum_{i=j+1}^{\infty} c_i g^i = \sum_{i=j}^{\infty} c'_i g^i \leq n',$$

also $n < n'$. Ist hingegen $c_j > c'_j$, so zeigt man analog, dass $n > n'$. □

Die Kleiner-Gleich-Relation auf \mathbf{N} entspricht also der abgewandelten lexikographischen Ordnung (im Sinne der Potenzierung von Ordinalzahlen, s. S. 49) auf der Menge der Ziffernfolgen, wenn wir diese als Abbildungen von \mathbf{N} in die Menge $\{0, 1, \dots, g-1\}$ der Ziffern auffassen.

Betrachten wir neben dem g -adischen auch das h -adische System, wobei h eine Potenz von g ist, sagen wir $h = g^k$, so können aus der g -adischen Darstellung

$$n = c_0 + c_1 g + c_2 g^2 + \dots$$

einer natürlichen Zahl leicht die h -adische Darstellung gewinnen. Wir fassen dazu immer k aufeinanderfolgende Terme zusammen und klammern die

höchstmögliche Potenz von g aus:

$$\begin{aligned}
 n = & (c_0 + c_1g + c_2g^2 + \dots + c_{k-1}g^{k-1}) \\
 & + (c_k + c_{k+1}g + c_{k+2}g^2 + \dots + c_{2k-1}g^{k-1})g^k \\
 & + (c_{2k} + c_{2k+1}g + c_{2k+2}g^2 + \dots + c_{3k-1}g^{k-1})g^{2k} \\
 & + \dots \\
 & + (c_{lk} + c_{lk+1}g + c_{lk+2}g^2 + \dots + c_{l(k-1)}g^{k-1})g^{lk} \\
 & + \dots
 \end{aligned}$$

Strenggenommen müsste man ein weiteres Gesetz für das Summenzeichen benutzen und schreiben

$$\sum_{i=0}^{\infty} c_i g^i = \sum_{l=0}^{\infty} \left(\sum_{j=0}^{k-1} c_{lk+(k-1)j} g^j \right) g^{lk}.$$

Nach einem Potenzgesetz ist $g^{lk} = h^l$, und nach der dritten binomischen Formel ist

$$\begin{aligned}
 c_{lk} + c_{lk+1}g + c_{lk+2}g^2 + \dots + c_{l(k-1)}g^{k-1} \\
 \leq (g-1)(1 + g + g^2 + \dots + g^{k-1}) = g^k - 1 < h,
 \end{aligned}$$

also eine h -adische Ziffer. Umgekehrt kann man aus der h -adischen Darstellung die g -adische gewinnen, indem man die h -adischen Ziffern im g -adischen System darstellt und die so gewonnenen Blöcke einfach hintereinanderschreibt. Das wird in der Informatik für $g = 2$ und $h = 8$ oder $h = 16$ angewendet sowie im täglichen Leben für $g = 10$ und $h = 1000$. So schreibt man z. B. eine Zahl im Dezimalsystem in der Form³² 13.527.849 und benennt beim Vorlesen praktisch ihre Ziffern im Tausendersystem.

3.7 Schriftliche Rechenverfahren

In der Schule macht man sich keine Gedanken, warum die schriftlichen Rechenverfahren funktionieren. Wir wollen sie nun begründen und ansatzweise verstehen, wie sie als Algorithmen in der arithmetisch-logischen Einheit eines Prozessors umgesetzt werden können.

Schriftliche Addition

Sind zwei natürliche Zahlen im g -adischen System gegeben, so können wir die Ziffern ihrer Summe nicht einfach dadurch ermitteln, dass wir ihre Ziffern

³²Im Englischen benutzt man statt der Punkte Kommas.

Stelle für Stelle addieren, weil die dabei entstehenden Zahlen nicht immer kleiner als g sind. Wir behaupten, dass die Summe zweier Ziffern a und b im g -adischen System höchstens zweistellig ist, also von der Form $c + ug$ mit Ziffern c und u , und dass $u \leq 1$ ist. Sind a_i und b_i die Ziffern an der i -ten Stelle, so ist der Beitrag zur Summe gleich

$$a_i g^i + b_i g^i = c_i g^i + u_i g^{i+1},$$

der Übertrag ist also zur $(i + 1)$ ten Stelle hinzuzufügen. Darum muss man mit der Einerstelle, also $i = 0$, beginnen und zu immer höheren Stellen fortschreiten. Nun müssen wir an einer Stelle aber bereits den Übertrag $u_i \leq 1$ von der vorhergehenden Stelle berücksichtigen und erhalten

$$a_i + b_i + u_{i-1} \leq (g - 1) + (g - 1) + 1 \leq 1 \cdot g + (g - 1).$$

Nach Satz 38 ist die Summe höchstens zweistellig, und es entsteht ein Übertrag $u_{i+1} \leq 1$ zur nächsthöheren Stelle. Wir haben praktisch durch vollständige Induktion bewiesen, dass an allen Stellen höchstens der Übertrag 1 auftreten kann.

Versucht man mehr als zwei Zahlen gleichzeitig zu addieren, so können beliebig große Überträge mit beliebig vielen Stellen entstehen, und es handelt sich dann nicht mehr um einen Algorithmus. Wenn man z. B. versucht, tausende von einstelligen Zahlen zu addieren, so hat man die Schwierigkeit durch das schriftliche Verfahren nicht verringert, sondern rechnet praktisch im Kopf. Der Ausweg, insbesondere für den Prozessor eines Computers, besteht darin, einen Summanden nach dem anderen zu einem Register zu addieren, das am Anfang die Zahl 0 und am Ende die Summe enthält.

Schriftliche Subtraktion

Wir bezeichnen die i te Ziffer des Minuenden m mit a_i und die i te Ziffer des Subtrahenden n mit b_i , wobei wir entsprechend Folgerung 10 natürlich $m \geq n$ voraussetzen. Im Fall $a_i \geq b_i$ entsteht der Beitrag $a_i g^i - b_i g^i$ zur Differenz. Andernfalls benutzt man die Tatsache, dass sich der Wert des Minuenden nicht ändert, wenn man seine nächsthöhere Ziffer um eins verringert (was den Minuenden um g^{i+1} verringert) und dafür die Zahl a_i um g erhöht. Dies nennt man die Borgetechnik. Sie versagt aber in dieser einfachen Form, wenn die zu verringernde Ziffer eine Null ist.

Geschickter ist die Erweiterungstechnik, die darauf beruht, dass eine Verringerung des Minuenden um g^{i+1} das Selbe bewirkt wie eine Vergrößerung des Subtrahenden um g^{i+1} . Bei Anwendung dieser Technik ist der Übertrag also der nächsthöheren Stelle des Subtrahenden zuzuschlagen. Wir behaupten, dass der Übertrag höchstens 1 sein kann. An der i ten Stelle ist bereits

ein Übertrag $u_i \leq 1$ von der $(i - 1)$ ten Stelle zu berücksichtigen. Dabei gibt es zwei Fälle.

Ist $a_i \geq b_i + u_i$, so erhalten wir als *ite* Ziffer der Differenz die Zahl $c_i = a_i - (b_i + u_i)$, die nicht größer als a_i , also kleiner als g ist, und es entsteht kein neuer Übertrag, d. h. $u_{i+1} = 0$. Dies tritt insbesondere ein, wenn $a_i > b_i$ ist. An der höchsten solchen Stelle j entsteht also kein neuer Übertrag, und nach Satz 38 stimmen wegen $m \geq n$ die Ziffern an allen höheren Stellen überein, so dass $c_i = 0$ für $i > j$ ist.

Ist hingegen $a_i < b_i + u_i$, so erhöhen wir a_i um g und dafür die nächsthöhere Stelle des Subtrahenden um 1. Als *ite* Ziffer der Differenz ergibt sich

$$c_i = (a_i + g) - (b_i + u_i) = a_i + (g - (b_i + u_i)),$$

was nach Satz 33 wohldefiniert ist. Außerdem gilt in diesem Fall $a_i + g < g + (b_i + u_i)$, so dass $c_i < g$ ist; wir erhalten also tatsächlich eine g -adische Ziffer. In diesem Fall pflanzt sich ein Übertrag $u_{i+1} = 1$ zur nächsthöheren Stelle fort.

Somit funktioniert das schriftliche Subtraktionsverfahren.

Schriftliche Multiplikation

Man zerlegt den zweiten Faktor (den Multiplikator) n in Terme der Form $b_j g^j$ und benutzt das Distributivgesetz. Damit wird die Multiplikation auf das Teilproblem zurückgeführt, den ersten Faktor (den Multiplizierten) m mit einer Zahl der Form $b g^j$ zu multiplizieren. Nach dem Assoziativgesetz kann man erst mit b und dann mit g^j multiplizieren, wobei der zweite Schritt eine Verschiebung der Ziffern um j Stellen nach links und das Auffüllen der freigewordenen Stellen mit Nullen bewirkt. Diese Nullen werden im Zwischenergebnis meist nicht mitgeschrieben.

Um nun den Multiplizierten m mit einer Ziffer b des Multiplikators zu vervielfachen, geht man stellenweise von rechts nach links vor. Wir behaupten, dass die auftretenden Überträge kleiner als $g - 1$ sind. Steht an der *iten* Stelle des Multiplizierten die Ziffer a_i , so liefert sie den Beitrag $a_i b g^i$. Kommt von der $(i - 1)$ ten Stelle bereits ein Übertrag $u_i < g - 1$ hinzu, so erhalten wir

$$a_i b + u_i < (g - 1)(g - 1) + (g - 1) = (g - 1)g,$$

und nach Satz 38 ist $a_i b + u_i = c_i + u_{i+1} g$ mit $c_i < g$ und $u_{i+1} < g - 1$. Damit ist unsere Behauptung durch vollständige Induktion bewiesen, und somit funktioniert das schriftliche Multiplikationsverfahren.

Bei mehrstelligem Multiplikator müsste man mehrmals verschiedene Überträge an die selbe Stelle des Multiplizierten schreiben. Deshalb behält man

die Überträge nur im Kopf. Außerdem sind die Produkte mb_jg^j zu addieren. Um einen Algorithmus zu erhalten, muss man eines dieser Produkte nach dem anderen berechnen und (entsprechend der Schlussbemerkung zur Addition) zu einem Register hinzufügen.

Schriftliche Division

Wir wollen eine natürliche Zahl m mit Rest durch eine natürliche Zahl n dividieren, d. h. natürliche Zahlen q und r mit den Eigenschaften

$$m = qn + r, \quad r < n$$

finden, die ja nach Satz 34 existieren. Dazu bestimmt man zunächst eine natürliche Zahl i mit der Eigenschaft

$$g^{i+1}n > m.$$

Da die Multiplikation mit g^i eine Verschiebung der g -adischen Stellen bewirkt, ist ein solches i leicht mit Hilfe von Satz 38 zu finden. (Natürlich wird man i möglichst klein wählen, aber das ist nicht unbedingt notwendig.) Als Nächstes bestimmt man den abgerundeten Quotienten c_i und den Rest r_i bei der Division von m durch $g^i n$, d. h.

$$m = c_i g^i n + r_i, \quad r_i < g^i n.$$

Wäre $c_i \geq g$, so hätten wir $m \geq g^{i+1}n + r_i \geq g^{i+1}n$ im Widerspruch zur Wahl von i . Somit gilt

$$c_i < g,$$

das heißt, c_i ist eine g -adische Ziffer. Wenden wir das selbe Verfahren auf den Rest r_i an, so können wir wegen $r_i < g^i n$ die Zahl i durch $i - 1$ ersetzen und finden

$$r_i = c_{i-1} g^{i-1} n + r_{i-1}, \quad r_{i-1} < g^{i-1} n.$$

Setzt man dies rekursiv fort, so kommt man schließlich bei $i = 0$ an, und durch Einsetzen findet man

$$m = (c_i g^i + \dots + c_0)n + r_0,$$

also

$$q = c_i g^i + \dots + c_0, \quad r = r_0.$$

Mit diesem Verfahren wird die Division von m durch n auf mehrere Divisionen durch Zahlen der Form ng^i zurückgeführt. Der Vorteil ist, dass hier als abgerundete Quotienten nur Werte kleiner als g in Frage kommen. Einen

besseren Algorithmus als die wiederholte Subtraktion haben wir dafür aber nicht. In der Praxis genügt bei einstelligen Divisoren n die Kenntnis des kleinen Einmaleins, bei mehrstelligen Divisoren errät man c_i durch einen Überblick, den man mitunter nachbessern muss. Bei Aufgaben wie $85472:17095$ bringt das schriftliche Divisionsverfahren überhaupt keine Erleichterung im Vergleich zum Kopfrechnen. Es gibt aber eine Grundzahl, bei der das Verfahren einen wirklichen Algorithmus darstellt, nämlich $g = 2$. In diesem Fall kommen für c_i nur die Zahlen 0 und 1 in Frage, und die Bestimmung von c_i läuft auf einen Vergleich an Hand von Satz 38 hinaus.

4 Ganze Zahlen

4.1 Operationen mit ganzen Zahlen

Es ist lästig, dass die Subtraktion natürlicher Zahlen nicht uneingeschränkt ausführbar ist. Diese Formulierung ist allerdings etwas irreführend, weil sie suggeriert, dass die Subtraktion existiere, wir sie aber nur nicht ausführen könnten. Gemeint ist, dass es nicht für beliebige natürliche Zahlen m und n eine eindeutig bestimmte natürliche Zahl k gibt, so dass $n + k = m$ ist.

Man erweitert den Bereich \mathbf{N} der natürlichen Zahlen zum Bereich \mathbf{Z} der ganzen Zahlen, in dem die bekannten Rechengesetze weiterhin gelten, aber die Subtraktion uneingeschränkt ausführbar ist. Die Frage, wie man einen solchen Zahlbereich konstruiert, wollen wir auf später verschieben.

Annahme 1. *Es gibt eine Menge \mathbf{Z} mit Operationen Addition und Multiplikation, so dass \mathbf{N} eine Teilmenge von \mathbf{Z} ist und dass die Rechenoperationen für ganze Zahlen, wenn wir sie auf natürliche Zahlen anwenden, mit den früher betrachteten Operationen übereinstimmen. Außerdem gelten für beliebige ganze Zahlen a , b und c die Kommutativ-, Assoziativ- und Distributivgesetze*

$$\begin{aligned} a + b &= b + a, & a \cdot b &= b \cdot a, \\ (a + b) + c &= a + (b + c), & (a \cdot b) \cdot c &= a \cdot (b \cdot c), \\ a \cdot (b + c) &= a \cdot b + a \cdot c. \end{aligned} \tag{4}$$

Schließlich gibt es für beliebige ganze Zahlen a und b genau eine ganze Zahl d , so dass

$$a = b + d.$$

Diese Zahl d bezeichnet man dann als Differenz von a und b , abgekürzt $a - b$.

Aus den genannten Rechengesetzen folgen automatisch weitere, nämlich die Assoziativ- und Distributivgesetze der Subtraktion:

$$\begin{aligned} (a + b) - c &= a + (b - c), & (a - b) - c &= a - (b + c), \\ (a - b) + c &= a - (b - c), & a \cdot (b - c) &= a \cdot b - a \cdot c. \end{aligned} \tag{5}$$

Der Beweis ist ähnlich wie für natürliche Zahlen, nur einfacher, weil man jetzt keine Bedingungen für die Existenz der Differenzen nachprüfen muss. Zum Beweis des zweiten Assoziativgesetzes bezeichnen wir $(a - b) - c$ mit d . Dann ist d nach Definition diejenige Zahl, für die gilt $a - b = c + d$. Dies bedeutet wiederum nach der Definition der Differenz, dass $a = b + (c + d)$. Dann gilt aber nach Assoziativgesetz der Addition $a = (b + c) + d$, also wiederum nach

der Definition der Differenz $d = a - (b + c)$, und durch Einsetzen erhalten wir das Gewünschte. Ähnlich beweist man die anderen Gesetze.

