

Scriptum zur Vorlesung Zählen und Zahlbereiche

Prof. W. Hoffmann
WS 2008/09

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.

Man kann das Wort „Negation“ auch als „Gegenteil“ übersetzen, sollte sich aber vor Missverständnissen hüten. Die Negation der Aussage

„Ich habe immer Zeit“

ist nicht die Aussage

„Ich habe nie Zeit“,

sondern z. B.

„Es ist nicht wahr, dass ich immer Zeit habe.“

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) Sein oder Nichtsein, das ist hier die Frage.

Im ersten Beispiel wird man auch bestraft, wenn man beides tut, während im zweiten Beispiel nur einer der beiden Fälle möglich ist. 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 ich verspreche:

„Hilfst du mir, so helf’ ich dir.“

Man kann genauso gut sagen

„Wenn du mir hilfst, dann helfe ich dir.“

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 letzten beiden Zeilen, die Anfängern Probleme bereiten. Im obigen Beispiel hatte ich für den Fall, dass die Bedingung nicht erfüllt ist, nichts versprochen. In diesem Fall habe ich das Versprechen eingehalten, ganz gleich, ob ich helfe oder nicht.

Das Pfeilzeichen bedeutet 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.“

Das Wort „wenn“ kann auch durch das Wort „falls“ ersetzt werden. Die Bedingung kann auch am Ende des Satzes genannt werden:

„Du wirst es später schwer haben, wenn du die Übungen auf die leichte Schulter nimmst.“

Zwei Aussagen heißen äquivalent, wenn sie den selben Wahrheitswert haben. Man behauptet dies, indem man die Aussagen durch die Worte „genau dann, wenn“ verknüpft. Damit bildet man die *Äquivalenz*². Beispiel:

¹auch *Subjunktion* genannt

²auch *Bisubjunktion* genannt

„Die Sanktionen werden genau dann zurückgenommen, wenn der Iran seine Urananreicherung einstellt.“

Die Aussage „genau dann A , wenn 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

Man kann Aussagen, die durch eine Verknüpfung entstanden sind, wiederum verknüpfen, wie zum Beispiel $\neg\neg A$. 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.

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“ kann man also nicht nur sagen „Wenn es Nacht ist, kann man die Sonne nicht sehen“, sondern auch „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 wir 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.

Uns fehlt noch die Verknüpfung „entweder A oder B “, die wahr ist, 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 $A \succ\prec B$ 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. In einer Klasse wird diskutiert, wer Mitglied in der Schulband ist. Von Anne, Björn und Christoph ist den Anwesenden folgendes bekannt:

- (1) Anne oder Christoph ist Mitglied.
- (2) Entweder Anne oder Björn ist Mitglied.
- (3) Entweder Björn oder Christoph ist Mitglied.

Wer von den dreien ist Mitglied?

Eine Lösungsmöglichkeit besteht darin, eine Wahrheitstafel für die Aussagen

A : Anne ist Mitglied,

B : Björn ist Mitglied,

C : Christoph ist Mitglied

aufzustellen und die Wahrheitswerte der Aussagen (1), (2) und (3), nämlich

$$A \vee C, \quad A \succ\prec B, \quad B \succ\prec C,$$

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

Kürzer (aber anspruchsvoller) ist folgender Lösungsweg. Angenommen, Björn ist Mitglied. Dann folgt aus Aussage (2), dass Anne kein Mitglied ist,

und aus (3), dass Christoph kein Mitglied ist. Dann wäre aber Aussage (1) falsch. Da wir alle drei Aussagen als wahr vorausgesetzt haben, muss unsere Annahme falsch sein. Somit ist Björn kein Mitglied, und aus Aussage (2) folgt nun, dass Anna Mitglied ist, während aus Aussage (3) folgt, dass Christoph Mitglied ist.

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 „ a ist ein Element“ hingegen nicht. Man kann sagen „ a ist ein Element von M “, abgekürzt $a \in M$, was man auch salopp mit „ a gehört zu M “ ausdrücken kann. Das Wort „Element“ dient also nur zur Formulierung einer Aussage über die Objekte a und M , die wahr oder falsch sein kann.

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*. Auch „ $x \in M$ “ ist eine Aussageform, die die Variable x enthält.

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

{Anna, Björn, Christoph}

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 $(\frac{p}{2})^2 - q \geq 0$ 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 im Fall $\left(\frac{p}{2}\right)^2 - q = 0$ nur aus einem Element besteht.

Dieselbe Menge kann auf verschiedene Weise beschrieben werden. So ist z. B. die Menge der bisherigen weiblichen Bundeskanzler gleich der Menge der in der ehemaligen DDR aufgewachsenen bisherigen Bundeskanzler. 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.

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

Definition 1 *Man sagt [genau dann], 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 $x \in M$.*

Die Definition einer Aussageform (in diesem Fall der Aussageform $N \subseteq M$, in der die Variablen M und N vorkommen) hat die logische Struktur einer Äquivalenz, müsste also immer mit den Worten „genau dann, wenn“ formuliert werden. In der Praxis benutzt man meist nur das Wort „wenn“.

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 $N \subseteq M$ 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

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

das man leicht mittels Wahrheitstabellen nachprüfen kann. 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.

$$\{\text{Adenauer, Erhard, Kiesinger, Brandt, Schmidt, Kohl, Schröder, Merkel}\} \\ = \{x \mid x \text{ ist bisheriger Bundeskanzler}\}$$

(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 Elemente, 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 Elemente, 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 Elemente, die zur Menge M , aber⁴ nicht zur Menge N gehören, d. h.

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

³manche Autoren benutzen einen Doppelpunkt

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

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

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

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 Durchschnittes 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 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

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

so ist $M \times N$ 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 oder Funktion ist zentral in der Mathematik und ihren Anwendungen. Hier einige praktische Beispiele:

- (i) In der Bibliothek gehört (hoffentlich) zu jedem Eintrag im Katalog ein Buch im Regal.
- (ii) Jeder Teilnehmer dieser Veranstaltung muss sich in eine Übungsgruppe einschreiben.
- (iii) Zu jedem Punkt auf dem Computerbildschirm gehört bei Benutzung des Beamers ein Bildpunkt auf der Leinwand.
- (iv) Zu jedem Zeitpunkt zeigt das Tachometer eine bestimmte Geschwindigkeit an.

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

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

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 (iii). Man nennt M den *Definitionsbereich* und N den *Zielbereich* der Abbildung. Besteht N aus Zahlen wie im Beispiel (iv), 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 “. Wenn wir z. B. die Abbildung, die jedem Teilnehmer seine Gruppe zuordnet, mit g bezeichnen, und ist Fritzchen in die Gruppe Müller1 eingeschrieben, so ist $g(\text{Fritzchen})$ eine andere Bezeichnung für Müller1.