Mit Hilfe der Kommutativgesetze folgert man schließlich aus den angegebenen (linken) Distributivgesetzen die rechten Distributivgesetze

$$(b + c) \cdot a = b \cdot a + c \cdot a, \quad (b - c) \cdot a = b \cdot a - c \cdot a. \quad (6)$$

Wendet man die Rechenoperationen auf Differenzen von ganzen Zahlen an, so kann man das Ergebnis wieder als Differenz schreiben. Es gilt nämlich für beliebige ganze Zahlen a, b, c und d

$$\begin{aligned} (a - b) + (c - d) &= (a + c) - (b + d), \\ (a - b) - (c - d) &= (a + d) - (b + c), \\ (a - b) \cdot (c - d) &= (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c). \end{aligned} \quad (7)$$

Wir führen erst den Beweis im Fall der Subtraktion: Indem wir nacheinander das dritte und das zweite Assoziativgesetz der Subtraktion, das Kommutativitätsgesetz der Addition, das erste Assoziativitätsgesetz der Subtraktion und wieder das Kommutativitätsgesetz der Addition anwenden, erhalten wir

$$\begin{aligned} (a - b) - (c - d) &= ((a - b) - c) + d = (a - (b + c)) + d \\ &= d + (a - (b + c)) = (d + a) - (b + c) = (a + d) - (b + c). \end{aligned}$$

Nun kommen wir zum Beweis im Fall der Multiplikation. Nach den Distributivgesetzen der Subtraktion ist

$$(a - b) \cdot (c - d) = (a - b) \cdot c - (a - b) \cdot d = (a \cdot c - b \cdot c) - (a \cdot d - b \cdot d).$$

Dies ist nach der eben bewiesenen Formel für die Subtraktion gleich

$$(a \cdot c + b \cdot d) - (b \cdot c + a \cdot d),$$

und durch Anwendung des Kommutativgesetzes folgt die Behauptung.

Der Beweis im Fall der Addition ist Gegenstand einer Übungsaufgabe.

Der neue Zahlbereich \mathbf{Z} soll nicht unnötig groß sein.

Annahme 2. *Jedes Element der Menge \mathbf{Z} ist eine Differenz natürlicher Zahlen.*

Dies ist eigentlich keine einschränkende Bedingung. Angenommen, wir haben einen Zahlbereich \mathbf{Z} konstruiert, der die Annahme 1 erfüllt. Eine Teilmenge von \mathbf{Z} , die die Menge \mathbf{N} enthält und abgeschlossen³³ unter Addition, Multiplikation und Subtraktion ist, erfüllt ebenfalls die Annahme 1 und

³³Dieser Begriff der Abgeschlossenheit ist analog zu dem in Definition 23 betrachteten.

zusätzlich die Annahme 2. Die Rechengesetzen (4.1) zeigen, dass wir dafür die Menge aller Differenzen natürlicher Zahlen nehmen können.

Mit Hilfe von Annahme 2 können wir zeigen, dass für alle ganzen Zahlen a gilt

$$a + 0 = a, \quad a - 0 = a, \quad a \cdot 0 = 0, \quad a \cdot 1 = a$$

(und die analogen Gleichungen, die man mit den Kommutativgesetzen erhält). In der Tat, wir können $a = m - n$ für geeignete natürliche Zahlen m und n schreiben, und dann ist

$$(m - n) + 0 = m - (n - 0) = m - n, \quad (m - n) - 0 = m - (n + 0) = m - n, \\ (m - n) \cdot 0 = m \cdot 0 - n \cdot 0 = 0, \quad (m - n) \cdot 1 = m \cdot 1 - n \cdot 1 = m - n.$$

Die Definition der Differenz besagt im Spezialfall $a = 0$, dass es zu jeder ganzen Zahl b genau eine ganze Zahl e gibt, so dass $b + e = 0$ ist. Man nennt e die zu b *entgegengesetzte Zahl*. Laut Definition der Differenz können wir sie als $0 - b$ schreiben. Es hat sich eingebürgert, dafür die Abkürzung $-b$ zu verwenden. Ebenso kann man anstelle von $0 + b$ auch $+b$ schreiben, was aber das selbe wie b ist und darum kaum vorkommt.

Wenn wir in den Rechengesetzen (4.1) für je zwei Variablen Null einsetzen, ergeben sich folgende Regeln für beliebige ganze Zahlen a, b, c und d :

$$\begin{aligned} a + (-d) &= a - d, & (-b) + c &= c - b, & (-b) + (-d) &= -(b + d), \\ a - (-d) &= a + d, & (-b) - c &= -(b + c), & (-b) - (-d) &= d - b, \\ & & -(c - d) &= d - c, & & \\ a \cdot (-d) &= -a \cdot d, & (-b) \cdot c &= -b \cdot c, & (-b) \cdot (-d) &= b \cdot d. \end{aligned}$$

Setzen wir drei Variablen gleich Null, so folgt

$$-(-d) = d.$$

Das Minuszeichen in einem Ausdruck $-n$, wobei n eine natürliche Zahl ist, nennt man ein *Vorzeichen*.³⁴ Da sich die Assoziativgesetze (5) der Subtraktion schwer einprägen lassen, verwandelt man lieber jede Differenz mit Hilfe der ersten oben genannten Vorzeichenregel in eine Summe, so dass man nur noch die Assoziativgesetze der Addition benötigt.

³⁴In mathematikdidaktischen Schriften kommt die irrige Auffassung vor, Vorzeichen seien grundsätzlich von Operationszeichen zu unterscheiden, es werden sogar Bezeichnungen wie n^- oder ^-n vorgeschlagen.

4.2 Vergleich von ganzen Zahlen

Wir wollen auch für ganze Zahlen über eine Kleiner-Gleich-Relation verfügen. Auch hier verschieben wir den Beweis ihrer Existenz auf später.

Annahme 3. *Es gibt eine Ordnung auf der Menge der ganzen Zahlen, die bei Anwendung auf natürliche Zahlen mit der bereits betrachteten Kleiner-Gleich-Relation übereinstimmt (weshalb wir sie mit dem selben Symbol \leq bezeichnen), so dass das **Monotoniegesetz der Addition** aus Satz 21 auch für ganze Zahlen a, b, c und d gilt, nämlich*

$$\text{Wenn } a \leq b \text{ und } c \leq d, \text{ dann } a + c \leq b + d.$$

Für den Begriff der Ordnung verweisen wir auf Definition 28 und merken an, dass aus der Totalität die Reflexivität folgt.

Aus der Annahme 3 lassen sich eine Reihe von Folgerungen ableiten. Die erste ist die Äquivalenz

$$a - b \leq c - d \iff a + d \leq b + c. \quad (8)$$

Aus der linken Ungleichung und der (nach Reflexivität gültigen) Ungleichung $-(c - d) \leq -(c - d)$ folgt nämlich mit Annahme 3, dass $(a - b) - (c - d) \leq 0$, nach (4.1) also $(a + d) - (b + c) \leq 0$, und wiederum mit Annahme 3 die rechte Ungleichung. Ähnlich zeigt man die Umkehrung.

Folgerung 11. *Für ganze Zahlen a und b gilt genau dann $a \leq b$, wenn $-b \leq -a$ gilt, und genau dann, wenn es eine natürliche Zahl p gibt, so dass*

$$a + p = b.$$

Beweis. Die erste Aussage ergibt sich, wenn wir in (8) a und c gleich Null setzen und dann d durch a ersetzen.

Die Aussage $0 \leq p$ gilt für alle Kardinalzahlen p , insbesondere für alle natürlichen Zahlen p . Mit Annahme 3 folgt daraus $a \leq a + p$. Zum Beweis der Umkehrung schreiben wir $a = k - l$ und $b = m - n$ mit natürlichen Zahlen k, l, m und n , was nach Annahme 2 möglich ist. Aus

$$a \leq b$$

folgt nach (8)

$$k + n \leq l + m.$$

Laut Satz 25 existiert eine natürliche Zahl p , so dass

$$(k + n) + p = l + m.$$

Mit den Rechengesetzen für ganze Zahlen und der Definition der Differenz erhalten wir

$$((p + k) + n) - (m + l) = 0$$

und mit (4.1) schließlich

$$((p + k) - l) - (m - n) = 0.$$

Wiederum mit der Definition der Differenz und einem Assoziativgesetz der Subtraktion ergibt sich

$$p + (k - l) = m - n. \quad \square$$

Die zweite Aussage von Folgerung 11 ist sogar im Fall $a = 0$ interessant:

Folgerung 12. *Eine ganze Zahl ist genau dann eine natürliche Zahl, wenn sie größer oder gleich Null ist.*

Wenden wir die erste Aussage von Folgerung 11 auf die Zahlen a und 0 an, so erhalten wir mit der Totalität:

Folgerung 13. *Eine ganze Zahl ist eine natürliche Zahl oder die entgegengesetzte Zahl einer natürlichen Zahl.*

Wegen der Antisymmetrie können nur für die Zahl Null beide Fälle gleichzeitig eintreten.

Folgerung 14. *Für beliebige von Null verschiedene ganze Zahlen a und b gilt $a \cdot b \neq 0$.*

Dies ist offensichtlich für von Null verschiedene natürliche Zahlen $a = m$ und $b = n$, denn aus $m \geq 1$ und $n \geq 1$ folgt nach Satz 21, dass $m \cdot n \geq 1 \cdot 1$. Die anderen nach Folgerung 13 möglichen Fälle

$$a = -m \text{ und } b = n,$$

$$a = m \text{ und } b = -n,$$

$$a = -m \text{ und } b = -n$$

behandelt man mit Hilfe der Vorzeichenregeln für die Multiplikation.

Die letzte Folgerung ist äquivalent zu ihrer Kontraposition, nämlich:

Folgerung 15. *Gilt $a \cdot b = 0$ für ganze Zahlen a und b , so ist $a = 0$ oder $b = 0$.*

Es gibt also keine von Null verschiedenen ganzen Zahlen a und b , so dass $a \cdot b = 0$ ist. Aus diesem Grunde sagt man, dass es unter den ganzen Zahlen keine Nullteiler gibt.

Für die Addition ganzer Zahlen braucht man keine Kürzungsregel wie in Satz 32, denn aus $a + c = b + c$ folgt $(a + c) - c = (b + c) - c$, woraus man mit Hilfe von (5) leicht die Aussage $a = b$ folgert. Hingegen gibt es eine Kürzungsregel für die Multiplikation ganzer Zahlen.

Folgerung 16. *Gilt $a \cdot c = b \cdot c$ für ganze Zahlen a, b und c , wobei $c \neq 0$, so ist $a = b$.*

Nach Folgerung 15 folgt aus $(a - b) \cdot c = 0$ nämlich $a - b = 0$, und nach Definition der Differenz ist dies gleichbedeutend mit der Behauptung.

In der Annahme 3 haben wir das **Monotoniegesetz der Multiplikation** aus Satz 21 nicht erwähnt, weil es leider nicht in vollem Umfang für ganze Zahlen gilt.

Folgerung 17. *Für beliebige natürliche Zahlen m und ganze Zahlen c, d gilt:*

$$\text{Wenn } c \leq d, \text{ dann } m \cdot c \leq m \cdot d.$$

Der Beweis ist Gegenstand von Aufgabe 47.

4.3 Konstruktion der ganzen Zahlen

Wir wissen noch nicht, ob die Annahmen 1 und 2 aus Abschnitt 4.1 richtig sind. Nehmen wir noch für einen Augenblick an, das sei der Fall. Dann ist die durch

$$f(m, n) = m - n$$

definierte Abbildung $f : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{Z}$ surjektiv. Um festzustellen, ob f injektiv ist, betrachten wir Paare (k, l) und (m, n) von natürlichen Zahlen mit der Eigenschaft $f(k, l) = f(m, n)$, das heißt

$$k - l = m - n.$$

Nach Definition der Differenz und nach den Rechengesetzen folgt

$$k = l + (m - n) = (l + m) - n,$$

also

$$k + n = l + m. \tag{9}$$

Da wir die Umformungen auch in umgekehrter Reihenfolge vornehmen können, ist die Bedingung (9) äquivalent zu $f(k, l) = f(m, n)$. Man findet leicht

Beispiele für verschiedene Paare natürlicher Zahlen mit dieser Eigenschaft, etwa $(0, 0)$ und $(1, 1)$, also ist f nicht injektiv. Für jedes Element a von \mathbf{Z} haben wir die Menge

$$\{(m, n) \in \mathbf{N} \times \mathbf{N} \mid f(m, n) = a\}, \quad (10)$$

die wegen der Surjektivität von f nicht leer ist.

Wenn wir auf der Menge $\mathbf{N} \times \mathbf{N}$ die Relation der Differenzgleichheit, abgekürzt³⁵ \sim , dadurch definieren, dass

$$(k, l) \sim (m, n), \text{ wenn } f(k, l) = f(m, n),$$

so ist \sim eine *Äquivalenzrelation*, d. h. sie ist reflexiv, symmetrisch und transitiv. Mit dem Analogon von Satz 8 folgt daraus, dass die Menge $\mathbf{N} \times \mathbf{N}$ in Äquivalenzklassen zerfällt, und diese sind genau die Mengen in (10). Glücklicherweise können wir die Relation \sim mittels (9) und die Rechenoperationen mittels (7) beschreiben, ohne die gesuchte Menge \mathbf{Z} zu benutzen.

Damit können wir den unsicheren Boden der Annahmen verlassen und mit der Konstruktion der ganzen Zahlen beginnen.

Definition 33. *Wir definieren die Relation der Differenzgleichheit, abgekürzt \sim , auf der Menge $\mathbf{N} \times \mathbf{N}$ wie folgt:*

$$(k, l) \sim (m, n) \text{ genau dann, wenn } k + n = l + m.$$

Wir definieren Operationen $+$ und \cdot auf $\mathbf{N} \times \mathbf{N}$ wie folgt:

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

Satz 39. *(i) Die Relation \sim auf $\mathbf{N} \times \mathbf{N}$ ist eine Äquivalenzrelation.*

(ii) Ist $(k, l) \sim (k', l')$ und $(m, n) \sim (m', n')$, so gilt

$$\begin{aligned} (k, l) + (m, n) &\sim (k', l') + (m', n'), \\ (k, l) \cdot (m, n) &\sim (k', l') \cdot (m', n'). \end{aligned}$$

Beweis. (i) Die Relation \sim ist *reflexiv*, denn die Bedingung $(m, n) \sim (m, n)$ bedeutet nach Definition, dass $m+n = n+m$, was wegen der Kommutativität der Addition erfüllt ist.

Die Relation \sim ist *symmetrisch*, d. h.

³⁵Da dies eine Relation zwischen geordneten Paaren ist, während die Gleichmächtigkeit eine Relation zwischen Mengen war, ist trotz Verwendung des selben Symbols keine Verwechslung zu befürchten.

wenn $(k, l) \sim (m, n)$, dann $(m, n) \sim (k, l)$,

denn nach dem Kommutativitätsgesetz der Addition gilt

wenn $k + n = l + m$, dann $m + l = n + k$.

Die Relation \sim ist *transitiv*, d. h.

wenn $(k, l) \sim (m, n)$ und $(m, n) \sim (p, q)$, dann $(k, l) \sim (p, q)$.

Diese Aussage bedeutet:

Wenn $k + n = l + m$ und $m + q = n + p$, dann $k + q = l + p$.

Es ist nicht leicht, dies unmittelbar zu beweisen. Aus $k + n = l + m$ und $m + q = n + p$ folgt zunächst einmal, dass

$$(k + n) + (m + q) = (l + m) + (n + p).$$

Mit Hilfe der Rechengesetze der Addition (Satz 10) können wir beide Seiten umformen und erhalten

$$(k + q) + (m + n) = (l + p) + (m + n),$$

und nach der Kürzungsregel (Satz 32) folgt nun die Behauptung.

(ii) Es sei $(k, l) \sim (k', l')$ und $(m, n) \sim (m', n')$, das heißt

$$k + l' = l + k', \quad m + n' = n + m'.$$

Wir müssen nachprüfen, dass die geordneten Paare

$$(k, l) + (m, n) \quad \text{und} \quad (k', l') + (m', n'),$$

das heißt

$$(k + m, l + n) \quad \text{und} \quad (k' + m', l' + n'),$$

differenzgleich sind. Mit anderen Worten, wir müssen zeigen, dass

$$(k + m) + (l' + n') = (l + n) + (k' + m').$$

Dazu addieren wir die gegebenen Gleichungen und erhalten

$$(k + l') + (m + n') = (l + k') + (n + m'),$$

Daraus folgt das Gewünschte mit Hilfe der Rechengesetze der Addition natürlicher Zahlen.

Der Beweis für die Multiplikation ist Gegenstand der Übungsaufgabe 49.

□

Nun können wir die ganzen Zahlen definieren. Bei Vorliegen einer Äquivalenzrelation auf einer Menge zerfällt diese Menge in Äquivalenzklassen. Der Beweis ist ganz ähnlich zu dem von Satz 8. Anstatt nun jeder Äquivalenzklasse eine ganze Zahl zuzuordnen, die man sich ja irgendwoher beschaffen müsste, deklarieren wir einfach die Klassen selbst als ganze Zahlen.

Definition 34. *Eine ganze Zahl ist eine Äquivalenzklasse von geordneten Paaren natürlicher Zahlen bezüglich der Relation der Differenzgleichheit. Die Menge der ganzen Zahlen bezeichnen wir mit \mathbf{Z} , die Klasse eines geordneten Paares (m, n) natürlicher Zahlen bezeichnen wir mit $[m, n]$. Wir definieren die Addition und die Multiplikation ganzer Zahlen durch*

$$\begin{aligned}[k, l] + [m, n] &= [k + m, l + n], \\ [k, l] \cdot [m, n] &= [k \cdot m + l \cdot n, k \cdot n + l \cdot m].\end{aligned}$$

Der vorangehende Satz zeigt, dass diese Definition korrekt ist. Nun können wir auch die Rechengesetze beweisen.

Satz 40. (i) *Für beliebige ganze Zahlen a, b und c gelten die Rechengesetze (4).*

(ii) *Die Subtraktion ganzer Zahlen ist uneingeschränkt ausführbar.*

(iii) *Die Abbildung $i : \mathbf{N} \rightarrow \mathbf{Z}$, die durch $i(n) = [n, 0]$ gegeben ist, ist injektiv, und für alle natürlichen Zahlen m, n gilt*

$$i(m + n) = i(m) + i(n), \quad i(m \cdot n) = i(m) \cdot i(n).$$

Beweis. (i) Wir beweisen zum Beispiel das Assoziativgesetz der Multiplikation. Es sei $a = [k, l]$, $b = [m, n]$ und $c = [p, q]$. Dann ist nach Definition

$$\begin{aligned}(a \cdot b) \cdot c &= ([k, l] \cdot [m, n]) \cdot [p, q] = [km + ln, kn + lm] \cdot [p, q] \\ &= [(km + ln)p + (kn + lm)q, (km + ln)q + (kn + lm)p]\end{aligned}$$

und

$$\begin{aligned}a \cdot (b \cdot c) &= [k, l] \cdot ([m, n] \cdot [p, q]) = [k, l] \cdot [mp + nq, mq + np] \\ &= [k(mp + nq) + l(mq + np), k(mq + np) + l(mp + nq)].\end{aligned}$$

Mit Hilfe der Rechengesetze für natürliche Zahlen können wir prüfen, dass nicht nur die Äquivalenzklassen, sondern sogar die geordneten Paare selbst gleich sind:

$$\begin{aligned}(km + ln)p + (kn + lm)q &= (kmp + lnp) + (knq + lmq) \\ &= (kmp + knq) + (lnp + lmq) = k(mp + nq) + l(mq + np),\end{aligned}$$

und für die zweiten Komponenten prüft man es auf ähnliche Weise.

Ähnlich beweist man die anderen Rechengesetze.

(ii) Wir müssen zeigen, dass es für beliebige ganze Zahlen $a = [k, l]$ und $b = [m, n]$ genau eine ganze Zahl $d = [r, s]$ gibt, so dass $a = b + d$. Dies bedeutet laut Definition der Addition, dass $[k, l] = [m + r, n + s]$, und nach Definition der ganzen Zahlen, dass $k + (n + s) = l + (m + r)$. Nach den Rechengesetzen der natürlichen Zahlen ist das gleichbedeutend mit $r + (l + m) = s + (k + n)$, also nach Definition der ganzen Zahlen mit $[r, s] = [k + n, l + m]$. Es gibt somit genau eine Lösung, nämlich $d = [k + n, l + m]$.

(iii) Ist $i(m) = i(n)$ für natürliche Zahlen m und n , so bedeutet dies $(m, 0) \sim (n, 0)$, also $m + 0 = n + 0$ und somit $m = n$. Folglich ist i injektiv. Laut Definition gilt

$$\begin{aligned} [m, 0] + [n, 0] &= [m + n, 0 + 0] = [m + n, 0], \\ [m, 0] \cdot [n, 0] &= [m \cdot n + 0 \cdot 0, m \cdot 0 + 0 \cdot n] = [m \cdot n, 0], \end{aligned}$$

und hieraus folgen die anderen Behauptungen. □

Der Satz beweist unsere Annahme 1 mit Ausnahme der Aussage $\mathbf{N} \subset \mathbf{Z}$. Allerdings bietet die Aussage (iii) des Satzes einen hinreichenden Ersatz, worauf wir später noch zurückkommen.

Zunächst müssen wir noch eine Ordnung auf \mathbf{Z} einführen, die der Annahme 3 genügt. Zur Motivation nehmen wir für einen Augenblick an, all unsere Annahmen wären erfüllt. Da sich ganze Zahlen dann als Differenzen natürlicher Zahlen darstellen lassen, geht es um Aussagen der Form

$$k - l \leq m - n,$$

wobei k, l, m und n natürliche Zahlen sind. Diese Aussage wäre dann aber nach (8) äquivalent zur Ungleichung

$$k + n \leq l + m,$$

in der nur natürliche Zahlen vorkommen. Wir können also die letztere Ungleichung zur Definition der Kleiner-Gleich-Relation auf ganzen Zahlen benutzen, vorausgesetzt, ihre Gültigkeit hängt nicht von der Wahl von Repräsentanten ab.

Satz 41. *Es seien k, l, m, n, k', l', m' und n' natürliche Zahlen. Ist $(k, l) \sim (k', l')$ und $(m, n) \sim (m', n')$, so gilt*

$$\text{genau dann } k + n \leq l + m, \quad \text{wenn } k' + n' \leq l' + m'.$$

Beweis. Die Differenzungleichheit $(k, l) \sim (k', l')$ bedeutet

$$k + l' = l + k'.$$

Angenommen, es gilt die Ungleichung

$$k + n \leq l + m.$$

Um obige Gleichheit darauf anwenden zu können, benutzen wir Satz 21 und erhalten die Ungleichung

$$k + n + l' \leq l + m + l',$$

wobei wir die Klammern wegen des Assoziativgesetzes weglassen können. Durch Einsetzen erhalten wir

$$l + k' + n \leq l + m + l',$$

und mit der Kürzungsregel aus Aufgabe 31(a) folgt

$$n + k' \leq m + l'.$$

Aus der ursprünglichen Ungleichung folgt also diejenige mit (k', l') an Stelle von (k, l) .

Die Relation $(m, n) \sim (m', n')$ bedeutet

$$m + n' = n + m'.$$

Um mit ihrer Hilfe auch (m, n) durch (m', n') zu ersetzen, wenden wir wiederum Satz 21 an und erhalten

$$n + k' + n' \leq m + l' + n'.$$

Einsetzen ergibt

$$n + k' + n' \leq n + m' + l',$$

und mit der Kürzungsregel folgt

$$k' + n' \leq l' + m'.$$

Die Umkehrung beweist man analog oder führt sie durch Vertauschung der Bezeichnungen mit und ohne Strich auf das bereits Bewiesene zurück. \square

Der Satz rechtfertigt die folgende Definition.

Definition 35. Wir definieren eine Relation \leq auf der Menge \mathbf{Z} , indem wir für beliebige natürliche Zahlen k, l, m und n setzen

$$[k, l] \leq [m, n], \text{ wenn } k + n \leq l + m.$$

Satz 42. (i) Die Relation \leq auf der Menge \mathbf{Z} ist eine Ordnung.

(ii) Es gilt die Annahme 3.

(iii) Ist $i : \mathbf{N} \rightarrow \mathbf{Z}$ die Abbildung aus Satz 40, so gilt für beliebige natürliche Zahlen m und n

$$\text{genau dann } i(m) \leq i(n), \text{ wenn } m \leq n.$$

Beweis. Für Teil (i) müssen wir die drei Eigenschaften nachprüfen, die eine Ordnung ausmachen. Dabei schreiben wir die vorkommenden ganzen Zahlen in der Form $a = [k, l]$, $b = [m, n]$ und $c = [p, q]$. Die *Totalität* besagt, dass für beliebige a und b gilt

$$a \leq b \quad \text{oder} \quad b \leq a,$$

das heißt

$$k + n \leq l + m \quad \text{oder} \quad m + l \leq n + k.$$

Dies gilt in der Tat wegen der Totalität der Kleiner-Gleich-Relation auf \mathbf{N} (Folgerung 8) und der Kommutivität.

Die *Antisymmetrie* besagt, dass für ganze Zahlen a und b gilt:

$$\text{Wenn } a \leq b \text{ und } b \leq a, \text{ dann } a = b.$$

Dies bedeutet laut Definitionen 35 und 34:

$$\text{Wenn } k + n \leq l + m \quad \text{und} \quad m + l \leq n + k, \quad \text{dann } k + n = l + m.$$

Letzteres gilt wegen der Antisymmetrie der Kleiner-Gleich-Relation auf \mathbf{N} , die sogar für Kardinalzahlen in Satz 22 bewiesen wurde, und der Kommutivität.

Die *Transitivität* besagt, dass für ganze Zahlen a, b und c gilt:

$$\text{Wenn } a \leq b \text{ und } b \leq c, \text{ dann } a \leq c.$$

Dies bedeutet:

$$\text{Wenn } k + n \leq l + m \quad \text{und} \quad m + q \leq n + p, \quad \text{dann } k + q \leq l + p.$$

Wenden wir Satz 21 auf die ersten beiden Ungleichungen an, so erhalten wir

$$(k + n) + (m + q) \leq (l + m) + (n + p),$$

und mit der Kürzungsregel folgt die dritte Ungleichung. Die behauptete Implikation ist also wahr.

(ii) Zusätzlich zu den bisherigen Bezeichnungen sei $d = [r, s]$. Angenommen, es gilt $a \leq b$ und $c \leq d$, das heißt

$$k + n \leq l + m \quad \text{und} \quad p + s \leq q + r.$$

Wir wollen zeigen, dass dann gilt $a + c \leq b + d$, das heißt

$$(k + p) + (n + s) \leq (l + q) + (m + r),$$

wobei die Klammern natürlich unnötig sind. Genau dies ist das Ergebnis, wenn wir Satz 21 auf die beiden vorangehenden Ungleichungen anwenden.

(iii) Mit Hilfe der Definition der Abbildung i wird die Aussage $i(m) \leq i(n)$ zu $[m, 0] \leq [n, 0]$. Nach Definition 35 bedeutet dies $m + 0 \leq 0 + n$, und das ist äquivalent zu $m \leq n$. \square

Zwar hat sich unser Wunsch, dass \mathbf{Z} die Menge \mathbf{N} als Teilmenge enthält, nicht erfüllt, aber die Aussagen (iii) der Sätze 40 und 42 sind ein hinreichender Ersatz, weil wir mit den Bildern der natürlichen Zahlen unter der Abbildung i genau so rechnen können wie mit diesen Zahlen selbst.³⁶ Gewöhnlich benutzt man für die ganze Zahl $[n, 0]$ einfach die Bezeichnung n . Dann wird die Bezeichnung $[m, n]$ überhaupt überflüssig, weil ja $m - n$ das selbe bedeutet.

Es gibt noch andere Möglichkeiten, den Zahlbereich \mathbf{Z} zu konstruieren, z. B. indem man zu den natürlichen Zahlen weitere Objekte hinzunimmt. Dann sind in den Beweisen der Rechengesetze allerdings umfangreiche Fallunterscheidungen nötig. In der Schule wird dieser Weg vorgezogen, da man dort die Beweise ohnehin meist weggelässt. Letztendlich kommt es nicht auf die Methode zur Konstruktion der ganzen Zahlen an.

Man kann nämlich beweisen, dass die Menge \mathbf{Z} mit den Operationen $+$ und $-$ durch ihre Eigenschaften (als minimale Erweiterung der natürlichen Zahlen unter Erhalt der Rechengesetze, in der die Subtraktion uneingeschränkt ausführbar ist) im Wesentlichen eindeutig bestimmt ist. Das bedeutet, dass es zwischen zwei solchen Erweiterungen \mathbf{Z} und \mathbf{Z}' eine bijektive Abbildung gibt, die jede natürliche Zahl auf sich selbst abbildet und mit den Rechenoperationen verträglich ist. In diesem Sinne sind \mathbf{Z} und \mathbf{Z}' dann *isomorph* (griechisch für „gleichgestaltig“).

³⁶Man ändert einfach die bisherigen Bezeichnungen ab, indem man entweder den Wertebereich von i mit \mathbf{N} bezeichnet oder diesen Wertebereich aus \mathbf{Z} herausnimmt und durch \mathbf{N} ersetzt.

Ganzzahlige Exponenten

Als Anwendung wollen wir nun für eine Abbildung f einer Menge M in sich selbst den Begriff der Potenz, den wir in (3) nur für natürliche Exponenten definiert hatten, auf ganzzahlige Exponenten verallgemeinern, so dass die Potenzgesetze

$$f^{a+b} = f^a \circ f^b, \quad (f \circ g)^a = f^a \circ g^a, \quad f^{a \cdot b} = (f^a)^b$$

für alle miteinander kommutierenden Abbildungen $f, g : M \rightarrow M$ und alle ganzen Zahlen a, b gelten. Wegen $f^0 = \text{id}_M$ müsste als Spezialfall des ersten Gesetzes dann gelten

$$\text{id}_M = f \circ f^{-1}, \quad \text{id}_M = f^{-1} \circ f.$$

Dies zeigt mit Satz 6, dass unser Vorhaben nur realisierbar sein kann, wenn f umkehrbar ist, und dass f^{-1} dann gleich der Umkehrabbildung sein muss.

Nehmen wir also an, dass f eine Umkehrabbildung h besitzt. Für $a = [k, l]$ wäre, wenn die Potenzgesetze gelten,

$$f^a = f^{k-l} = f^k \circ f^{(-1) \cdot l} = f^k \circ h^l.$$

Wir würden die rechte Seite gern als Definition nehmen. Dies ist nur dann korrekt, wenn für alle natürlichen Zahlen k, l, m und n mit der Eigenschaft $(k, l) \sim (m, n)$ gilt

$$f^k \circ h^l = f^m \circ h^n. \quad (11)$$

Dazu müssen wir zunächst prüfen, dass für beliebige natürliche Zahlen m und n gilt

$$f^m \circ h^n = h^n \circ f^m.$$

Im Fall $m \leq n$ gibt es nach Satz 25 eine natürliche Zahl p , so dass $n + p = m$, und dann gilt nach Satz 4 und den Potenzgesetzen für natürliche Exponenten

$$f^m \circ h^n = f^m \circ (h^m \circ h^p) = (f^m \circ h^m) \circ h^p = (f \circ h)^m \circ h^p = \text{id}_M \circ h^p = h^p,$$

und analog zeigt man, dass auch $h^n \circ f^m = h^p$. Den Fall $m \geq n$ behandelt man ähnlich.

Wir sehen also, dass Gleichung (11) äquivalent ist zu

$$f^k \circ h^l = h^n \circ f^m.$$

Wenn wir beide Seiten von links mit f^n und von rechts mit f^l verketten, so folgt

$$f^n \circ f^k = f^m \circ f^l.$$

Wir können auch die umgekehrte Implikation zeigen, indem wir von links mit h^n und von rechts mit h^l verketten. Also ist (11) äquivalent zu der letzten Gleichung, aber die ist wegen $k + n = l + m$ eine Folgerung aus den Potenzgesetzen für natürliche Exponenten.

Wir können also für $a = [k, l]$ definieren

$$f^a = f^k \circ h^l,$$

wobei h die Umkehrabbildung von f bezeichnet.

4.4 Kombinatorik

Die Kombinatorik befasst sich mit der Abzählung endlicher Mengen, die eine gewisse Struktur aufweisen. In diesem Sinne gehört sie eigentlich in den Abschnitt über natürliche Zahlen.³⁷ Dort haben wir bereits einige Abzählprobleme kennengelernt:

- Die Anzahl der geordneten Paare (x, y) , wobei x zu einer Menge M und y zu einer Menge N gehört, ist nach Definition 15 gleich $|M| \cdot |N|$.
- Die Anzahl der Abbildungen von einer Menge N der Mächtigkeit n in eine Menge M der Mächtigkeit m ist nach Definition 17 gegeben durch

$$|M^N| = m^n.$$

Im Fall $N = \{1, 2, 3, \dots, n\}$ können wir solche Abbildungen auch als n -Tupel von Elementen aus M auffassen, welches nichts anderes darstellen als die untere Zeile der Wertetabelle, vgl. S. 58. Die Aussage lautet dann

$$|M^n| = m^n \quad (n \geq 1).$$

In der Schule wird die Potenz natürlicher Zahlen, wie wir schon bemerkt haben, anders definiert, nämlich rekursiv. Dann muss man die obige Formel beweisen.

Da die Potenz M^n ebenfalls rekursiv definiert ist, bietet sich dafür die vollständige Induktion an. Die Formel gilt für $n = 1$, weil laut Definition gilt

$$M^1 = M, \quad m^1 = m.$$

Gilt die Formel bereits für eine natürliche Zahl n , so folgt mit Hilfe der rekursiven Definitionen und der Definition der Multiplikation, dass

$$|M^{n+1}| = |M^n \times M| = |M^n| \cdot |M| = m^n \cdot m = m^{n+1}.$$

Das Abzählen injektiver Abbildungen führt auf folgenden Begriff.