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 auch nur ein Teilnehmer in mehrere Gruppen eingetragen hat, so liegt immer noch 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 Funktionen (und Abbildungen allgemein) 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 Tabelle angeben. So ist in der Tabelle der Kodierung [ASCII](#)⁶ für jeden Buchstaben des Alphabets eine Folge von Nullen und Einsen angegeben, mit der dieser Buchstabe im Computer gespeichert wird. Dem Buchstaben A ist z. B. die Folge 1000001 zugeordnet, dem Buchstaben B die Folge 1000010 usw.

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, bei dem sich die Teilnehmer bei jeder Frage zwischen den Antworten A, B und C entscheiden müssen, erzeugen sie faktisch eine Abbildung von der Menge F der Fragen in die Menge $\{A,B,C\}$. Auf dem Fragebogen geben sie allerdings keine Wertetabelle an, sondern kreuzen

⁶American Standard Code for Information Interchange

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 derjenigen geordneten Paare (x, y) , für die $y = f(x)$ gilt.*

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 , so dass gilt $(x, y) \in G$. 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 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 einem Element der Definitionsbereich zugeordnet sein.

Definition 6 *Eine Abbildung $f : M \rightarrow N$ heißt injektiv,⁷ 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:

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

Die Abbildungen in den Beispielen (i) und (iii) am Anfang des Abschnittes sollten injektiv sein, die in Beispiel (ii) nicht.

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

⁷Im Deutschen nennt man solche Abbildungen eineindeutig, aber die französische Bezeichnung hat sich mittlerweile allgemein durchgesetzt.

⁸Im 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.

Man nennt die Menge derjenigen Elemente y von N , zu denen es ein $x \in M$ gibt, so dass $f(x) = y$, 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 Abbildungen in den Beispielen (i) und (ii) sollten surjektiv sein, die in Beispiel (iii) nicht unbedingt.

Definition 8 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.

Aus der Schule ist bekannt, dass eine Abbildung genau dann eine Umkehrabbildung besitzt, wenn sie bijektiv ist.

Ein Beispiel einer bijektiven 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

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

In der Praxis werden häufig mehrere Zuordnungen verkettet. So wurden z. B. die Jahrgangsstufen des Gymnasiums früher mit lateinischen Zahlwörtern von der Abschlussklasse abwärts gezählt, wobei die oberen Klassen über zwei Jahre gingen. Die Zuordnung zu den heute üblichen Klassenstufen ist durch folgende Tabelle gegeben:

OI	UI	OII	UII	OIII	UIII	IV	V	VI
13	12	11	10	9	8	7	6	5

Diese Klassenstufen werden ihrerseits im Computer in eine Folge von Nullen und Einsen verwandelt (entweder als Folge von zwei Zeichen mit Hilfe des ASCII-Codes oder, was wir hier vorziehen, direkt als Binärzahlen):

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
1111	1110	1101	1100	1011	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001	0000

Geht man direkt von lateinischen Klassenstufen zu Binärzahlen über, so hat man zwei Abbildungen verkettet.

Definition 9 Gegeben seien die Abbildungen $f : M \rightarrow N$ und $g : L \rightarrow M$. Dann ist eine Abbildung $h : L \rightarrow N$ durch die Vorschrift $h(x) = f(g(x))$ gegeben, die man die Verkettung von f und g nennt und mit $f \circ g$ abkürzt.

⁹Im Deutschen „umkehrbar eindeutig“

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

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

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

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

(iii) 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. (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.

(iii) Diese Aussage hat die Struktur einer Äquivalenz $A \Leftrightarrow B$. Es genügt darum, die Implikation $A \Rightarrow B$ und ihre Umkehrung $B \Rightarrow A$ zu beweisen.

Angenommen, g ist die Umkehrabbildung von f . Ist $x \in M$ und bezeichnen wir $f(x)$ mit y , also $f(x) = y$, so ist nach Definition der Umkehrabbildung $g(y) = x$, und es folgt $g(f(x)) = g(y) = x$. Wir haben also gezeigt, dass für jedes $x \in M$ 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 bezeichnen wir $f(x)$ mit y , so folgt

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

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

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) Es seien¹⁰ $u, v \in L$. 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.

(ii) Es seien wieder $u, v \in L$. Ist $g(u) = g(v)$, so folgt $f(g(u)) = f(g(v))$, das heißt $(f \circ g)(u) = (f \circ g)(v)$. Wegen der Injektivität von $f \circ g$ folgt daraus, dass $u = v$. Da dies für beliebige u und v gilt, ist g injektiv.

Der Beweis von (iii) und (iv) ist Inhalt der Übungsaufgabe 9. \square

¹⁰Strenggenommen müsste man schreiben: $u \in L$ und $v \in L$.

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 6 *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 $g : N \rightarrow M$, und diese ist bekanntlich ebenfalls bijektiv.¹¹ Also ist N gleichmächtig zu M . Die Umkehrung beweist man ebenso.

¹¹Da 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.

(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, die man mit $\{\}$ oder \emptyset bezeichnet, 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 $\{\text{Sonne}\}$ ist. Ebenso kann man festlegen, dass eine Zweiermenge eine solche Menge ist, die gleichmächtig zur Menge $\{\text{Sonne}, \text{Mond}\}$ ist.

Wir klassifizieren Mengen nach ihrer Mächtigkeit,¹² Ähnlich wie man Lebewesen oder Steuerpflichtige 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 Klasse der Menge $\{\text{Sonne}\}$ gerade die Klasse der Einermengen. Statt Mächtigkeitsklasse sagen wir hier kurz Klasse, was wohl niemand mit Steuerklasse oder sozialer Klasse verwechseln wird. Aus Satz 6 erhalten wir eine Reihe von Folgerungen:

- *Jede Menge gehört zu einer Klasse (nämlich zu ihrer eigenen wegen (i)), und jede Klasse enthält wenigstens eine Menge (laut Definition).*
- *Alle Mengen in einer Klasse sind gleichmächtig.* Gehören nämlich L und N zur Klasse von M , also $L \sim M$ und $N \sim M$, so folgt aus (ii) und (iii), dass $L \sim N$.
- *Eine Menge M gehört genau dann zur Klasse von N , wenn N zur Klasse von M gehört.* Das folgt aus (ii).
- *Gehört M zur Klasse von N , so stimmt die Klasse von M mit der Klasse von N überein.* Jede Menge L aus der Klasse von M gehört dann nämlich wegen (iii) zur Klasse von N , also ist die Klasse von M in der Klasse von N enthalten. Aufgrund der vorigen Folgerung können wir die Rollen von M und N vertauschen.

¹²Dieser Begriff ist offenbar durch die Mächtigkeit von Gesteinsschichten motiviert.

- *Haben zwei Klassen eine Menge gemeinsam, so stimmen sie überein.* Gehört z. B. die Menge M sowohl zur Klasse von L als auch zu der von N , so stimmt nach der vorigen Folgerung die Klasse von M mit der von L als auch mit der von N überein.
- *Mengen in verschiedenen Klassen sind nicht gleichmächtig.* Andernfalls würde die eine Menge laut Definition zur Klasse der anderen gehören, und dann müssten ihre Klassen übereinstimmen.

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 Buchstaben des lateinischen Alphabets 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 einfach mit den Klassen gleichzusetzen.¹³

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 Klasse verschiedene Bezeichnungen vereinbaren, z. B.

≡, ≡, 5, V, 5

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

Nun können wir Sätzen wie „In der taoistischen Tradition gibt es fünf Elemente“ einen Sinn geben. Da wir unendliche Mengen bisher nicht ausgeschlossen haben, sprechen wir nicht von der Anzahl, sondern der Mächtigkeit.

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

¹³Das ist nicht ganz befriedigend, weil man dann nicht von der Menge der Kardinalzahlen sprechen kann, aber für diese erste Einführung ausreichend.

So ist zum Beispiel

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

Hat M die Mächtigkeit m , so nennt man M auch einen Repräsentanten der Kardinalzahl m .

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*.¹⁴ 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 7 *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 M disjunkt zu N , so gilt

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

¹⁴Die Verwendung des lateinischen Wortes *disjunkt* (deutsch: getrennt) hat nichts mit der logischen Disjunktion zu tun.

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, kommen 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 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 $y \in M \cup N$. 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.¹⁵ 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 7.

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.

¹⁵Hat man zunächst irgendwelche Repräsentanten M und N , so kann man sie durch die disjunkten Repräsentanten $M \times \{a\}$ und $N \times \{b\}$ ersetzen.

Satz 8 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

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

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 9 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 7 ähnlich 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 $|N| = n$.

Für die Multiplikation gelten die vertrauten Rechengesetze:

Satz 10 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 . Wir definieren eine Abbildung

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

indem wir festlegen

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

Diese Abbildung ist offensichtlich bijektiv, also ist $M \times N \sim N \times M$, so dass

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

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 . 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, also ist $(L \times M) \times N \sim L \times (M \times N)$, so dass

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

Mit der Definition der Multiplikation folgt

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

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 der Übungsaufgabe 17. \square

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 $f(x) = (x, a)$. Folglich gilt für alle Kardinalzahlen m , dass

$$m \cdot 1 = m.$$

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 11 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 analog 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 12 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 Aufgabe 15 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 der Übungsaufgabe 20. □

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.

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 18 *Wir sagen, dass eine Menge M höchstens so mächtig wie eine Menge N 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 13 *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.

Die Umkehrung ist leicht zu sehen, sie ist Gegenstand der Präsenzaufgabe 6. 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 14 *Gilt für die Mengen K, L, M und N , dass*

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

so ist M genau dann höchstens so mächtig wie N , wenn K höchstens so mächtig wie L ist.

Beweis. Aufgrund unserer Voraussetzungen gibt es bijektive Abbildungen

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

Ist M höchstens so mächtig wie N , 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 K höchstens so mächtig wie L . Die Umkehrung beweist man analog mit Hilfe der Umkehrabbildungen von p und q . \square

Damit ist die folgende Definition gerechtfertigt.

Definition 19 *Wir sagen, dass die Kardinalzahl m kleiner oder gleich der Kardinalzahl n ist (abgekürzt $m \leq n$), wenn eine Menge M der Mächtigkeit m höchstens so mächtig wie eine Menge N der Mächtigkeit n ist.*

Natürlich gilt für jede Kardinalzahl $m \leq m$, weil es für einen beliebigen Repräsentanten M von m die identische Abbildung id_M gibt.

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 20 *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.*

Kann eine Menge M gleichmächtig zu einer ihrer echten Teilmengen sein? Dies würde bedeuten, 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.

Wir müssen Abbildungen f einer Menge M in sich selbst etwas näher untersuchen.

Definition 21 *Es sei f eine Abbildung der Menge M in sich selbst und L eine Teilmenge von M . Wir sagen, L sei f -abgeschlossen,¹⁶ wenn für jedes Element x von L auch $f(x) \in L$ ist.*

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 $f(x) \in K \cap L$.

Man kann übrigens den Durchschnitt einer beliebigen Familie von Mengen bilden, zu der wenigstens eine Menge gehört. Ein Objekt ist Element dieses Durchschnitts, wenn es Element einer jeden Menge aus der Familie ist. Haben wir eine Familie von f -abgeschlossenen Teilmengen einer Menge M , zu der wenigstens eine Menge gehört, so ist ihr Durchschnitt ebenfalls f -abgeschlossen.

Satz 15 *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).*

¹⁶oder „abgeschlossen unter der Abbildung f “

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 geben muss. So gibt es z. B. unter den nichtleeren Teilmengen einer Menge, die nicht Einermenge ist, keine kleinste.

Beweis von Satz 15. 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

Man kann den f -Abschluss einer Teilmenge K praktisch mitunter 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.

Wenn wir Kardinalzahlen m und n haben, so dass $m \leq n$ und $n \leq m$, dann sollten diese Kardinalzahlen eigentlich gleich sein. Um das zu beweisen, benötigen wir einen Hilfssatz.¹⁷

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

Satz 16 (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 .*

Beweis. 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

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

¹⁷In der Tradition von Euklids „Elementen“ bezeichnet man einen Hilfssatz als *Lemma* (Mehrzahl *Lemmata*).

Wegen der Injektivität von f und g und der Disjunktheit von M und N ist auch h injektiv. Wir betrachten die Menge

$$K = \{y \in N \mid \text{Es gibt kein } x \in M, \text{ so dass } f(x) = y\}$$

und bezeichnen ihren h -Abschluss mit L . Nun definieren wir eine Abbildung

$$i : M \rightarrow N$$

wie folgt. Nach Aufgabe 13 ist M die Vereinigung der disjunkten Mengen $M \setminus L$ und $M \cap L$.

- (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 $i(x) = y$.

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.

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 14 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 6 folgt $M \sim N$. \square

Folgerung 1 *Gelten für Kardinalzahlen m und n die beiden Aussagen*

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

so ist $m = n$.

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. Neben der obigen Folgerung, die man auch *Antisymmetrie* nennt, hat sie eine weitere wichtige Eigenschaft, nämlich die *Transitivität* – Für beliebige Kardinalzahlen l , m und n gilt:

Wenn $l \leq m$ und $m \leq n$, dann ist $l \leq n$.