³⁷Wir kommen hier noch einmal darauf zurück, weil wir für den folgenden Satz 43 ganze Zahlen benötigen.

Definition 36. Wir definieren das Pochhammer-Symbol für alle natürlichen Zahlen m und n rekursiv nach n durch

$$(m)_0 = 1, \quad (m)_{n+1} = (m)_n \cdot (m - n).$$

Für $n \geq 1$ gilt

$$(m)_n = \prod_{i=0}^{n-1} (m - i),$$

denn für festes m definieren die beiden Seiten Funktionen von n , die für $n = 1$ den selben Anfangswert m haben und der selben Rekursionsformel genügen. Somit müssen sie nach Satz 35 übereinstimmen. In einer weniger exakten Schreibweise ist

$$(m)_n = \underbrace{m(m-1)(m-2)\dots(m-n+1)}_{n \text{ Faktoren}},$$

also im Spezialfall $m = n$

$$(n)_n = \prod_{j=0}^{n-1} (n - j) = \prod_{i=1}^n i = n!$$

wobei wir die zweite Substitutionsregel aus Satz 36 benutzt haben.

Satz 43. Sind M und N endliche Mengen, wobei $|M| = m$ und $|N| = n$, so gibt es $(m)_n$ injektive Abbildungen $N \rightarrow M$.

Beweis durch vollständige Induktion nach n . Wir halten die Menge M fest. Es gibt genau eine Abbildung $\emptyset \rightarrow M$, und die ist injektiv, also ist die Aussage für $n = 0$ bewiesen.

Angenommen, die Aussage gilt für alle Mengen N der Mächtigkeit n . Nun betrachten wir eine Menge N' der Mächtigkeit $n + 1$. Nach Lemma 3 gibt es ein Element $a \in N'$, und wenn wir $N = N' \setminus \{a\}$ setzen, dann ist $|N| = n$.

Jede Abbildung $g : N' \rightarrow M$ hat eine Einschränkung auf N ; das ist die Abbildung $f : N \rightarrow M$, die durch die Vorgabe $f(x) = g(x)$ für alle $x \in N$ definiert ist. Wenn g injektiv ist, so gilt das auch für die Einschränkung f . Umgekehrt gibt es im Allgemeinen mehrere Möglichkeiten, eine injektive Abbildung $f : N \rightarrow M$ zu einer injektiven Abbildung $g : N' \rightarrow M$ fortzusetzen, indem man den Wert $g(a)$ festlegt. Den Wertebereich von f bezeichnen wir mit

$$M_f = \{y \in M \mid \text{Es gibt ein } x \in N, \text{ so dass } f(x) = y\}.$$

Die Abbildung g wird genau dann injektiv sein, wenn $g(a)$ nicht in M_f liegt, d. h. wenn $g(a) \in M \setminus M_f$. Wegen der Injektivität von f ist $|M_f| = |N|$, also gibt es

$$|M \setminus M_f| = |M| - |M_f| = m - n$$

Möglichkeiten für die Wahl von $g(a)$. Laut Induktionsvoraussetzung gibt es $(m)_n$ injektive Abbildungen $N \rightarrow M$, und jede von ihnen hat $m - n$ verschiedene injektive Fortsetzungen auf N' . Dabei sind die Mengen der Fortsetzungen verschiedener Abbildungen $N \rightarrow M$ disjunkt. Nach Satz 16 ist die Anzahl injektiver Abbildungen $N' \rightarrow M$ gleich

$$(m)_n \cdot (m - n),$$

und diese Zahl ist nach der rekursiven Definition gleich $(m)_{n+1}$. Somit gilt die Behauptung auch für die Menge N' .

Bei der Berechnung von $|M \setminus M_f|$ haben wir stillschweigend $n \leq m$ vorausgesetzt. Andernfalls gibt es nach Definition der Kleiner-Gleich-Relation keine injektiven Abbildungen $N \rightarrow M$. Nach Induktionsvoraussetzung ist dann $(m)_n = 0$, und wir erhalten $(m)_{n+1} = 0 \cdot (m - n)$, was die richtige Anzahl der injektiven Abbildungen $N' \rightarrow M$ angibt. \square

Beispiel. Es sei $M = \{a, b, c, d\}$ und $N = \{1, 2, 3\}$. Die Abbildungen $f : N \rightarrow M$ sind durch die Tripel $(f(1), f(2), f(3))$ gegeben. Hier ist eine vollständige Liste:

$(a, a, a), (a, a, b), (a, a, c), (a, a, d), (a, b, a), (a, b, b), (a, b, c), (a, b, d),$
 $(a, c, a), (a, c, b), (a, c, c), (a, c, d), (a, d, a), (a, d, b), (a, d, c), (a, d, d),$
 $(b, a, a), (b, a, b), (b, a, c), (b, a, d), (b, b, a), (b, b, b), (b, b, c), (b, b, d),$
 $(b, c, a), (b, c, b), (b, c, c), (b, c, d), (b, d, a), (b, d, b), (b, d, c), (b, d, d),$
 $(c, a, a), (c, a, b), (c, a, c), (c, a, d), (c, b, a), (c, b, b), (c, b, c), (c, b, d),$
 $(c, c, a), (c, c, b), (c, c, c), (c, c, d), (c, d, a), (c, d, b), (c, d, c), (c, d, d),$
 $(d, a, a), (d, a, b), (d, a, c), (d, a, d), (d, b, a), (d, b, b), (d, b, c), (d, b, d),$
 $(d, c, a), (d, c, b), (d, c, c), (d, c, d), (d, d, a), (d, d, b), (d, d, c), (d, d, d).$

Die Tripel, die nicht injektiven Abbildungen entsprechen, sind ausgegraut.

In der klassischen kombinatorischen Terminologie nennt man Abbildungen oder n -Tupel *Variationen mit Wiederholung*, und injektive Abbildungen nennt man *Variationen ohne Wiederholung*.³⁸ Der Begriff von Elementen einer Menge war damals nicht geläufig, man sprach von Dingen. Durch Abzählen unserer Liste sehen wir, dass

³⁸Man beachte, dass bei den Variationen mit Wiederholung die Variationen ohne Wiederholung mitgezählt werden.

die Anzahl der Variationen mit Wiederholung
von 4 Dingen zur Klasse 3 gleich 64

ist, während

die Anzahl der Variationen ohne Wiederholung
von 4 Dingen zur Klasse 3 gleich 24

ist. Dies erhalten wir natürlich auch aus unseren Formeln:

$$4^3 = 64, \quad (4)_3 = 4 \cdot 3 \cdot 2 = 24.$$

Beispiel. Die möglichen Gewinnzahlen für die Gewinnklasse I im Spiel 77 sind die siebenstelligen Endnummern, also die Variationen mit Wiederholung von zehn Dingen (Ziffern) zur Klasse 7.

Beispiel. Die möglichen Sitzpläne für n Schüler in einem Klassenraum mit m Stühlen sind die Variationen ohne Wiederholung von m Dingen zur Klasse n .

Die bijektiven Abbildungen einer Menge in sich selbst nennt man traditionell *Permutationen*. Da nach Satz 27 jede injektive Abbildung einer endlichen Menge in sich selbst auch surjektiv und somit bijektiv ist, erhalten wir als Spezialfall von Satz 43:

Folgerung 18. *Die Anzahl der Permutationen einer endlichen Menge der Mächtigkeit n ist gleich $n!$.*

Ein weiteres kombinatorisches Problem ist die Abzählung von Teilmengen.

Satz 44. *Eine endlichen Menge der Mächtigkeit n hat 2^n Teilmengen.*

Beweis. Ist M eine Teilmenge von N , so hat für jedes Element x von N die Aussage $x \in M$ einen Wahrheitswert, den wir mit $f(x)$ bezeichnen. Auf diese Weise erhalten wir eine Abbildung $f : N \rightarrow \{w, f\}$. So wird z. B. der Teilmenge $\{b, d\}$ von $\{a, b, c, d\}$ die Funktion mit der Wertetabelle

x	a	b	c	d
$f(x)$	f	w	f	w

zugeordnet. Ist umgekehrt eine Abbildung $f : N \rightarrow \{w, f\}$ gegeben, so erhalten wir eine Teilmenge $M = \{x \in N \mid f(x)\}$. Es gibt also genauso viele Teilmengen, wie es Abbildungen $N \rightarrow \{w, f\}$ gibt. Für $|N| = n$ ist die Anzahl solcher Abbildungen nach Definition 17 (vgl. Anfang dieses Abschnitts) gleich 2^n . \square

In der Mathematik ersetzt man in diesem Zusammenhang häufig w durch 1 und f durch 0 , und man nennt die einer Teilmenge zugeordnete Funktion $f : N \rightarrow \{0, 1\}$ die *charakteristische Funktion* dieser Teilmenge.

Definition 37. *Es seien n und k natürliche Zahlen. Die Anzahl der Teilmengen der Mächtigkeit k in einer Menge der Mächtigkeit n bezeichnet man mit $\binom{n}{k}$, gelesen³⁹ „ n über k “.*

Man nennt diese Zahlen auch *Binomialkoeffizienten*, weil sie in der Formel für die Potenz eines zweigliedrigen Terms (eines Binoms) vorkommen.

Satz 45 (erste binomische Formel). *Für beliebige $a, b \in \mathbf{Z}$ und $n \in \mathbf{N}$ gilt*

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

Dabei sind natürliche Potenzen von ganzen Zahlen wieder rekursiv definiert, und die Potenzgesetze gelten auch in diesem Fall. Ohne Benutzung des Summenzeichens kann man die Formel so schreiben:

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a b^{n-1} + b^n.$$

Zum Beweis benötigen wir folgende Eigenschaft der Binomialkoeffizienten, die man auch zu ihrer Berechnung im *Pascalschen Dreieck* benutzt:

Lemma 4. *Für natürliche Zahlen n und k gilt*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Beweis. Wir betrachten eine Menge N mit $|N| = n$ und $M = N \cup \{a\}$ mit $a \notin N$. Es sei \mathcal{N} die Menge der Teilmengen der Mächtigkeit k von N und \mathcal{M} die Menge der Teilmengen der Mächtigkeit $k+1$ von M . Wir zerlegen \mathcal{M} in zwei disjunkte Teilmengen:

$$\mathcal{M}_{\text{mit } a} = \{L \in \mathcal{M} \mid a \in L\}, \quad \mathcal{M}_{\text{ohne } a} = \{L \in \mathcal{M} \mid a \notin L\}$$

Wir behaupten, dass \mathcal{N} gleichmächtig zu $\mathcal{M}_{\text{mit } a}$ ist. Dazu ordnen wir jeder Teilmenge $K \in \mathcal{N}$ die Teilmenge

$$f(K) = K \cup \{a\}$$

³⁹Die Englische Lesart „(from) n choose k “ macht die Herkunft noch deutlicher.

von M und jeder Teilmenge $L \in \mathcal{M}_{\text{mit } a}$ die Teilmenge

$$g(L) = L \setminus \{a\}$$

von N zu. Wegen $a \notin K$ gilt dann $|f(K)| = k + 1$, und wegen $a \in L$ gilt $|g(L)| + 1 = k$ nach Definition der Addition. Wir erhalten Abbildungen $f : \mathcal{N} \rightarrow \mathcal{M}_{\text{mit } a}$ und $g : \mathcal{M}_{\text{mit } a} \rightarrow \mathcal{N}$. Offensichtlich sind f und g Umkehrabbildungen voneinander, und unsere Behauptung ist bewiesen. Es folgt $|\mathcal{M}_{\text{mit } a}| = \binom{n}{k}$.

Die Elemente von $\mathcal{M}_{\text{ohne } a}$ sind nichts anderes als die Teilmengen der Mächtigkeit $k + 1$ in N , also ist $|\mathcal{M}_{\text{ohne } a}| = \binom{n}{k+1}$. Insgesamt ergibt sich $|\mathcal{M}| = \binom{n}{k+1} + \binom{n}{k}$. \square

Beweis von Satz 45. Die Formel gilt für $n = 0$, weil dann beide Seiten laut Definition gleich 1 sind.

Angenommen, die Formel gilt für eine Zahl n . Nach Definition der Potenz und nach Induktionsvoraussetzung ist

$$(a + b)^{n+1} = (a + b) \cdot (a + b)^n = (a + b) \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k.$$

Nach den Distributivgesetzen aus Satz 13 und Satz 36 sowie der Definition der Potenz ist die rechte Seite gleich

$$a \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k + b \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^n \binom{n}{k} a^{(n-k)+1} b^k + \sum_{k=0}^n \binom{n}{k} a^{n-k} b^{k+1}.$$

In der zweiten Summe können wir $\binom{n}{k} = \binom{n}{(k+1)-1}$ und (im Exponenten) $n - k = (n + 1) - (k + 1)$ schreiben. Unter Benutzung der Substitutionsregel aus Satz 36 wird unser Ausdruck zu

$$\sum_{k=0}^n \binom{n}{i} a^{(n-k)+1} b^k + \sum_{l=1}^{n+1} \binom{n}{l-1} a^{(n+1)-l} b^l.$$

Mit Hilfe von Satz 36 spalten wir von der ersten Summe den Term mit $k = 0$ ab. Weil es in einer Menge der Mächtigkeit n keine Teilmenge der Mächtigkeit $n + 1$ gibt, ist $\binom{n}{n+1} = 0$, und wir können den Summationsindex k auch in der ersten Summe bis $n + 1$ laufen lassen (und durch l ersetzen). Nach dem Assoziativgesetz aus Satz 36 erhalten wir

$$(a + b)^{n+1} = a^{n+1} + \sum_{l=1}^{n+1} \left(\binom{n}{l} + \binom{n}{l-1} \right) a^{(n+1)-l} b^l.$$

Mit Hilfe des Lemmas und nach Wiedereingliederung des Terms mit $l = 0$ folgt die Induktionsbehauptung. \square

Wem dieser Beweis zu unübersichtlich ist, dem sei empfohlen, ihn ohne Benutzung des Summenzeichens nachzuvollziehen. Dann erspart man sich die Anwendung der Substitutionsregel auf Kosten der logischen Strenge.

Es gibt eine einleuchtende Begründung, warum die Binomialkoeffizienten in der Formel auftreten. Beim Ausmultiplizieren von

$$(a + b)^n = \underbrace{(a + b) \cdot (a + b) \cdot \dots \cdot (a + b)}_{n \text{ Faktoren}}$$

muss man sich bei jedem entstehenden Term entscheiden, aus welchen der Faktoren $a + b$ man den Summanden a und aus welchen man b nimmt. Man muss also eine Teilmenge von Faktoren auswählen, bei denen man das b nimmt, und von allen übrigen ist dann das a zu nehmen. Ein Term $a^{n-k}b^k$ entsteht dabei so oft, wie es Teilmengen der Mächtigkeit k gibt, also $\binom{n}{k}$ mal. Man kann diese Argumentation zu einem streng logischen Beweis ausbauen, was wir hier aber nicht tun werden.

Neben Variationen betrachtet man auch *Kombinationen*, bei denen es nicht auf die Reihenfolge der Dinge ankommt. So sind z. B. (c, b, b) und (b, c, b) verschiedene Variationen, stellen aber die selbe Kombination dar. Um dies mathematisch exakt zu definieren, sollten wir besser die Sprache von Abbildungen benutzen. Der Zusammenhang zwischen den Abbildungen $f, g : \{1, 2, 3\} \rightarrow \{a, b, c, d\}$ mit den Wertetabellen

$$\begin{array}{c|ccc} x & 1 & 2 & 3 \\ \hline f(x) & c & b & b \end{array} \quad \begin{array}{c|ccc} x & 1 & 2 & 3 \\ \hline g(x) & b & c & b \end{array}$$

besteht darin, dass es eine Permutation p der Menge $\{1, 2, 3\}$ gibt (hier z. B. die Transposition von 1 und 2), so dass $g = f \circ p$ ist.

Definition 38. Die Kombinationen von m Dingen zur Klasse n sind die Äquivalenzklassen von Abbildungen aus einer Menge N der Mächtigkeit n in eine Menge M der Mächtigkeit m , wobei zwei Abbildungen f, g als äquivalent gelten, wenn es eine Permutation $p : N \rightarrow N$ gibt, so dass $g = f \circ p$. Betrachtet man nur injektive Abbildungen, so spricht man von Kombinationen ohne Wiederholung, andernfalls von Kombinationen mit Wiederholung.

Man überzeugt sich leicht, dass die angegebene Relation tatsächlich eine Äquivalenzrelation auf der Menge M^N ist (Übungsaufgabe 59).

Beispiel. Die Tippmöglichkeiten in der Lotterie 6 aus 49 sind die Kombinationen ohne Wiederholung von 49 Dingen zur Klasse 6.