Dies folgt leicht aus Satz 5(i). Eine weitere Eigenschaft ist die *Totalität* – Für beliebige Kardinalzahlen m und n gilt

$m \leq n$ oder $n \leq m$.

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.

Definition 22 *Wir sagen, dass eine Kardinalzahl m kleiner als eine Kardinalzahl n ist (abgekürzt $m < n$), wenn $m \leq n$, aber $m \neq n$ ist.*

Aus der Antisymmetrie und der Totalität folgt, dass die Aussage $m < n$ die Negation der Aussage $n \leq m$ ist. Auch die Kleiner-Relation ist transitiv. Zum Schluss sei noch einmal daran erinnert, dass die Mächtigkeit einer echten Teilmenge nicht unbedingt kleiner als die Mächtigkeit der gesamten Menge sein muss.

3 Natürliche Zahlen

3.1 Nachfolger

Das Zählen im Unterschied zum Abzählen bedeutet, beginnend mit einer ersten Zahl von einer Zahl zur nächsten fortzuschreiten. Dies lässt sich mit einer Abbildung erfassen.

Definition 23 Eine Abbildung s einer Menge N in sich selbst nennen wir Nachfolgerabbildung, wenn

- (i) die Abbildung s injektiv ist,
- (ii) es genau ein Element a von N gibt, das nicht im Wertebereich von s liegt,
- (iii) jede s -abgeschlossene Teilmenge von N , die a enthält, gleich N ist.

Wir nennen a das Anfangselement, und für jedes Element $x \in N$ nennen wir $s(x)$ den Nachfolger (lateinisch successor) von x .

Zunächst überzeugen wir uns, dass es Mengen mit Nachfolgerabbildung gibt. Wir hatten im vorigen Abschnitt das Axiom erwähnt, dass es wenigstens eine injektiven Abbildung f einer Menge M in sich selbst geben soll, die nicht surjektiv ist. Es muss also ein Element $a \in M$ geben, das nicht im Wertebereich von f liegt. Wir bezeichnen den f -Abschluss der Teilmenge $\{a\}$ mit N und definieren eine Abbildung $s : N \rightarrow N$ durch $s(x) = f(x)$, was wegen der f -Abgeschlossenheit von N für alle $x \in N$ wieder in N liegt. Mit anderen Worten, s ist die Einschränkung von f auf N . Wir behaupten, dass s dann eine Nachfolgerabbildung ist. In der Tat:

- (i) Aus der Injektivität von f folgt die von s .
- (ii) Nach Lemma 1 liegt jedes von a verschiedene Element von N im Wertebereich von s .
- (iii) Jede s -abgeschlossene Teilmenge von N ist eine f -abgeschlossene Teilmenge von M , und wenn sie a enthält, muss sie nach Definition des f -Abschlusses auch N enthalten.

Man kann die Elemente einer Menge mit Nachfolgerabbildung gewissermaßen nummerieren, wobei wir es in dieser Vorlesung vorziehen, die Zählung (wie bei Stockwerken im Deutschen) mit der Null zu beginnen. Dabei orientieren wir uns an Robinson Crusoe, der die Anzahl der Kerben in seinem Kalender zählen musste, um zu wissen, der wievielte Tag seit seiner Ankunft

es gerade war. Die Menge der verfloßenen Tage ist aber schwerer zu beschreiben als die Menge der bevorstehenden. Dies bringt uns auf folgende Idee.

Ist $s : N \rightarrow N$ eine Nachfolgerabbildung, so ordnen wir jedem Element x von N wie folgt eine Kardinalzahl $\text{nr}(x)$ (gelesen: Nummer von x) zu. Wir bilden den s -Abschluss L der Menge $\{x\}$ und setzen

$$\text{nr}(x) = |N \setminus L|.$$

Ist a das Anfangselement, so ist der s -Abschluss von $\{a\}$ wegen Eigenschaft (iii) gleich N , also $\text{nr}(a) = 0$. Es leuchtet ein, dass für alle $x \in N$ gilt

$$\text{nr}(s(x)) = \text{nr}(x) + 1. \quad (2)$$

Der Beweis ist nicht ganz einfach, er ist Inhalt von Aufgabe 25*.

Definition 24 Eine natürliche Zahl ist eine Kardinalzahl der Form $\text{nr}(x)$ für ein Element x einer Menge N mit Nachfolgerabbildung. Eine Menge heißt endlich, wenn ihre Mächtigkeit eine natürliche Zahl ist.

Diese Definition ist noch unbefriedigend, da der Begriff einer natürlichen Zahl von der Wahl einer Nachfolgerabbildung abzuhängen scheint. Diese Befürchtung werden wir mit Hilfe des folgenden Satzes ausräumen.

Satz 17 (Rekursionsatz) Es sei $s : N \rightarrow N$ eine Nachfolgerabbildung mit Anfangselement a und $f : M \rightarrow M$ eine beliebige Abbildung einer Menge in sich selbst. Ist b ein beliebiges Element von M , so gibt es genau eine Abbildung $g : N \rightarrow M$, so dass $g(a) = b$ ist und für alle $x \in N$ gilt

$$f(g(x)) = g(s(x)).$$

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

$$h((x, y)) = (s(x), f(y))$$

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

Es sei K die Menge aller $x \in N$, für die es ein $y \in M$ gibt, so dass $(x, y) \in G$. In diesem Fall ist auch $h((x, y)) \in G$, das heißt $(s(x), f(y)) \in G$ und somit $s(x) \in K$. Also ist K eine s -abgeschlossene Teilmenge von N , die a enthält, und wegen (iii) ist $K = N$.

Es sei L die Menge aller $x \in N$, für die es nur ein $y \in M$ mit der Eigenschaft $(x, y) \in G$ gibt. Wir wollen zeigen, dass für $x \in L$ auch $s(x) \in L$ ist. Angenommen, es gibt $t \in M$ und $u \in M$, so dass $(s(x), t) \in G$ und $(s(x), u) \in G$. Weil s injektiv ist, ist auch h injektiv. Nach Lemma 1 muss es $(x, v) \in G$ und $(x, w) \in G$ geben, so dass

$$(s(x), t) = h((x, v)), \quad (s(x), u) = h((x, w)),$$

mit anderen Worten,

$$t = f(v), \quad u = f(w).$$

Wegen $x \in L$ ist $v = w$, also $t = u$. Damit haben wir bewiesen, dass auch $s(x) \in L$ ist. Somit ist L eine s -abgeschlossene Teilmenge von N , die a enthält, und wegen (iii) ist $L = N$.

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

$$y = g(x),$$

so ist auch $(s(x), f(y)) \in G$, also

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

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

Folgerung 2 Sind $s : N \rightarrow N$ und $s' : N' \rightarrow N'$ Nachfolgerabbildungen mit Anfangselementen a und a' , so gibt es genau eine bijektive Abbildung $g : N \rightarrow N'$, so dass $g(a) = a'$ und

$$s' \circ g = g \circ s.$$

Die Existenz dieser Abbildung folgt aus dem Satz (angewendet im Fall $M = N'$), ihre Bijektivität allerdings nicht. Wir können aber die Rollen von N und N' vertauschen und erhalten eine Abbildung $h : N' \rightarrow N$, so dass

$$s \circ h = h \circ s'.$$

Man kann den Satz schließlich auch im Fall $M = N$ anwenden. In diesem Fall hat die Abbildung id_N die gesuchten Eigenschaften $\text{id}_N(a) = a$ und

$$s \circ \text{id}_N = \text{id}_N \circ s,$$

aber auch die Abbildung $h \circ g$, und wegen der Eindeutigkeitsaussage folgt $h \circ g = \text{id}_N$. Analog zeigt man $g \circ h = \text{id}_{N'}$ und wendet Satz 4(iii) an.

Mit Hilfe der Nachfolgerabbildung s' können wir jedem Element $x' \in N'$ eine Kardinalzahl $\text{nr}'(x')$ zuordnen, und wegen der Folgerung sehen wir, dass

$$\text{nr}'(g(x)) = \text{nr}(x)$$

für alle $x \in N$. Der Begriff der natürlichen Zahl ändert sich also nicht, wenn wir s durch s' ersetzen.

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 18 *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 .*

Beweis. Wir wählen eine Nachfolgerabbildung $s : N \rightarrow N$. Es sei K die Menge aller $x \in N$, für die $A(nr(x))$ gilt. Die Gültigkeit von $A(0)$ bedeutet, dass das Anfangselement in K liegt. Ist $x \in N$ beliebig und $n = nr(x)$, so können wir mit Hilfe der Identität (2) aus der Aussage „wenn $A(n)$, dann $A(n + 1)$ “ folgern: „Wenn $x \in K$ ist, so ist auch $s(x) \in K$ “. Aus der Eigenschaft (iii) in Definition 23 folgt nun $K = N$, das heißt, für alle $x \in N$ gilt die Aussage $A(nr(x))$. \square

Nach diesem Satz genügt es für den Beweis einer Aussage $A(n)$ für alle natürlichen Zahlen n , zwei andere Aussagen zu beweisen, was manchmal einfacher ist. 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 viele Aussagen über natürliche Zahlen beweisen. wie z. B. den folgenden Satz.

Satz 19 Die Summe und das Produkt natürlicher Zahlen sind natürliche Zahlen.

Beweis. Um zu beweisen, dass die Kardinalzahl $m + n$ für alle natürlichen Zahlen m und n wieder eine natürliche Zahl ist, halten wir eine natürliche Zahl m fest und beweisen die Aussage für alle natürlichen Zahlen n durch vollständige Induktion. (Man sagt auch, wir benutzen vollständige Induktion nach der Variablen n .)

In dem Spezialfall $n = 0$ lautet die Behauptung $m + 0 = m$. Das haben wir schon früher bewiesen, siehe (1). Damit ist der Induktionsanfang abgeschlossen.

Nun nehmen wir an, dass für irgendeine natürliche Zahl n die Aussage

$$m + n \text{ ist eine natürliche Zahl}$$

wahr ist. (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

$$m + (n + 1) \text{ ist eine natürliche Zahl.}$$

(Dies ist die Induktionsbehauptung.) Wenn uns das gelingt, dann ist der Beweis auf Grund von Satz 18 abgeschlossen.¹⁸

Laut Assoziativität der Addition (Satz 8) ist

$$m + (n + 1) = (m + n) + 1.$$

Laut Induktionsbehauptung und Definition 24 gibt es ein $x \in N$, so dass $m + n = \text{nr}(x)$, wobei N natürlich eine Menge mit Nachfolgerabbildung bezeichnet. Unter Benutzung der Gleichung (2) folgt daraus

$$(m + n) + 1 = \text{nr}(s(x)).$$

Hieraus folgt laut Definition 24, dass $(m + n) + 1$ oder, was das selbe ist, $m + (n + 1)$, eine natürliche Zahl ist. Damit ist der Induktionsschritt abgeschlossen.

Der Beweis für das Produkt $m \cdot n$ ist Inhalt von Aufgabe 22. Anstelle der Identität (2) benutzt man dabei die eben bewiesene Aussage über die Summe natürlicher Zahlen. \square

Da die Methode der vollständigen Induktion zweifellos anspruchsvoll ist, versuchen manche Lehrer, ihren Schülern das inhaltliche Verständnis zu ersparen, indem sie eine starre Form vorgeben, etwa dass jeder Induktionsbeweis in die Abschnitte

¹⁸Mehr Hilfe kann die Methode der vollständigen Induktion nicht leisten. Von hier an muss man wie in jedem Beweis weitere Ideen einbringen.

1. Induktionsanfang
2. Induktionsvoraussetzung
3. Induktionsbehauptung
4. Induktionsbeweis

zu gliedern sei. Damit wird aber oft mehr Verwirrung gestiftet, weil 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 eine häufige Fehlerquelle.

Bevor wir ein weiteres Beispiel behandeln, führen wir einen leicht verständlichen Begriff ein.

Definition 25 *Es seien a und b zwei verschiedene 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.

Nun kommen wir zu einer Behauptung, die für unendliche Mengen falsch wäre.

Satz 20 *Ist M eine endliche Menge und $f : M \rightarrow M$ eine injektive Abbildung, so ist f auch surjektiv.*

Beweis. Die Behauptung gilt offensichtlich für die leere Menge, da es nur eine Abbildung $\emptyset \rightarrow \emptyset$ gibt.

Angenommen, die Behauptung gilt für Mengen der Mächtigkeit n . Wir betrachten nun eine Menge M der Mächtigkeit $n + 1$ und eine injektive Abbildung $f : M \rightarrow M$. Da M nicht leer ist, können wir ein Element $a \in M$ wählen, und wir setzen $f(a) = b$. Nun sind zwei Fälle zu unterscheiden.

Ist $a = b$, so kann ein Element von $M \setminus \{a\}$ wegen der Injektivität von f nicht auf a abgebildet werden, also können wir eine Abbildung g der Menge $M \setminus \{a\}$ in sich selbst definieren, indem wir $g(x) = f(x)$ für alle $x \in M \setminus \{a\}$ setzen. Aus der Injektivität von f folgt die Injektivität von g . Auf Grund

von $|M \setminus \{a\}| = n$ ist g laut Induktionsvoraussetzung surjektiv. Damit ist aber auch f surjektiv.