Beispiel. Die verschiedenen Dominosteine tragen die Kombinationen mit Wiederholung⁴⁰ von 7 Dingen ($\square, \blacksquare, \dots, \boxtimes$) zur Klasse 2.

⁴⁰Ein Dominostein oder ein Wurf mit gleichen Augenzahlen heißt Pasch.

Satz 46. *Es seien m und n natürliche Zahlen.*

(i) *Die Anzahl der Kombinationen ohne Wiederholung von m Dingen zur Klasse n ist gleich $\binom{m}{n}$.*

(ii) *Es gilt*

$$(m)_n = \binom{m}{n} \cdot n!.$$

Beweis. (i) Es seien M und N Mengen der Mächtigkeiten m und n . Wir ordnen jeder injektiven Abbildung $f : N \rightarrow M$ ihren Wertebereich zu. Jede Teilmenge K der Mächtigkeit n in M entsteht auf diese Weise, denn eine bijektive Abbildung $g : N \rightarrow K$ kann man als injektive Abbildung $N \rightarrow M$ umdeuten.

Haben zwei injektive Abbildungen f_1 und f_2 den selben Wertebereich K , so haben wir bijektive Abbildungen $g_1, g_2 : N \rightarrow K$. Ist p die Verkettung von g_2 mit der Umkehrabbildung von g_1 , so dass $g_2 = g_1 \circ p$, dann haben wir $f_2 = f_1 \circ p$. Ist andererseits $f : N \rightarrow M$ eine injektive Abbildung und $p : N \rightarrow N$ eine bijektive Abbildung, so ist auch $f \circ p : N \rightarrow M$ injektiv und hat den selben Wertebereich wie f .

Wir sehen also, dass zwei Abbildungen genau dann den selben Wertebereich haben, wenn sie äquivalent sind. Folglich gibt es genau so viele Äquivalenzklassen wie Teilmengen der Mächtigkeit n .

(ii) Halten wir eine injektive Abbildung $f : N \rightarrow M$ fest, so können wir jeder Permutation p von N die zu f äquivalente Abbildung $f \circ p$ zuordnen. Nach dem Beweis von Teil (i) entsteht jede Abbildung aus der Äquivalenzklasse von f auf diese Weise für eine eindeutig bestimmte Permutation p . Wir erhalten also eine bijektive Abbildung von der Menge der Permutationen von N auf die Äquivalenzklasse von f .

Da es nach Teil (i) genau $\binom{m}{n}$ Äquivalenzklassen gibt und jede von ihnen $n!$ Abbildungen enthält, gibt es nach Satz 16 insgesamt $\binom{m}{n} \cdot n!$ injektive Abbildungen. Vergleichen wir dieses Ergebnis mit Satz 43, so erhalten wir die behauptete Gleichung. \square

Mit Hilfe der Aussage (ii) kann man Binomialkoeffizienten berechnen:

Folgerung 19. *Die Zahl $(m)_n$ ist durch $n!$ teilbar, und es gilt*

$$\binom{m}{n} = (m)_n : n!.$$

Nun wenden wir uns den Kombinationen mit Wiederholung zu.

Beispiel. Die möglichen Ergebnisse beim Würfeln mit drei Würfeln aus einem Becher sind die Kombinationen mit Wiederholung von 6 Dingen zur Klasse 3. Hier ist eine vollständige Liste, wobei wir Augenzahlen durch arabische Ziffern wiedergeben und die Äquivalenzklasse, zu der ein Tripel gehört, durch das Tripel in eckigen Klammern bezeichnen:

[1,1,1], [1,1,2], [1,1,3], [1,1,4], [1,1,5], [1,1,6],
 [1,2,2], [1,2,3], [1,2,4], [1,2,5], [1,2,6],
 [1,3,3], [1,3,4], [1,3,5], [1,3,6],
 [1,4,4], [1,4,5], [1,4,6],
 [1,5,5], [1,5,6],
 [1,6,6],
 [2,2,2], [2,2,3], [2,2,4], [2,2,5], [2,2,6],
 [2,3,3], [2,3,4], [2,3,5], [2,3,6],
 [2,4,4], [2,4,5], [2,4,6],
 [2,5,5], [2,5,6],
 [2,6,6],
 [3,3,3], [3,3,4], [3,3,5], [3,3,6],
 [3,4,4], [3,4,5], [3,4,6],
 [3,5,5], [3,5,6],
 [3,6,6],
 [4,4,4], [4,4,5], [4,4,6],
 [4,5,5], [4,5,6],
 [4,6,6],
 [5,5,5], [5,5,6],
 [5,6,6],
 [6,6,6]

Satz 47. Die Anzahl der Kombinationen mit Wiederholung von m Dingen zur Klasse n ist gleich $\binom{m+n-1}{n}$.

Die Beweismethode von Satz 46 versagt hier, denn für beliebige Abbildungen $N \rightarrow M$ können sowohl die Äquivalenzklassen als auch die Wertebereiche verschiedene Mächtigkeiten haben:

$$\begin{aligned} [3, 4, 5] &= \{(3, 4, 5), (3, 5, 4), (4, 3, 5), (4, 5, 3), (5, 3, 4), (5, 4, 3)\}, & |\{3, 4, 5\}| &= 3, \\ [3, 3, 5] &= \{(3, 3, 5), (3, 5, 3), (5, 3, 3)\}, & |\{3, 3, 5\}| &= 2. \end{aligned}$$

Der Beweis gelingt nur durch einen Kunstgriff.

Beweis. Laut Definition müssen wir die Anzahl der Äquivalenzklassen von Abbildungen $N \rightarrow M$ abzählen, wobei M und N Mengen mit den Mächtigkeiten m und n sind. Wir wählen

$$M = \{1, 2, \dots, m\}, \quad N = \{1, 2, \dots, n\}.$$

Eine Abbildung $f : N \rightarrow M$ stellen wir durch das n -Tupel

$$(f(1), \dots, f(n)) \in M^n$$

dar. Zwei n -Tupel sind äquivalent, wenn eines aus dem anderen durch eine Vertauschung der Einträge hervorgeht. Zu jedem n -Tupel findet man ein äquivalentes, in dem die Einträge in aufsteigender Reihenfolge angeordnet sind, also

$$g(1) \leq g(2) \leq \dots \leq g(n).$$

Dabei gibt es in jeder Äquivalenzklasse nur ein aufsteigendes n -Tupel. Statt Äquivalenzklassen können wir also aufsteigende n -Tupel in M^n abzählen.

Da wir auch dafür noch keine Formel haben, ordnen wir jedem aufsteigenden n -Tupel eine Folge von Punkten und Strichen zu, in der genau n Punkte und $m - 1$ Striche vorkommen. Die Anzahl der Punkte vor dem ersten Strich gibt die Anzahl der Einsen in unserem n -Tupel an, die Anzahl der Punkte zwischen dem ersten und dem zweiten Strich die Anzahl der Zweien usw., bis schließlich die Anzahl der Punkte nach dem $(m - 1)$ ten Strich die Anzahl der Zahlen m angibt. Nach dieser Regel wird z. B. dem Septupel

$$(2, 2, 2, 3, 4, 4, 6)$$

aus der Menge $\{1, 2, \dots, 6\}^7$ die Folge

$$|\bullet\bullet\bullet|\bullet|\bullet\bullet|\bullet$$

zugeordnet. Man überzeugt sich leicht, dass auf diese Weise eine bijektive Abbildung zwischen aufsteigenden n -Tupeln und Folgen von $m - 1$ Strichen und n Punkten hergestellt wird. Es genügt also, diese Folgen abzuzählen.

Eine solche Zeichenfolge ist dadurch festgelegt, dass wir aus der Menge der $(m - 1) + n$ Stellen diejenigen n Stellen auswählen, an die wir die Punkte setzen. Die Anzahl solcher Teilmengen ist nach Definition der Binomialkoeffizienten gleich $\binom{(m-1)+n}{n}$. \square

5 Rationale Zahlen

5.1 Operationen mit rationalen Zahlen

Durch die Erweiterung des Bereiches \mathbf{N} der natürlichen Zahlen zum Bereich \mathbf{Z} der ganzen Zahlen wurde die Subtraktion uneingeschränkt ausführbar. Man würde gern eine zweite Erweiterung vornehmen, um auch die Division uneingeschränkt ausführbar zu machen. Die Elemente des neuen Zahlbereichs \mathbf{Q} nennt man rationale Zahlen.

Annahme 4. *Es gibt eine Menge \mathbf{Q} mit Operationen Addition und Multiplikation, so dass \mathbf{Z} eine Teilmenge von \mathbf{Q} ist und dass die Rechenoperationen für rationale Zahlen, wenn wir sie auf ganze Zahlen anwenden, mit den früher betrachteten Operationen übereinstimmen. Außerdem gelten für beliebige Zahlen r , s und t in \mathbf{Q} die gewohnten Kommutativ-, Assoziativ- und Distributivgesetze*

$$\begin{aligned}r + s &= s + r, & r \cdot s &= s \cdot r, \\(r + s) + t &= r + (s + t), & (r \cdot s) \cdot t &= r \cdot (s \cdot t), \\r \cdot (s + t) &= r \cdot s + r \cdot t.\end{aligned}\tag{12}$$

Des Weiteren ist die Subtraktion auch in \mathbf{Q} uneingeschränkt ausführbar, und es wird auch die Division uneingeschränkt ausführbar, das heißt, für beliebige Zahlen r und $s \neq 0$ in \mathbf{Q} gibt es genau eine Zahl $t \in \mathbf{Q}$, so dass $r = s \cdot t$ gilt. Diese Zahl t nennt man dann den Quotienten von r und s , abgekürzt $r : s$.

Für alle $t \in \mathbf{Q}$ gilt

$$t \cdot 0 = 0.$$

Dies folgt aus den obigen Gesetzen wegen

$$t \cdot 0 = t \cdot (0 + 0) = t \cdot 0 + t \cdot 0$$

und der Eindeutigkeit der Differenz gelten $0 \cdot t = t \cdot 0 = 0$. Die Gleichung $r = 0 \cdot t$ hat also für gegebenes $r \neq 0$ keine Lösung, während im Fall $r = 0$ jedes t eine Lösung wäre. Darum kann man die Existenz von $r : 0$ nicht verlangen.

Wir behaupten, dass für jedes $r \in \mathbf{Q}$ gilt

$$r \cdot 1 = r.$$

Wegen $1 \neq 0$ gibt es nämlich den Quotienten $u = r : 1$, so dass $u \cdot 1 = r$, und aus dem Assoziativgesetz folgt $(u \cdot 1) \cdot 1 = u \cdot (1 \cdot 1) = u \cdot 1$. Nun folgt aus der Definition von Quotienten auch, dass für beliebige $r \in \mathbf{Q}$ gilt

$$r : 1 = r, \quad r : r = 1.$$

Genau wie im Fall der ganzen Zahlen folgert man wieder das rechte Distributivgesetz

$$(s + t) \cdot r = s \cdot r + t \cdot r$$

sowie die Rechengesetze für die Subtraktion einschließlich der Vorzeichenregeln für die Multiplikation, die wir hier nicht noch einmal anführen wollen. Diesmal kommt es uns mehr auf die Rechengesetze der Division an, nämlich:

$$\begin{aligned} (r \cdot s) : t &= r \cdot (s : t), & (r : s) : t &= r : (s \cdot t), & (r : s) \cdot t &= r : (s : t), \\ (r + s) : t &= r : t + s : t, & (r - s) : t &= r : t - s : t, & & (13) \\ r : (-s) &= -r : s, & (-r) : (-s) &= r : s. \end{aligned}$$

Dabei wird vorausgesetzt, dass die Variablen, durch die dividiert wird, von Null verschiedene Zahlen bezeichnen. Man beachte, dass hier nur das rechte Distributivgesetz gilt. Die Beweise der Assoziativgesetze sind eine genaue Kopie der Beweise für die analogen Gesetze (5) der Subtraktion, wobei man $+$ durch \cdot und $-$ durch $:$ zu ersetzen hat, während man die Distributivgesetze und Vorzeichenregeln der Division mit Hilfe ihrer Definition und den entsprechenden Gesetzen der Multiplikation herleitet. Wir führen hier als Beispiel den Beweis des ersten Assoziativgesetzes vor, wobei wir natürlich $t \neq 0$ voraussetzen:

Bezeichnen wir $s : t$ mit u , so ist u nach Definition diejenige Zahl, für die $s = t \cdot u$ gilt. Dann ist aber nach Kommutativ- und Assoziativgesetz der Multiplikation

$$r \cdot s = r \cdot (t \cdot u) = r \cdot (u \cdot t) = (r \cdot u) \cdot t,$$

also nach Definition $(r \cdot s) : t = r \cdot u$, und durch Einsetzen folgt die gewünschte Behauptung. Insbesondere kann man durch eine Zahl $t \neq 0$ dividieren, indem man mit ihrem *Kehrwert*⁴¹ $1 : t$ multipliziert.

Als Spezialfall des Distributivgesetzes von Division und Subtraktion erhalten wir

$$(-s) : t = -s : t.$$

Damit folgt die zweite Vorzeichenregel in (13) aus der ersten. Diese ist nach Definition von Quotienten äquivalent zu

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

und folgt somit aus einer Vorzeichenregel der Multiplikation und den Assoziativgesetzen in (13).

⁴¹lat.: ihrem *Reziproken*

Aus Annahme 4 können wir auch Regeln für das Rechnen mit Quotienten herleiten, die uns auf eine Idee für die Konstruktion der rationalen Zahlen bringen sollen. Am einfachsten sind die für Multiplikation und Division:

$$\begin{aligned}(r : s) \cdot (t : u) &= (r \cdot t) : (s \cdot u), \\ (r : s) : (t : u) &= (r \cdot u) : (s \cdot t).\end{aligned}\tag{14}$$

Der Beweis ist wieder eine Kopie der analogen Regeln (7) für Differenzen ganzer Zahlen, wobei man $+$ durch \cdot und $-$ durch $:$ ersetzt. Insbesondere sieht man, dass das Produkt von Null verschiedener Zahlen s und u wieder von null verschieden ist und das Produkt ihrer Kehrwerte gleich dem Kehrwert des Produktes ist. Als Spezialfall dieser Regeln erhalten wir

$$\begin{aligned}r : s &= (r : s) \cdot 1 = (r : s) \cdot (u : u) = (r \cdot u) : (s \cdot u), \\ t : u &= 1 \cdot (t : u) = (s : s) \cdot (t : u) = (s \cdot t) : (s \cdot u).\end{aligned}$$

Die Regeln für die Addition und Subtraktion

$$\begin{aligned}(r : s) + (t : u) &= (r \cdot u + s \cdot t) : (s \cdot u), \\ (r : s) - (t : u) &= (r \cdot u - s \cdot t) : (s \cdot u)\end{aligned}\tag{15}$$

folgen nun mit Hilfe der Distributivgesetze, z. B.

$$(r : s) + (t : u) = (r \cdot u) : (s \cdot u) + (s \cdot t) : (s \cdot u) = (r \cdot u + s \cdot t) : (s \cdot u).$$

Ähnlich beweist man die Regel für die Subtraktion.

Auch der Bereich der rationalen Zahlen soll nicht unnötig groß sein.

Annahme 5. *Jedes Element von \mathbf{Q} ist ein Quotient⁴² ganzer Zahlen.*

Dies ist keine einschränkende Bedingung. Angenommen, wir haben einen Zahlbereich \mathbf{Q} konstruiert, der die Annahme 4 erfüllt. Eine Teilmenge von \mathbf{Q} , die \mathbf{Z} enthält und abgeschlossen unter Addition, Multiplikation, Subtraktion und Division ist, erfüllt ebenfalls die Annahme 4 und zusätzlich die Annahme 5. Die obigen Rechengesetze zeigen, dass wir dafür die Menge aller Quotienten ganzer Zahlen nehmen können.

Wir wollen auch für rationale Zahlen über eine Kleiner-Gleich-Relation verfügen. Den Beweis ihrer Existenz verschieben wir wieder auf später.

⁴²Daher die Wahl des Buchstabens \mathbf{Q} .