Ist $a \neq b$, so betrachten wir die Abbildung $g = t \circ f$, wobei t die Transposition von a und b bezeichnet. Nach Satz 5(i) ist g injektiv, und wegen

$$g(a) = t(f(a)) = t(b) = a$$

können wir wie im schon betrachteten Fall schließen, dass g surjektiv ist. Aus der Gleichheit

$$f = t \circ t \circ f = t \circ g$$

folgt mit Satz 5(iii), dass auch f surjektiv ist. \square

Folgerung 3 *Eine echte Teilmenge einer endlichen Menge hat eine kleinere Mächtigkeit als diese.*

Es gilt übrigens auch die Umkehrung von Satz 20.
Ganz ähnlich beweist man folgenden Satz.

Satz 21 *Jede Teilmenge einer endlichen Menge ist eine endliche Menge.*

Beweis. Die Behauptung gilt offensichtlich für die leere Menge.

Angenommen, sie gilt für alle Mengen der Mächtigkeit n . Ist nun M eine Menge der Mächtigkeit $n + 1$ und N ihre Teilmenge, so gibt es zwei Möglichkeiten. Ist $N = M$, so ist N offensichtlich eine endliche Menge. Ist hingegen $N \subset M$, so gibt es ein Element a von M , das nicht zu N gehört, also ist $N \subseteq M \setminus \{a\}$. Wegen $|M \setminus \{a\}| = n$ ist N nach Induktionsvoraussetzung eine endliche Menge. \square

Folgerung 4 *Gilt für Kardinalzahlen m und n die Ungleichung $m \leq n$ und ist n eine natürliche Zahl, so ist auch m eine natürliche Zahl.*

3.3 Wohlordnung

Wir fragen uns, was es für Mengen gibt, die unter einer Nachfolgerabbildung abgeschlossen sind. Es stellt sich heraus, dass alle solchen Mengen gleich aussehen.

Satz 22 *Ist $s : N \rightarrow N$ eine Nachfolgerabbildung, so ist jede nichtleere s -abgeschlossene Teilmenge von N der s -Abschluss einer Einermenge.*

Beweis. Es sei L eine s -abgeschlossene Teilmenge von N , die nicht der s -Abschluss einer Einermenge ist. Wir bezeichnen mit K die Menge aller Elemente x von N mit der Eigenschaft, dass L im s -Abschluss von $\{x\}$ enthalten ist.

Das Anfangselement a ist natürlich in K enthalten, denn wegen Eigenschaft (iii) aus der Definition 23 ist der s -Abschluss von $\{a\}$ gleich der gesamten Menge N . Ist nun x ein beliebiges Element von K , ist also L im s -Abschluss von $\{x\}$ enthalten, so kann x nicht zu L gehören, denn sonst wäre der s -Abschluss von $\{x\}$ in L enthalten, also gleich L , was unserer Annahme widerspricht. Entfernen wir x aus dem s -Abschluss von x , so erhalten wir laut Aufgabe 25 den s -Abschluss von $s(x)$, und in diesem ist L , wie wir gesehen haben, immer noch enthalten. Mit anderen Worten, es gilt $s(x) \in K$.

Wegen Eigenschaft (iii) der Nachfolgerabbildung s ist $K = N$, das heißt, L liegt im s -Abschluss einer beliebigen Einermenge in N . Ist nun x ein beliebiges Element von N , so muss L insbesondere im s -Abschluss von $\{s(x)\}$ enthalten sein. Da dieser nach Aufgabe 25 nicht das Element x enthält, ist $x \notin L$. Somit ist L die leere Menge.

Wir haben also für jede s -abgeschlossene Teilmenge L von N bewiesen: Ist L nicht der s -Abschluss einer Einermenge, so ist L leer. Die Kontraposition¹⁹ dieser Aussage ist die Behauptung des Satzes. \square

Folgerung 5 *Sind x und y Elemente einer Menge mit Nachfolgerabbildung s , so ist x im s -Abschluss von $\{y\}$ enthalten oder y im s -Abschluss von $\{x\}$ enthalten.*

Gewöhnlich werden für Folgerungen keine Beweise angegeben, da diese kurz und offensichtlich sind. Wir werden sie hier mitunter trotzdem aufschreiben, da es sich um eine Einführung für Anfänger handelt.

Beweis. Der s -Abschluss von $\{x, y\}$, nennen wir ihn L , ist nach Satz 22 der s -Abschluss einer Einermenge $\{z\}$. Wäre $z \notin \{x, y\}$, so wäre $\{x, y\}$ in der Menge $L \setminus \{z\}$ enthalten, die nach Aufgabe 25(a) s -abgeschlossen ist – Widerspruch. Somit ist $z = x$ oder $z = y$. \square

Folgerung 6 *Sind x und y verschiedene Elemente einer Menge N mit Nachfolgerabbildung, so ist $\text{nr}(x) \neq \text{nr}(y)$.*

Beweis. Nach der vorangehenden Folgerung gibt es zwei Fälle. Ist z. B. y im s -Abschluss von x enthalten, aber verschieden von x , so ist der s -Abschluss

¹⁹vgl. Musterlösung zu Aufgabe 2

L von y eine echte Teilmenge des s -Abschlusses K von x , also $N \setminus K \subset N \setminus L$, und mit der Folgerung aus Satz 20 erhalten wir $\text{nr}(x) < \text{nr}(y)$. \square

Da jedem Element von N genau eine natürliche Zahl zugeordnet ist und umgekehrt, bilden auch die natürlichen Zahlen eine Menge, die wir mit \mathbf{N} bezeichnen.²⁰ Die Zuordnung $\text{nr} : N \rightarrow \mathbf{N}$ wird damit zu einer bijektiven Abbildung. Es gibt zwar viele Mengen N mit Nachfolgerabbildungen s , aber nur eine Menge \mathbf{N} der natürlichen Zahlen.

Wir wollen die obigen Ergebnisse in Aussagen über natürliche Zahlen übersetzen. Dazu dient der folgende Satz.

Satz 23 *Es sei $s : N \rightarrow N$ eine Nachfolgerabbildung. Das Element y liegt genau dann im s -Abschluss von $\{x\}$, wenn $\text{nr}(x) \leq \text{nr}(y)$ ist.*

Beweis. Liegt y im s -Abschluss K von $\{x\}$, so ist der s -Abschluss L von $\{y\}$ in K enthalten, und die Argumentation aus dem Beweis der vorangehenden Folgerung liefert $\text{nr}(x) \leq \text{nr}(y)$.