Annahme 6. Es gibt eine Ordnung auf der Menge der rationalen Zahlen, die bei Anwendung auf ganze Zahlen mit der bereits betrachteten Kleiner-Gleich-Relation übereinstimmt (weshalb wir sie mit dem selben Symbol \leq bezeichnen), so dass die **Monotoniegesetze** aus Annahme 3 und⁴³ Folgerung 17 auch für rationale Zahlen r, s, t und u gelten, nämlich:

$$\text{Wenn } r \leq s \text{ und } t \leq u, \text{ dann } r + t \leq s + u, \quad (16)$$

$$\text{wenn } r \leq s \text{ und } u \geq 0, \text{ dann } r \cdot u \leq s \cdot u. \quad (17)$$

Aus (16) folgt wie schon im Fall der ganzen Zahlen, dass

$$r \leq s \iff -s \leq -r.$$

Damit kann man die Spezialfälle von (17) für $r = 0$ bzw. $s = 0$ ergänzen durch die Regel

$$\text{wenn } r \leq 0 \text{ und } s \leq 0, \text{ dann } r \cdot s \geq 0.$$

Wir definieren den (*absoluten*) Betrag einer rationalen Zahl r , abgekürzt $|r|$, durch

$$|r| = \begin{cases} r, & \text{wenn } r \geq 0, \\ -r, & \text{wenn } r < 0. \end{cases}$$

Dieser ist immer nichtnegativ, und durch eine Unterscheidung von vier Fällen findet man die Regel

$$|r \cdot s| = |r| \cdot |s|.$$

Eine kompliziertere Fallunterscheidung (siehe Aufgabe 63) beweist die Dreiecksungleichung

$$|r + s| \leq |r| + |s|.$$

Die Aussage $r < s$ bedeutet wieder, dass $r \leq s$ und $r \neq s$ ist. Eine Zahl r heißt positiv, wenn $r > 0$ ist, und negativ, wenn $r < 0$ ist. Wir sehen, dass das Produkt zweier positiver oder zweier negativer rationaler Zahlen positiv ist. Außerdem ist der Kehrwert $r = 1 : u$ einer positiven Zahl u positiv ist, denn sonst würde aus (17) mit $s = 0$ folgen, dass $1 \leq 0$.

Es lassen sich weitere Folgerungen ableiten, so z. B. für positive rationale Zahlen s und u

$$r : s \leq t : u \iff r \cdot u \leq t \cdot s. \quad (18)$$

Multiplizieren wir nämlich entsprechend der Regel (17) beide Seiten der linken Ungleichung mit $s \cdot u$, so erhalten wir die rechte. Ersetzen wir u durch $1 : s$ und s durch $1 : u$, so ergibt sich die umgekehrte Implikation. Als Spezialfall erhalten wir für positive rationale Zahlen s und u

$$1 : s \leq 1 : u \iff u \leq s.$$

⁴³Mit etwas mehr Arbeit könnte man (17) aus den anderen Annahmen folgern.

5.2 Konstruktion der rationalen Zahlen

Wir wissen noch nicht, ob die Annahmen 4 und 5 richtig sind. Nehmen wir noch für einen Augenblick an, das sei der Fall. Dann ist die durch

$$q(a, b) = a : b$$

gegebene Abbildung $q : \mathbf{Z} \times (\mathbf{Z} \setminus \{0\}) \rightarrow \mathbf{Q}$ nach Annahme 5 und der letzten Regel aus (13) surjektiv. Um festzustellen, ob sie injektiv ist, betrachten wir Paare (a, b) und (c, d) in $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ mit der Eigenschaft $q(a, b) = q(c, d)$, das heißt

$$a : b = c : d.$$

Nach Definition der Division und den auf Annahme 4 beruhenden Rechengesetzen folgt

$$a = b \cdot (c : d) = (b \cdot c) : d,$$

also

$$a \cdot d = b \cdot c. \tag{19}$$

Da wir die Umformungen in umgekehrter Reihenfolge vornehmen können, ist die letzte Bedingung äquivalent zu $q(a, b) = q(c, d)$. Nun sieht man, dass die Abbildung q nicht injektiv ist, denn es gilt z. B. $q(1, 3) = q(2, 6)$. Für jedes Element r von \mathbf{Q} haben wir die Menge

$$\{(a, b) \in \mathbf{Z} \times (\mathbf{Z} \setminus \{0\}) \mid q(a, b) = r\}, \tag{20}$$

die wegen der Surjektivität von p nicht leer ist.

Wenn wir auf der Menge $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ die Relation der Quotientengleichheit, abgekürzt \approx , dadurch definieren, dass

$$(a, b) \approx (c, d), \text{ wenn } q(a, b) = q(c, d),$$

so ist \approx eine Äquivalenzrelation. Die entsprechenden Äquivalenzklassen sind die Mengen in (20).

Nun wollen wir uns nicht mehr auf Annahmen verlassen und mit der Konstruktion der rationalen Zahlen beginnen. Glücklicherweise können wir die Relation \approx mittels (19) und die Rechenoperationen mittels (14) und (15) beschreiben, ohne die gesuchte Menge \mathbf{Q} zu benutzen.

Definition 39. *Wir definieren die Relation der Quotientengleichheit, abgekürzt \approx , auf der Menge $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ wie folgt:*

$$(a, b) \approx (c, d) \text{ genau dann, wenn } a \cdot d = b \cdot c.$$

Wir definieren Operationen $+$ und \cdot auf $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ wie folgt:

$$\begin{aligned}(a, b) + (c, d) &= (a \cdot d + b \cdot c, b \cdot d), \\ (a, b) \cdot (c, d) &= (a \cdot c, b \cdot d).\end{aligned}$$

Satz 48. (i) Die Relation \approx auf $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ ist eine Äquivalenzrelation.

(ii) Ist $(a, b) \approx (a', b')$ und $(c, d) \approx (c', d')$, so gilt

$$\begin{aligned}(a, b) + (c, d) &\approx (a', b') + (c', d'), \\ (a, b) \cdot (c, d) &\approx (a', b') \cdot (c', d').\end{aligned}$$

Beweis. Den größten Teil des Beweises von Aussage (i) erhalten wir aus dem Beweis der analogen Aussage von Satz 39, indem wir $+$ durch \cdot ersetzen: Die Relation ist *reflexiv*, denn die Bedingung $(a, b) \approx (a, b)$ bedeutet nach Definition, dass $a \cdot b = b \cdot a$, was wegen der Kommutativität der Multiplikation erfüllt ist. Die Relation \approx ist *symmetrisch*, d. h.

$$\text{wenn } (a, b) \approx (c, d), \text{ dann } (c, d) \approx (a, b),$$

denn nach dem Kommutativgesetz der Multiplikation gilt

$$\text{wenn } a \cdot d = b \cdot c, \text{ dann } c \cdot b = d \cdot a.$$

Die Relation \approx ist *transitiv*, d. h.

$$\text{wenn } (a, b) \approx (c, d) \text{ und } (c, d) \approx (e, f), \text{ dann } (a, b) \approx (e, f).$$

Diese Aussage bedeutet:

$$\text{Wenn } a \cdot d = b \cdot c \text{ und } c \cdot f = d \cdot e, \text{ dann } a \cdot f = b \cdot e.$$

In der Tat folgt aus den in dieser Aussage genannten Voraussetzungen, dass

$$(a \cdot d) \cdot (c \cdot f) = (b \cdot c) \cdot (d \cdot e),$$

also nach den Rechengesetzen (4)

$$((a \cdot f) \cdot c) \cdot d = ((b \cdot e) \cdot c) \cdot d.$$

Da d nach Voraussetzung nicht Null ist, gilt wegen Folgerung 16, dass

$$(a \cdot f) \cdot c = (b \cdot e) \cdot c.$$

Ist $c \neq 0$, so können wir auch c kürzen und sind fertig. Ist hingegen $c = 0$, so erhalten wir mit Folgerung 15, dass $a = 0$ und $e = 0$, also ist auch in diesem Fall unsere Behauptung richtig.

(ii) Es sei $(a, b) \approx (a', b')$ und $(c, d) \approx (c', d')$, das heißt

$$a \cdot b' = b \cdot a' \quad \text{und} \quad c \cdot d' = d \cdot c'.$$

Der Beweis, dass dann $(a, b) \cdot (c, d) \approx (a', b') \cdot (c', d')$, ergibt sich wieder aus dem analogen Beweis von Satz 39(ii), indem man $+$ durch \cdot ersetzt, und braucht hier nicht vorgeführt zu werden.

Nun beweisen wir, dass

$$(a, b) + (c, d) \approx (a', b') + (c', d').$$

Dies bedeutet nach Definition der Addition, dass

$$(ad + bc, bd) \approx (a'd' + b'c', b'd'),$$

und dies bedeutet wiederum nach Definition der Quotientengleichheit, dass

$$(ad + bc)b'd' = bd(a'd' + b'c'),$$

wobei wir das Zeichen für die Multiplikation ganzer Zahlen wie üblich weglassen. Zum Beweis multiplizieren wir beide Seiten der gegebenen Gleichungen mit dd' bzw. bb' und erhalten

$$(ab')(dd') = (ba')(dd'), \quad (cd')(bb') = (dc')(bb').$$

Addieren wir die linken und die rechten Seiten, so folgt die behauptete Gleichung mit Hilfe der Rechengesetze (4). \square

Nun können wir die rationalen Zahlen definieren. Jeder Äquivalenzklasse von Paaren ganzer Zahlen bezüglich der Quotientengleichheit müssten wir eine rationale Zahl zuordnen. Anstatt uns diese von irgendwoher zu beschaffen, deklarieren wir einfach die Äquivalenzklassen selbst als rationale Zahlen.

Definition 40. Die Menge \mathbf{Q} ist die Menge der Äquivalenzklassen in $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ bezüglich der Relation der Quotientengleichheit. Die Elemente von \mathbf{Q} nennen wir rationale Zahlen, die Klasse eines Paares (a, b) bezeichnen wir mit $\frac{a}{b}$. Wir definieren die Addition und Multiplikation rationaler Zahlen durch die Festlegungen

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{a \cdot d + b \cdot c}{b \cdot d}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{a \cdot c}{b \cdot d}. \end{aligned}$$

Der vorangehende Satz zeigt, dass diese Definition korrekt ist.

Traditionell spricht man von äquivalenten Brüchen, die die selbe Zahl darstellen. Inkonsequenter Weise benutzt man aber das Symbol des Bruches als Bezeichnung der Zahl, was z. B. in Gleichungen wie $\frac{1}{2} = \frac{2}{4}$ deutlich wird. Für eine korrekte Darlegung braucht man eigentlich ein weiteres Symbol, um einen Bruch im Unterschied von der durch ihn dargestellten Zahl zu bezeichnen. Wir brauchen das nicht, denn für uns ist ein *Bruch* einfach ein geordnetes Paar $(a, b) \in \mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$, sein *Zähler* ist a und sein *Nenner* ist b .

Nun können wir den größten Teil von Annahme 4 beweisen.

Satz 49. (i) Für beliebige rationale Zahlen r, s und t gelten die Rechengesetze (12).

(ii) Die Subtraktion von rationalen Zahlen ist uneingeschränkt ausführbar.

(iii) Die Division von rationalen Zahlen ist mit Ausnahme der Division durch $\frac{0}{1}$ uneingeschränkt ausführbar.

(iv) Die Abbildung $j : \mathbf{Z} \rightarrow \mathbf{Q}$, die durch $j(a) = \frac{a}{1}$ gegeben ist, ist injektiv, und es gilt

$$j(a + b) = j(a) + j(b), \quad j(a \cdot b) = j(a) \cdot j(b).$$

Beweis. (i) Wir beweisen z. B. das Distributivgesetz. Es sei

$$r = \frac{a}{b}, \quad s = \frac{c}{d}, \quad t = \frac{e}{f}.$$

Dann ist nach Definition

$$r \cdot (s + t) = \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f} \right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{a(cf + de)}{b(df)},$$

wobei wir rechts die Malzeichen der Kürze halber weglassen, und

$$r \cdot s + r \cdot t = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{(ac)(bf) + (bd)(ae)}{(bd)(bf)}.$$

Laut Definition der Quotientengleichheit bleibt zu zeigen, dass

$$(a(cf + de))((bd)(bf)) = (b(df))((ac)(bf) + (bd)(ae)).$$

Wenn man beide Seiten mit Hilfe des Distributivgesetzes ausmultipliziert, so sind die Terme auf beiden Seiten aufgrund des Assoziativ- und Kommutativgesetzes gleich.

Die Beweise der anderen Rechengesetze für die Multiplikation ergeben sich wieder aus den Beweisen für die Addition ganzer Zahlen in Satz 40, indem man $+$ durch \cdot ersetzt. Das Kommutativgesetz der Addition ist offensichtlich, und der Beweis des Assoziativgesetzes ist Gegenstand von Aufgabe 64.

(ii) Wegen (14) vermuten wir, dass die Differenz von rationalen Zahlen $r = \frac{a}{b}$ und $s = \frac{c}{d}$ gleich

$$\frac{a \cdot d - b \cdot c}{b \cdot d}$$

ist, und in der Tat gilt nach Teil (i)

$$\frac{a \cdot d - b \cdot c}{b \cdot d} + \frac{c}{d} = \frac{(ad - bc) \cdot d + (bd)c}{(bd)d} = \frac{(ad)d}{(bd)d} = \frac{a}{b}.$$

(iii) Wegen (14) vermuten wir, dass für $\frac{e}{f} \neq \frac{0}{1}$ der Quotient von $s = \frac{c}{d}$ und $t = \frac{e}{f}$ gleich

$$\frac{c \cdot f}{d \cdot e}$$

ist. In der Tat ist laut Definition $e \cdot 1 \neq f \cdot 0$, also darf $d \cdot e$ im Nenner stehen, und

$$\frac{c \cdot f}{d \cdot e} \cdot \frac{e}{f} = \frac{(cf)e}{(de)f} = \frac{c}{d}.$$

(iv) Für $a, b \in \mathbf{Z}$ gilt nach Definition

$$\begin{aligned} \frac{a}{1} + \frac{b}{1} &= \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} = \frac{a + b}{1}, \\ \frac{a}{1} \cdot \frac{b}{1} &= \frac{a \cdot b}{1 \cdot 1} = \frac{a \cdot b}{1}. \end{aligned}$$

Ist $j(a) = j(b)$, so ist nach Definition $a \cdot 1 = 1 \cdot b$, also $a = b$. Somit ist j injektiv. \square

Damit ist Annahme 4 mit Ausnahme der Relation $\mathbf{Z} \subset \mathbf{Q}$ bewiesen, also auch die daraus gezogenen Schlüsse:

Folgerung 20. *Für alle rationalen Zahlen gelten die Rechengesetze der Subtraktion (vgl. (5)) und der Division (13). Außerdem gelten die Regeln (14) und (15) für rationale Zahlen an Stelle von ganzen Zahlen.*

Haben a und b den gemeinsamen Teiler d , gibt es also ganze Zahlen u und v , so dass $a = du$ und $b = dv$, so ist $(a, b) \approx (u, v)$, also $\frac{a}{b} = \frac{u}{v}$, und man sagt, dass (u, v) durch *Kürzen* aus (a, b) und umgekehrt (a, b) durch *Erweitern* aus (u, v) hervorgeht. Zu jedem Bruch findet man einen äquivalenten, bei dem

Zähler und Nenner teilerfremd sind, z. B. indem man durch den größten gemeinsamen Teiler kürzt. Einen solchen Bruch nennt man *unkürzbar*. Wegen $(a, b) \approx (-a, -b)$ kann man in jeder Äquivalenzklasse $\frac{a}{b}$ einen unkürzbaren Vertreter mit positivem Nenner wählen, und mit Hilfe von elementarer Zahlentheorie kann man zeigen, dass dieser eindeutig bestimmt ist.

Brüche heißen *gleichnamig*, wenn sie den selben Nenner haben. In diesem Fall vereinfacht sich die Summe durch Kürzung:

$$\frac{a}{b} + \frac{c}{b} = \frac{a \cdot b + b \cdot c}{b \cdot b} = \frac{a + c}{b}.$$

Haben die Nenner zweier Brüche (a, b) und (c, d) ein gemeinsames Vielfaches m , so findet man einen Vertreter für die Summe mit dem Nenner m . Es gibt dann nämlich ganze Zahlen x und y , so dass $m = bx$ und $m = dy$, und es folgt

$$\frac{a}{b} + \frac{c}{d} = \frac{ax}{m} + \frac{cy}{m} = \frac{ax + cy}{m}.$$

Insbesondere kann man für m das kleinste gemeinsame Vielfache von b und d nehmen, welches als *Hauptnenner* der beiden Brüche bezeichnet wird. In der elementaren Zahlentheorie lernt man, wie man das kleinste gemeinsame Vielfache durch einen effizienten Algorithmus bestimmen kann.

Nun müssen wir noch die Kleiner-Gleich-Relation auf \mathbf{Q} definieren. Wenn Annahme 6 richtig ist, dann ist für ganze Zahlen a, b, c und d , von denen b und d nicht Null sind, die Aussage

$$a : b \leq c : d$$

nach (18) äquivalent zu

$$a \cdot d \leq b \cdot c.$$

Da in der letzteren Ungleichung nur ganze Zahlen vorkommen, für die die Kleiner-Gleich-Relation ja mit der bisher betrachteten übereinstimmen soll, können wir diese Ungleichung zur Definition der genannten Relation auf den rationalen Zahlen benutzen, vorausgesetzt, die Gültigkeit dieser Ungleichung hängt nicht von der Wahl der Repräsentanten ab.