Ist hingegen $y \notin K$, so zeigt Folgerung 5, dass $x \in L$, also $K \subseteq L$ und $N \setminus L \subseteq N \setminus K$. Gleichheit kann hier nicht gelten, weil y in der rechten, aber nicht in der linken Menge enthalten ist. Wegen der Folgerung aus Satz 20 gilt dann $\text{nr}(y) < \text{nr}(x)$, also die Negation von $\text{nr}(x) \leq \text{nr}(y)$. \square

Hier ist die Übersetzung von Satz 22.

Folgerung 7 *Jede nichtleere Teilmenge der Menge der natürlichen Zahlen hat ein kleinstes Element.*

Beweis. Es sei M eine beliebige nichtleere Teilmenge von \mathbf{N} und

$$K = \{x \in N \mid \text{nr}(x) \in M\}.$$

Der s -Abschluss L von K ist nach Satz 22 der s -Abschluss einer Einermenge $\{z\}$. Wäre $z \notin K$, so wäre $L \setminus \{z\}$ nach Aufgabe 25(a) eine s -abgeschlossene Menge, die K enthält – Widerspruch. Also ist $z \in K$, und $\text{nr}(z)$ ist nach Satz 23 das kleinste Element von M . \square

Hier ist die Übersetzung von Folgerung 5 mit Hilfe von Satz 23.

Folgerung 8 *Für beliebige natürliche Zahlen m und n gilt*

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

²⁰An der Tafel wird das fettgedruckte \mathbf{N} meist als \mathbb{N} wiedergegeben.

Man kann dies auch beweisen, indem man Folgerung 7 auf die Menge $\{m, n\}$ von natürlichen Zahlen anwendet. Die Kleiner-Gleich-Relation auf der Menge der natürlichen Zahlen ist also eine totale Relation. Wie wir auf S. 33 erwähnt haben, gilt das auch für die Kleiner-Gleich-Relation auf den Kardinalzahlen, auch wenn wir das damals nicht beweisen konnten.

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

Satz 24 *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. Dieser Satz gilt auch, wenn wir das Wort „natürliche Zahl“ überall durch das Wort „Kardinalzahl“ ersetzen. Da wir im vorigen Abschnitt versäumt haben, ihn zu beweisen, holen wir das jetzt nach. Wir wählen Repräsentanten M und N der Kardinalzahlen m und n . Ist $m \leq n$, so gibt es eine injektive Abbildung $f : M \rightarrow N$. Da M gleichmächtig zum Wertebereich von f ist, können wir M durch diesen ersetzen, so dass $M \subseteq N$. Wegen

$$|M| + |N \setminus M| = |N|$$

brauchen wir nur $l = |N \setminus M|$ zu setzen. Umgekehrt folgt aus der Existenz einer Kardinalzahl l mit der Eigenschaft $m + l = n$ die Ungleichung $m \leq n$ sofort mittels der Definition der Addition.

Sind nun m und n natürliche Zahlen und $m \leq n$, dann gibt es nach dem Bewiesenen eine Kardinalzahl l , so dass $m + l = n$, und wiederum nach dem Bewiesenen ist $l \leq n$. Nach der Folgerung aus Satz 21 ist $l \in \mathbf{N}$. \square

Für Ungleichungen gelten die folgenden Rechenregeln.

Satz 25 *Für alle natürlichen Zahlen 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. Wir halten k und l fest und beweisen die erste Aussage zunächst im Fall $m = n$ durch Induktion nach n . Für $n = 0$ gilt die Behauptung wegen $k + 0 = k$ und $l + 0 = l$. Damit ist der Induktionsanfang beendet.

Angenommen, es gilt $k + n \leq l + n$. Wir müssen beweisen, dass dann gilt

$$k + (n + 1) \leq l + (n + 1).$$

Aufgrund der Assoziativität ist diese Aussage äquivalent zu

$$(k + n) + 1 \leq (l + n) + 1.$$

Um dies zu beweisen, wählen wir eine Nachfolgerabbildung $s : N \rightarrow N$ und Elemente x und y von N , so dass $\text{nr}(x) = k + n$ und $\text{nr}(y) = l + n$. Nach Satz 23 ist y im s -Abschluss von $\{x\}$ enthalten, den wir L nennen. Dann ist aber $s(y)$ im s -Abschluss von $\{s(x)\}$ enthalten, denn dieser ist $\{s(u) \mid u \in L\}$. Mittels Satz 23 übersetzen wir dies zurück in die Aussage

$$\text{nr}(s(x)) \leq \text{nr}(s(y)),$$

und mit der Identität (2) folgt die Induktionsbehauptung.

Nun betrachten wir den Fall, dass m und n verschieden sein können. Aus $k \leq l$ folgt nach dem Bewiesenen

$$k + n \leq l + n,$$

und aus $m \leq n$ folgt durch Umbenennung der Variablen

$$m + k \leq n + k.$$

Unter Benutzung der Kommutativität und der Transitivität folgt dann die Behauptung.

Der Beweis für die Multiplikation ist Inhalt der Übungsaufgabe 26. \square

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 26 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)

Man nennt \preceq eine Wohlordnung, wenn außerdem gilt:

- (iv) Jede nichtleere Teilmenge von M hat ein kleinstes Element bezüglich \preceq .

Wie wir in Folgerung 7 gesehen haben, ist die Kleiner-Gleich-Relation auf der Menge der natürlichen Zahlen eine Wohlordnung. Zu jeder Relation gibt es die umgekehrte Relation, die man mit dem gespiegelten Symbol bezeichnet:

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

So ist die Größer-Gleich-Relation die umgekehrte Relation zur Kleiner-Gleich-Relation. Sie ist eine Ordnung, aber keine Wohlordnung.²¹

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 natürlich 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 27 *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 leicht nach (siehe Aufgabe 29), dass dies tatsächlich eine Ordnung ist. Die Aussage $(v, w) \trianglelefteq (x, y)$ könnte man auch so formulieren:

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

²¹Die Bezeichnung „kleinstes Element“ ist für diese Relation natürlich irreführend, man sollte eher vom ersten Element sprechen, das in diesem Fall das größte sein müsste.

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

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 $x, y \in M$ gilt genau dann $f(x) \preceq f(y)$, 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 die Potenz anders definieren muss, da die lexikographische Ordnung auf N^M im Allgemeinen keine Wohlordnung ist (vgl. Aufgabe 30).

Ein Abschnitt einer wohlgeordneten Menge (M, \leq) ist eine Teilmenge der Form $\{x \in M \mid x \prec y\}$ 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

Folgende Definition ist aus der Schule bekannt.