Satz 50. *Es seien (a, b) , (c, d) , (a', b') und (c', d') Elemente von $\mathbf{Z} \times (\mathbf{N} \setminus \{0\})$. Ist $(a, b) \approx (a', b')$ und $(c, d) \approx (c', d')$, so gilt*

$$\text{genau dann } a \cdot d \leq b \cdot c, \text{ wenn } a' \cdot d' \leq b' \cdot c'.$$

Für den Beweis benötigen wir noch eine Kürzungsregel für Ungleichungen zwischen ganzen Zahlen.

Lemma 5. Für alle ganzen Zahlen a, b und c gilt:

Wenn $a \cdot c \leq b \cdot c$ und $c > 0$, dann $a \leq b$.

Beweis. Es gibt zwei Fälle. Ist $a \cdot c = b \cdot c$, so gilt $a = b$ nach Folgerung 16. Ist hingegen $a \cdot c < b \cdot c$, so behaupten wir, dass sogar $a < b$ folgt. Wäre nämlich $a \geq b$, so wäre nach Folgerung 17 $a \cdot c \geq b \cdot c$ entgegen unserer Voraussetzung. \square

Beweis des Satzes. Die Quotientengleichheit $(a, b) \approx (a', b')$ bedeutet

$$a \cdot b' = b \cdot a'.$$

Angenommen, es gilt die Ungleichung

$$a \cdot d \leq b \cdot c.$$

Um die obige Gleichheit anwenden zu können, benutzen wir Satz 17(ii) und erhalten wegen $b' > 0$

$$a \cdot d \cdot b' \leq b \cdot c \cdot b'.$$

Durch Einsetzen ergibt sich

$$b \cdot a' \cdot d \leq b \cdot c \cdot b',$$

und mit Lemma 5 folgt wegen $b > 0$, dass

$$a' \cdot d \leq b' \cdot c.$$

Analog folgert man hieraus mit Hilfe von $(c, d) \approx (c', d')$ die Ungleichung

$$a' \cdot d' \leq b' \cdot c'.$$

Die Umkehrung führt man durch Vertauschung der Variablen mit und ohne Strich auf das Beweisene zurück. \square

Der Satz rechtfertigt folgende Definition.

Definition 41. Wir definieren eine Relation \leq auf der Menge \mathbf{Q} , indem wir für beliebige ganze Zahlen a, b, c und d , wobei $b > 0$ und $d > 0$ ist, festlegen:

$$\frac{a}{b} \leq \frac{c}{d}, \text{ wenn } a \cdot d \leq b \cdot c.$$

Trotz der Einschränkung $b > 0, d > 0$ ist die Relation \leq zwischen allen rationalen Zahlen definiert, denn es gilt $\frac{a}{b} = \frac{-a}{-b}$. Nun wollen wir Annahme 6 beweisen.

Satz 51. (i) Die Relation \leq auf der Menge \mathbf{Q} ist eine Ordnung.

(ii) Für rationale Zahlen gelten die Rechenregeln (16) und (17).

(iii) Ist $j : \mathbf{Z} \rightarrow \mathbf{Q}$ die Abbildung aus Satz 49, so gilt für beliebige ganze Zahlen a und b

genau dann $j(a) \leq j(b)$, wenn $a \leq b$.

Beweis. Für Teil (i) müssen wir die drei Eigenschaften nachprüfen, die eine Ordnung ausmachen. Dabei schreiben wir die vorkommenden rationalen Zahlen in der Form $r = \frac{a}{b}$, $s = \frac{c}{d}$ und $t = \frac{e}{f}$, wobei $b > 0$, $d > 0$ und $f > 0$. Die *Totalität* besagt, dass für beliebige rationale Zahlen r und s gilt

$$r \leq s \quad \text{oder} \quad s \leq r,$$

das heißt

$$a \cdot d \leq b \cdot c \quad \text{oder} \quad c \cdot b \leq d \cdot a.$$

Dies gilt in der Tat wegen der Totalität der Kleiner-Gleich-Relation auf \mathbf{Z} (Satz 42) und der Kommutivität.

Die *Antisymmetrie* besagt, dass für alle rationalen Zahlen r und s gilt:

Wenn $r \leq s$ und $s \leq r$, dann $r = s$.

Dies bedeutet laut Definition 41:

Wenn $a \cdot d \leq b \cdot c$ und $c \cdot b \leq d \cdot a$, dann $a \cdot d = b \cdot c$.

Letzteres gilt wegen der Antisymmetrie der Kleiner-Gleich-Relation auf \mathbf{Z} (Satz 42) und der Kommutivität.

Die *Transitivität* besagt, dass für alle rationalen Zahlen r , s und t gilt:

Wenn $r \leq s$ und $s \leq t$, dann $r \leq t$.

Dies bedeutet:

Wenn $a \cdot d \leq b \cdot c$ und $c \cdot f \leq d \cdot e$, dann $a \cdot f \leq b \cdot e$.

Wenden wir Satz 17(ii) auf die ersten beiden Ungleichungen an, so erhalten wir wegen $f > 0$ und $b > 0$, dass

$$(a \cdot d) \cdot f \leq (b \cdot c) \cdot f, \quad b \cdot (c \cdot f) \leq b \cdot (d \cdot e).$$

Wegen der Transitivität der Kleiner-Gleich-Relation auf \mathbf{Z} folgt

$$(a \cdot d) \cdot f \leq b \cdot (d \cdot e),$$

und mit Lemma 5 folgt wegen $d > 0$ die dritte Ungleichung. Die behauptete Implikation ist also wahr.

(ii) Führen wir zusätzlich die Bezeichnung $u = \frac{g}{h}$ ein, wobei $h > 0$, so bedeutet $r \leq s$ und $t \leq u$, dass

$$a \cdot d \leq b \cdot c, \quad e \cdot h \leq f \cdot g.$$

Wegen

$$r + t = \frac{a \cdot f + b \cdot e}{b \cdot f}, \quad s + u = \frac{c \cdot h + d \cdot g}{d \cdot h}$$

bedeutet die zu beweisende Ungleichung $r + t \leq s + u$, dass

$$(a \cdot f + b \cdot e) \cdot (d \cdot h) \leq (b \cdot f) \cdot (c \cdot h + d \cdot g).$$

Dies ergibt sich in der Tat, wenn wir entsprechend Satz 17(ii) beide Seiten der ersten gegebenen Ungleichung mit $f \cdot h$ und die der zweiten mit $b \cdot d$ multiplizieren und die erhaltenen Ungleichungen entsprechend Satz 17(i) addieren.

(iii) Mit Hilfe der Definition der Abbildung j wird die Aussage $j(a) \leq j(b)$ zu $\frac{a}{1} \leq \frac{b}{1}$. Nach Definition 41 bedeutet dies $a \cdot 1 \leq 1 \cdot b$, und das ist äquivalent zu $a \leq b$. \square

Bemerkung. Ähnlich wie bei der Einführung der ganzen Zahlen hat sich unser Wunsch, dass \mathbf{Z} eine Teilmenge von \mathbf{Q} sei, nicht erfüllt, aber auf Grund von Satz 49(iv) und 51(iii) können wir mit den Zahlen $\frac{a}{1}$ genau so rechnen wie mit den ganzen Zahlen a selbst. Darum identifiziert man gewöhnlich a mit $\frac{a}{1}$ und somit \mathbf{Z} mit einer Teilmenge von \mathbf{Q} . Ähnlich wie die Bezeichnung $[m, n]$ wäre nun auch die Bezeichnung $\frac{a}{b}$ nicht mehr nötig, weil $a : b$ die selbe rationale Zahl bezeichnet. Aus Gründen der Platzersparnis hat aber im Gegenteil der Bruchstrich fast das Divisionszeichen verdrängt, und zwar nicht nur für Quotienten ganzer Zahlen.⁴⁴ Zur Vermeidung von Ober- und Unterlängen benutzt man auch geneigte Bruchstriche wie bei $1/2$.

Eine rationale Zahl ist genau dann nichtnegativ, wenn sie sich in der Form $\frac{m}{n}$ mit natürlichen Zahlen m und $n \neq 0$ schreiben lässt. Solche Zahlen nennt man *Bruchzahlen*. Nach Satz 34 gibt es natürliche Zahlen q und r , so dass $m = qn + r$ und $r < n$, also ist

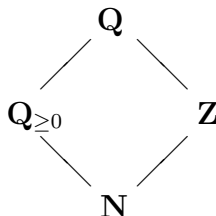
$$\frac{m}{n} = q + \frac{r}{n}.$$

Anstelle von Ausdrücken wie $1 + \frac{1}{2}$ schreibt man traditionell $1\frac{1}{2}$ und nennt dies eine *gemischte Zahl*. Brüche (m, n) mit $m < n$ nennt man *echte Brüche*.

⁴⁴So schreibt man z. B. für $\frac{a}{b} : \frac{c}{d}$ auch den Doppelbruch $\frac{\frac{a}{b}}{\frac{c}{d}}$.

Sie stellen Bruchzahlen dar, die kleiner als 1 sind. Brüche mit dem Zähler 1 nennt man *Stammbrüche*.

Wir haben zuerst den Bereich \mathbf{N} der natürlichen Zahlen zum Bereich \mathbf{Z} der ganzen Zahlen erweitert, um die Subtraktion uneingeschränkt ausführbar zu machen, und diesen dann zum Bereich \mathbf{Q} der rationalen Zahlen, um das Selbe für die Division zu erreichen. In der Schule geht man entsprechend der Erfahrungswelt der Schüler umgekehrt vor: Man erweitert den Bereich der natürlichen Zahlen zunächst zum Bereich der Bruchzahlen, in dem die Division uneingeschränkt ausführbar ist, und diesen dann zum Bereich der rationalen Zahlen. Die Methoden sind analog zu den obigen und hängen im Wesentlichen davon ab, welche Umkehroperation man jeweils uneingeschränkt ausführbar machen will. Manchmal wird die Menge der Bruchzahlen mit $\mathbf{Q}_{\geq 0}$ bezeichnet.



Ganzzahlige Exponenten

Die Definition von Potenzen ganzer Zahlen mit natürlichen Exponenten verallgemeinert sich sofort auf Potenzen rationaler Zahlen, und die Beweise der Potenzgesetze sind hierfür gültig. Wir können einen Schritt weitergehen und für eine von Null verschiedene rationale Zahl r und eine ganze Zahl a die Potenz r^a definieren. Dazu sei $a = [m, n]$ mit natürlichen Zahlen m und n . Wir setzen

$$r^a = r^m : r^n.$$

Ist u der Kehrwert von r , so gilt $r^n u^n = (ru)^n = 1$, also $r^a = r^m u^n$. Wie für Potenzen von bijektiven Abbildungen einer Menge in sich selbst beweist man, dass die Definition nicht von der Wahl von m und n abhängt, und dass die Potenzgesetze

$$(rs)^a = r^a s^a, \quad r^{a+b} = r^a r^b, \quad r^{ab} = (r^a)^b.$$

für beliebige rationale Zahlen $r \neq 0$ und $s \neq 0$ und ganze Zahlen a und b gelten. Wir bewiesen hier z. B. das erste Potenzgesetz. Ist v der Kehrwert von s , so ist uv der von rs , und es gilt nach Definition und dem entsprechenden Potenzgesetz für natürliche Exponenten

$$(rs)^a = (rs)^m (uv)^n = r^m s^m u^n v^n, \quad r^a s^a = r^m u^n s^m v^n.$$

Nach dem Kommutativgesetz stimmen beide Ausdrücke überein.

5.3 Systembrüche

Die Addition oder der Vergleich von zwei Bruchzahlen kann erheblichen Rechenaufwand erfordern. Deshalb verwendet man in der Praxis stattdessen meist Dezimalbrüche, die eng mit dem Dezimalsystem zusammenhängen. Wir betrachten hier ein Stellenwertsystem mit beliebiger Grundzahl $g > 1$ und sprechen dann von *Systembrüchen*. Dies sind Ausdrücke der Form

$$c_{-j}g^{-j} + c_{-j+1}g^{-j+1} + \dots,$$

wobei j eine natürliche Zahl ist und die c_i für alle $i \geq -j$ g -adische Ziffern sind, von denen nur endlich viele nicht Null sind. Multiplizieren wir diesen Systembruch mit g^j , so erhalten wir eine natürliche Zahl. Mit dem Monotoniegesetz (17) ergibt sich, dass sich Satz 38 sinngemäß auf Systembrüche überträgt.

Leider lassen sich nicht beliebige Bruchzahlen $\frac{m}{n}$ auf diese Weise darstellen, denn aus $\frac{m}{n}g^j = d$ folgt für teilerfremde natürliche Zahlen m und n , dass n ein Teiler von g^j ist. Man kann aber jede Bruchzahl beliebig gut durch Systembrüche annähern.

Das geht praktisch durch schriftliche Division. Hier ist ein Beispiel im Ternärsystem (mit der Grundzahl 3), wobei wir auf die Kennzeichnung durch eine tiefgestellte 3 verzichten:

$$\begin{array}{r} 11:21 = 0,120102\dots \\ \underline{0} \\ 110 \\ \underline{21} \\ 120 \\ \underline{112} \\ 10 \\ \underline{0} \\ 100 \\ \underline{21} \\ 20 \\ \underline{0} \\ 200 \\ \underline{112} \\ 11 \end{array}$$

An dieser Stelle tritt der Rest 11_3 zum zweiten Mal auf, und von nun an wiederholen sich die Reste, also auch die Ziffern des abgerundeten Quotienten. Das Ergebnis unserer bisherigen Rechnung lautet übrigens

$$\frac{11_3}{21_3} = 0,120102 + \frac{0,000011_3}{21_3}.$$

Wir wollen zeigen, dass sich allgemein jede Bruchzahl $\frac{m}{n}$ durch einen Systembruch mit j Nachkommastellen bis auf einen Fehler von weniger als g^{-j} annähern lässt. Je größer j ist, umso kleiner ist laut Aufgabe 62 die Zahl g^{-j} . Man kann sogar für eine beliebig vorgegebene positive rationale Zahl ε eine ganze Zahl j finden, so dass $g^{-j} \leq \varepsilon$ ist. Nach der Bernoulli-Ungleichung

$$g^j \geq 1 + j(g - 1)$$

aus Aufgabe 30 (die man für natürliche Zahlen auch durch vollständige Induktion beweisen oder aus Satz 45 folgern kann) genügt es nämlich, $j \geq \frac{1}{\varepsilon(g-1)}$ zu nehmen.

Satz 52. *Es sei $g > 1$ eine natürliche Zahl. Sind m und $n \neq 0$ natürliche Zahlen, so gibt es für alle ganzen Zahlen i eindeutig bestimmte g -adische Ziffern c_i mit folgenden beiden Eigenschaften:*

- (i) Für genügend großes i ist $c_i = 0$,
- (ii) für alle ganzen Zahlen j gilt

$$\sum_{i=-j}^{\infty} c_i g^i \leq \frac{m}{n} < \sum_{i=-j}^{\infty} c_i g^i + g^{-j}.$$

Außerdem gilt dann:

- (iii) Es gibt beliebig kleine Zahlen i , für die $c_i \neq g - 1$ ist.
- (iv) Es gibt natürliche Zahlen $k > 0$ und $l > 0$, so dass für alle $i \leq -k$ gilt $c_i = c_{i-l}$.
- (v) Man kann k und l so wählen, dass $k + l \leq n$ oder $c_i = 0$ für $i \leq -k$.

Jede Folge von g -adischen Ziffern c_i mit den Eigenschaften (i), (iii) und (iv) kommt von einer Bruchzahl $\frac{m}{n}$.

Bemerkung. Aussage (iv) besagt, dass die Ziffernfolge ab der k ten Nachkommastelle periodisch ist. Nach Aussage (iii) kommt z. B. im Dezimalsystem keine Neunerperiode vor.

Beweis. Es seien m und n wie im Satz gegeben. Durch Subtraktion einer geeigneten natürlichen Zahl können wir den Beweis auf den Fall $\frac{m}{n} < 1$, d. h. $m < n$ zurückführen. In diesem Fall muss $c_i = 0$ für $i \geq 0$ sein, weil die linke Seite in (ii) sonst mindestens 1 wäre, und damit ist (i) automatisch erfüllt.

(ii). Nach Satz 34 gibt es natürliche Zahlen q_1 und r_1 , so dass

$$mg = q_1n + r_1, \quad r_1 < n.$$

Dabei gilt

$$q_1n \leq mg < ng, \quad \text{also} \quad q_1 < g.$$

Wir können nun mit q_1 anstelle von m fortfahren und erhalten nacheinander natürliche Zahlen $q_k < g$ und $r_k < n$, so dass

$$\begin{aligned} mg &= q_1n + r_1, \\ r_1g &= q_2n + r_2, \\ r_2g &= q_3n + r_3, \\ &\dots \end{aligned}$$

Dividieren wir beide Seiten durch ng , so erhalten wir

$$\begin{aligned} \frac{m}{n} &= \left(q_1 + \frac{r_1}{n} \right) g^{-1}, \\ \frac{r_1}{n} &= \left(q_2 + \frac{r_2}{n} \right) g^{-1}, \\ \frac{r_2}{n} &= \left(q_3 + \frac{r_3}{n} \right) g^{-1}, \\ &\dots \end{aligned}$$

Durch fortlaufendes Einsetzen folgt

$$\begin{aligned} \frac{m}{n} &= \left(q_1 + \frac{r_1}{n} \right) g^{-1} = q_1g^{-1} + \left(q_2 + \frac{r_2}{n} \right) g^{-2} = \dots \\ &= q_1g^{-1} + q_2g^{-2} + \dots + \left(q_j + \frac{r_j}{n} \right) g^{-j}. \end{aligned}$$

Wir beweisen nun, dass $c_{-j} = q_j$ für alle natürlichen Zahlen $j > 0$ sein muss, damit (ii) erfüllt ist. Dazu setzen wir den obigen Ausdruck für $\frac{m}{n}$ in (ii) ein. Nach Satz 31 können wir annehmen, dass unsere Behauptung für alle $i < j$ bereits bewiesen ist, also ist die Bedingung äquivalent zu

$$c_{-j}g^{-j} \leq \left(q_j + \frac{r_j}{n} \right) g^{-j} < (c_{-j} + 1)g^{-j}$$

und schließlich zu

$$c_{-j} \leq q_j + \frac{r_j}{n} < c_{-j} + 1,$$

wobei wir die Monotoniegesetze (16) und (17) (und ihre Kontraposition) benutzt haben. Wegen $0 \leq \frac{r_j}{n} < 1$ ist dies tatsächlich nur für $c_{-j} = q_j$ erfüllt.

(iii). Nach Aussage (ii) gilt für alle positiven j und k

$$\sum_{i=-k}^{\infty} c_i g^i + g^{-k} - \frac{m}{n} > 0, \quad \sum_{i=-j}^{\infty} c_i g^i + g^{-j} - \frac{m}{n} \leq g^{-j}.$$

Gäbe es ein k , so dass $c_i = g - 1$ für alle $i < -k$ ist, so hätten wir für $j \geq k$ nach der dritten binomischen Formel (Aufgabe 43)

$$\sum_{i=-j}^{\infty} c_i g^i - \sum_{i=-k}^{\infty} c_i g^i = (g - 1) \sum_{i=-j}^{-k-1} g^i = g^{-k} - g^{-j},$$

also würden die linken Seiten in den obigen Ungleichungen ein und die selbe Zahl ε darstellen. Wie wir vor dem Satz bemerkt haben, ist das für beliebig große j unmöglich.

(iv) und (v). Tritt für ein $k > 0$ der Rest $r_k = 0$ auf, so sind von da an alle Reste (und folglich auch alle Ziffern q_i) gleich Null. Andernfalls gibt es nur $n - 1$ Möglichkeiten für die Reste, also tritt irgendwann ein Rest auf, der schon früher vorgekommen ist, d. h. $r_k = r_{k+l}$, wobei $l > 0$. Dann folgt $r_{k+1} = r_{k+l+1}$, $r_{k+2} = r_{k+l+2}$ usw. Da die Reste r_1, \dots, r_{k+l-1} verschieden sind, gilt $k + l \leq n$.

Zur letzten Aussage des Satzes kommen wir später. □

Auf Grund des Satzes schreibt man

$$\frac{m}{n} = \sum_{i=-\infty}^{\infty} c_i g^i$$

wobei man die linke Seite in diesem Zusammenhang als *gemeinen Bruch* bezeichnet, und nennt die unendliche Summe auf der rechten Seite einen *periodischen Systembruch* zur Grundzahl g . Man schreibt ihn im Stellenwertsystem, indem man die Ziffern in der Reihenfolge absteigender Potenzen von g aufzählt und nach der Einerstelle ein Komma einfügt. Die Nachkommastellen bis vor die k te nennt man *Vorperiode*, die nächsten l Stellen *Periode*. Es ist üblich, die Periode nur einmal zu schreiben und durch Überstreichen kenntlich zu machen. So ist z. B.

$$\frac{11_3}{21_3} = 0,\overline{120102}_3.$$

Periode und Vorperiode sind nicht eindeutig bestimmt, außer man besteht auf kleinstmöglicher Länge:

$$0,\overline{120102}_3 = 0,1\overline{201021}_3 = 0,\overline{120102120102}_3.$$

Der Beweis liefert eine weitere Methode zur Umrechnung von gemeinen Brüchen in g -adische Systembrüche, wobei die Rechnung auch im Dezimalsystem vorgenommen werden kann. Im obigen Beispiel ist $m = 11_3 = 4$, $n = 21_3 = 7$ und $g = 3$. Wie im Beweis erhalten wir

$$\begin{aligned} 4 \cdot 3 &= 1 \cdot 7 + 5, \\ 5 \cdot 3 &= 2 \cdot 7 + 1, \\ 1 \cdot 3 &= 0 \cdot 7 + 3, \\ 3 \cdot 3 &= 1 \cdot 7 + 2, \\ 2 \cdot 3 &= 0 \cdot 7 + 6, \\ 6 \cdot 3 &= 2 \cdot 7 + 4, \\ &\dots \end{aligned}$$

Da der Rest $4 = 11_3$ schon zu Beginn aufgetreten ist, wiederholt sich von hier an die Rechnung. Die abgerundeten Quotienten ergeben die Ternärziffern, und wir erhalten wiederum das Ergebnis

$$\frac{4}{7} = 0, \overline{120102}_3.$$

Die Reste sind die selben wie zuvor, nämlich $5 = 12_3$, $1 = 1_3$, $3 = 10_3$, $2 = 2_3$, $6 = 20_3$ und $4 = 11_3$.

Beweis der letzten Aussage von Satz 52. Gegeben sei eine Folge von Ziffern c_i mit den Eigenschaften (i), (iii) und (iv). Zunächst betrachten wir den Spezialfall eines *echten Systembruchs*, bei dem $c_i = 0$ für $i \geq 0$ ist, und wir nehmen an, dass er *rein periodisch* ist, d. h. dass es eine natürliche Zahl $l \neq 0$ gibt, so dass für *alle* $i < 0$ gilt $c_i = c_{i-l}$. Wir fassen jeweils l Summanden zusammen und klammern eine geeignete Potenz von g aus:

$$(c_{-1}g^{-1} + \dots + c_{-l}g^{-l}) + (c_{-l-1}g^{-1} + \dots + c_{-2l}g^{-l})g^{-l} + \dots$$

Wegen der Periodizität sind die Ausdrücke in allen Klammern gleich. Bezeichnen wir diese mit

$$p = c_{-1}g^{-1} + c_{-2}g^{-2} + \dots + c_{-l}g^{-l},$$

so ist nach der dritten binomischen Formel

$$\sum_{i=0}^{jl} c_{-i}g^{-i} = p(1 - g^{-jl}) : (1 - g^{-l}) = \frac{pg^l}{g^l - 1} - g^{-jl}p : (1 - g^{-l}).$$

Wegen (iii) ist $p < (g-1)(g^{-1} + g^{-2} + \dots + g^{-l}) = 1 - g^{-l}$. Es folgt also

$$\sum_{i=0}^{jl} c_{-i}g^{-i} \leq \frac{pg^l}{g^l - 1} < \sum_{i=0}^{jl} c_{-i}g^{-i} + g^{-jl}.$$

Setzen wir im Zähler den Ausdruck für p ein und benutzen im Nenner die dritte binomische Formel, so können wir die g -adischen Ziffern ablesen:

$$\frac{pg^l}{g^l - 1} = \frac{c_{-1}g^{l-1} + c_{-2}g^{l-2} + \dots + c_{-l}}{(g-1)(g^{l-1} + g^{l-2} + \dots + 1)}$$

Auf ähnliche Weise kann man den allgemeinen Fall behandeln. Da man die Periode an einer beliebigen Stelle $k+1$ beginnen lassen kann, braucht die obere Summationsgrenze kein Vielfaches von l mehr zu sein, und durch Vergleich mit Bedingung (iii) folgt

$$\sum_{i=-\infty}^{\infty} c_i g^i = \sum_{i=-k}^{\infty} c_i g^i + \frac{c_{-k-1}g^{l-1} + c_{-k-2}g^{l-2} + \dots + c_{-k-l}g^{-k}}{(g-1)(g^{l-1} + g^{l-2} + \dots + 1)} g^{-k}.$$

Die Summe auf der rechten Seite hat wegen (i) nur endlich viele von Null verschiedene Summanden, stellt also eine rationale Zahl dar. \square

So haben wir z. B. im Dezimalsystem⁴⁵

$$1,3\overline{428571} = 1,3 + 0,4\overline{28571} \cdot 10^{-1} = \frac{13}{10} + \frac{1}{10} \cdot \frac{428571}{999999} = \frac{47}{35}.$$

Wie schon eingangs bemerkt, lassen sich Systembrüche leicht miteinander vergleichen, weil sich Satz 38 sinngemäß überträgt.

Satz 53. *Es seien r und r' Bruchzahlen mit den g -adischen Ziffern c_i bzw. c'_i . Es gilt genau dann $r < r'$, wenn es eine ganze Zahl i gibt, so dass $c_i \neq c'_i$ ist, und wenn für die größte solche Zahl i gilt $c_i < c'_i$.*

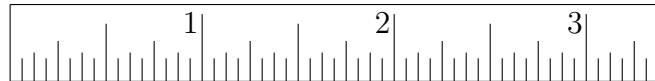
Beweis. Ist $r < r'$, so folgt mit Eigenschaft (ii) für alle j

$$\sum_{i=-j}^{\infty} c_i g^i < \sum_{i=-j}^{\infty} c'_i g^i + g^{-j}.$$

Wegen $r \neq r'$ gibt es ein i , so dass $c_i \neq c'_i$, und wegen (i) gibt es unter diesen ein größtes. Wählen wir $-j < i$, so folgt aus der Gültigkeit der Vergleichsregel für endliche Systembrüche, dass $c_i < c'_i$ ist. Durch Vertauschung der Bezeichnungen folgt die analoge Aussage für $r' < r$, und im Fall $r = r'$ folgt wegen der Eindeutigkeitsaussage von Satz 52, dass $c_i = c'_i$ für alle i . \square

⁴⁵Die klassische englische Schreibweise war $1.3\dot{4}2\dot{8}5\dot{7}1$, das Malzeichen war \times .

In der Praxis kommen neben Dezimalbrüchen auch andere Systembrüche vor. Computer benutzen intern Dualbrüche. Bei Maßangaben in Zoll verwendet man traditionell nur Dualbrüche, die allerdings als gemeine Brüche angegeben werden. So wird man z. B. nie ein Wasserrohr mit einer Nennweite von $\frac{2}{3}$ Zoll finden, wohl aber von $\frac{1}{2}$ Zoll oder $\frac{3}{4}$ Zoll (d. h. $0,1_2$ oder $0,11_2$ Zoll). Die Einteilung eines Zollstocks macht dies ebenfalls deutlich:



Man kann auch Systembrüche in gemischten Stellenwertsystemen betrachten. Die Babylonier als Nachfolger der Sumerer nutzten Brüche, in denen „nach dem Komma“ eine Sechserziffer folgte, dann eine Zehnerziffer, dann wieder eine Sechserziffer usw. Fasst man wieder zwei Ziffern zu einer Sechzigerziffer zusammen, so erhält man Hexagesimalbrüche. Beschränkt man sich aber auf drei Nachkommastellen, so kann man 360ste Teile des Ganzen wiedergeben. Das ist offenbar der Grund, warum der Kreis in 360 Grad eingeteilt wurde.

Index

- f -Abschluss, 36
- n -Tupel, 57
- Äquivalenz, 4
- Äquivalenzklasse, 80
- Äquivalenzrelation, 20
- Übertrag, 70

- Abbildung, 13
- Abbildung auf, 17
- abgerundeter Quotient, 53
- abgeschlossen unter f , 36
- absoluter Betrag, 101
- Addition, 24
- Alternative, 6
- antisymmetrisch, 36
- Antivalenz, 6
- assoziativ, 6, 10, 24, 27
- Aussage, 1
- Aussageform, 7
- Axiom, 32

- bündeln, 61
- bijektiv, 18
- Binom, 92
- Binomialkoeffizient, 92
- binomische Formel, 92
- Bisubjunktion, 4
- Bruch, 105
- Bruchzahl, 110

- Cartesisches Produkt, 11
- charakteristische Funktion, 92

- das Kleinste, 36
- Definitionsbereich, 13
- Dezimalbruch, 112
- Differenz, 51
- differenzgleich, 80
- Ding, 90

- disjunkt, 23
- Disjunktion, 2
- distributiv, 6, 10, 27
- Division, 51
- Division mit Rest, 53
- Doppelbruch, 110
- Durchschnitt, 10, 30

- echte Teilmenge, 33
- echter Bruch, 110
- Eigenschaft, 10
- eindeutig, 16
- Element, 8
- elementfremd, 23
- entgegengesetzte Zahl, 76
- entweder ... oder, 6
- erweitern, 106

- Fakultät, 54
- Folge, 11, 58
- Funktion, 13

- ganze Zahl, 82
- gemeiner Bruch, 115
- gemischte Zahl, 110
- genau dann, wenn, 4
- genau ein, 13
- geordnetes Paar, 11
- gleichmächtig, 20
- gleichnamig, 107
- Graph, 14
- Grundbegriff, 8
- Grundzahl, 62

- Halbordnung, 47
- Hauptnenner, 107

- identische Abbildung, 15
- Implikation, 3

Index, 57
 Induktionsanfang, 45
 Induktionsbehauptung, 45
 Induktionsschritt, 45
 Induktionsvoraussetzung, 45
 injektiv, 16
 isomorph, 86

 kürzen, 106
 Kürzungsregel, 50
 Kardinalzahl, 22
 Kehrwert, 99
 Klasse, 21
 kleiner, 32, 33, 85, 108
 kleines Einmaleins, 66
 Kombinationen, 94
 Kombinatorik, 88
 kommutativ, 5, 10, 24, 27
 Konjunktion, 2
 Kreuzprodukt, 11

 Lemma, 37
 lexikographische Ordnung, 48
 linkes/rechtes Distributivgesetz, 75
 logisches Gesetz, 4

 Mächtigkeit, 22
 Mächtigkeitsklasse, 21
 Menge, 8
 Mengenoperationen, 10
 Multiplikation, 26

 Nachfolger, 44
 Negation, 1
 Nenner, 105
 Null, 62

 oder, 2
 Ordinalzahl, 49
 Ordnung, 47

 Pascalsches Dreieck, 92
 Periode, 115

 periodischer Systembruch, 115
 Permutationen, 91
 Pochhammer-Symbol, 89
 Potenz von Kardinalzahlen, 29
 Potenzgesetze, 29, 56
 Prädikat, 7
 Produkt von Kardinalzahlen, 26
 Produktzeichen, 59

 quod erat demonstrandum, 9
 Quotient, 51
 quotientengleich, 102

 rationale Zahl, 104
 reflexiv, 20, 47
 rein periodisch, 116
 Rekursionssatz, 55
 rekursiv, 56
 Relation, 32
 Repräsentant, 21
 Rest, 53
 reziprok, 99

 Schnittmenge, 10
 schriftliche Rechenverfahren, 69
 Stammbruch, 111
 Stellenwertsystem, 62
 Subjunktion, 3
 Substitutionsregel, 59
 Subtraktion, 51
 Summationsgrenze, 58
 Summe von Kardinalzahlen, 24
 Summenzeichen, 59
 surjektiv, 17
 symmetrisch, 20
 Systembruch, 112

 teilbar, 51
 Teiler, 51
 Teilmenge, 8
 total, 36
 transitiv, 20

Transposition, 42
Tripel, 27

Umkehrabbildung, 18
umkehrbar eindeutig, 18
und, 2
uneingeschränkte Ausführbarkeit, 74
unkürzbar, 107

Variationen, 90
Vereinigung, 10, 30
Vereinigungsmenge, 10
Verkettung, 15
verknüpfen, 2
Vielfaches, 51
vollständige Induktion, 44
Vorperiode, 115
Vorzeichen, 76
Vorzeichenregeln, 76

Wahrheitstafel, 1
Wahrheitswert, 1
wenn ... dann, 3
Wertebereich, 17
Wertetabelle, 14
Wertevorrat, 17
Wiederholung, 90, 94
Wohlordnung, 48

Zähler, 105
Zielbereich, 13
Ziffer, 63
Zuordnung, 13