Definition 28 *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 . 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 .*

Man könnte meinen, dass sich auf dieselbe Weise die Differenz und der Quotient beliebiger Kardinalzahlen definieren ließen. Dies führt aber schnell zu Widersprüchen. Wie wir gesehen haben, gibt es wenigstens eine Mengen N , die gleichmächtig zu einer echten Teilmenge M ist. Mit der Bezeichnung $|M| = |N| = n$ und $|N \setminus M| = k$ erhalten wir laut Definition der Addition

$$n + k = n, \quad k \neq 0,$$

und gleichzeitig ist natürlich $n+0 = n$. Es gäbe also mehrere Kardinalzahlen, die als Differenz in Frage kämen!

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

Satz 26 *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 $k = l$.

Beweis. 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.

Bevor wir zum Induktionsschritt kommen, beweisen wir die Aussage für den Fall $n = 1$. Wir nehmen also an, dass für gewisse natürliche Zahlen k und l gilt

$$k + 1 = l + 1.$$

Wählen wir eine Nachfolgerabbildung $s : N \rightarrow N$, so gibt es nach Definition 24 Elemente $x, y \in N$, so dass $\text{nr}(x) = k$ und $\text{nr}(y) = l$. Mit Hilfe der Formel (2) können wir unsere Annahme in der Form

$$\text{nr}(s(x)) = \text{nr}(s(y))$$

formulieren. Mit Folgerung 6 folgt $s(x) = s(y)$, und wegen der Injektivität von s folgt $x = y$. Somit ist $k = l$.

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 folgt aus dem schon bewiesenen Fall, dass

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

und dann folgt aus der Induktionsvoraussetzung, dass $k = l$.

Der Beweis der Kürzungsregel für die Multiplikation ist Gegenstand der Übungsaufgabe 32. \square

Wir sehen, dass die Differenz und der Quotient von natürlichen Zahlen m und n , wenn sie denn existieren, eindeutig bestimmt sind. Man bezeichnet sie mit $m - n$ bzw. $m : n$. (In englischsprachigen Ländern schreibt man den Quotienten als $m \div n$, und das entsprechende Zeichen findet man auch auf den meisten Taschenrechnern.) Die Rechenoperationen zur Ermittlung dieser Zahlen nennt man bekanntlich *Subtraktion* bzw. *Division*. Aus Satz 24 erhalten wir:

Folgerung 9 *Die Differenz von natürlichen Zahlen m und n existiert genau dann, wenn $m \geq n$ ist.*

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

Definition 29 *Es seien m und n natürliche Zahlen. Man nennt m ein Vielfaches von n und nennt n einen Teiler von m , wenn es eine natürliche Zahl k gibt, so dass $n \cdot k = m$. Als Abkürzung schreibt man $n \mid m$ (gelesen „ n teilt m “).*

Der Quotient $m : n$ existiert also genau dann, wenn $n \neq 0$ und $n \mid m$. In diesem Fall sagt man, dass m durch n teilbar ist. Zahlen, die durch 2 teilbar sind, nennt man auch gerade Zahlen.

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: Die Assoziativgesetze der Subtraktion und der Division sowie das Distributivgesetz der Division.

Satz 27 *Es seien l , m und n natürliche Zahlen. Ist $n \geq l$, so gilt*

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

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. Ist $n \geq l$, so gibt es nach Satz 24 eine natürliche Zahl k , so dass $l+k = n$. Nun ist wegen der Kommutativität und Distributivität der Addition

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

und nach Definition der Subtraktion folgt

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

Durch Einsetzen der ersten Gleichung in die zweite folgt das Assoziativgesetz der Subtraktion. Die anderen Gesetze sind in Aufgabe 33 zu beweisen. \square

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 25, 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 folgenden Satz begründet.

Satz 28 *Sind m und $n \neq 0$ beliebige natürliche Zahlen, so 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 ist Gegenstand von Aufgabe 27. Nun zur Eindeutigkeit. Angenommen, es gibt natürliche Zahlen q' und r' , die auch die Eigenschaften

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

haben. Wegen der Totalität gilt $r \leq r'$ oder $r' \leq r$, und wir können die Bezeichnungen so wählen, dass $r \leq r'$. Es gilt die Gleichung

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

Die linke Seite der Gleichung (und somit auch die rechte) ist nach Satz 24 größer oder gleich r , also können wir auf beiden Seiten die Zahl r subtrahieren. Nach Satz 27 erhalten wir

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

Hier ist die rechte Seite größer oder gleich $q' \cdot n$, und durch Subtraktion dieser Zahl von beiden Seiten erhalten wir

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

Mit der Distributivität aus Satz 27 folgt

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

Wäre $q - q' \neq 0$, so wäre nach Satz 25 die linke Seite größer oder gleich n . Das kann aber nicht sein, denn die rechte Seite ist kleiner oder gleich r' , also kleiner als n . Damit muss $q - q' = 0$ sein, und wenn wir dies einsetzen, folgt $r' - r = 0$. Somit ist $q = q'$ und $r = r'$. \square

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 Zahl 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

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

fort. Diese beiden Gleichungen bilden eine sogenannte rekursive Definition.

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

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 b begonnen und bei jeder folgende Silbe zum linken Nachbarn übergegangen. Nummeriert man die Silben durch, so wird jeder natürlichen Zahl n ein Kind zugeordnet.

In den drei betrachteten Beispielen wird jeweils einer natürlichen Zahl nach der anderen ein Element einer gegebenen Menge M zugeordnet. Um damit eine Abbildung $g : \mathbf{N} \rightarrow M$ zu definieren, muss die gesamte Zurodnung gewissermaßen sofort gegeben sein. Dass diese Abbildung g existiert, folgt aus Satz 17:

Folgerung 10 *Ist f eine Abbildung einer Menge M in sich selbst und $b \in M$, so gibt es genau eine Abbildung $g : \mathbf{N} \rightarrow M$, so dass*

$$g(0) = b \quad \text{und} \quad g(n+1) = f(g(n)) \quad \text{für alle } n \in \mathbf{N}.$$

Dies lässt sich am Einfachsten begründen, wenn man die Menge der natürlichen Zahlen selbst als Menge mit der Nachfolgerabbildung $s(n) = n+1$ betrachtet.

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

Will man aus einer Definition wie in obiger Folgerung z. B. eine Formel für $g(100)$ 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 b einsetzen kann. Aus diesem Grund spricht man von einer *rekursiven* (lat. rückläufigen) Definition.

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:

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

Da die Verkettung nicht kommutativ ist, braucht $(f \circ g)^n$ nicht gleich $f^n \circ g^n$ zu sein, aber die übrigen Potenzgesetze gelten, z. B.

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

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 die Zwischenergebnisse

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

aus dem Beweis von Satz 10.

Die letztgenannte Gleichmächtigkeit wurde durch eine bijektive Abbildung vermittelt, die die verschachtelten geordneten Paare

$$((x, y), z), \quad (x, (y, z))$$

aufeinander bezog. Vereinfachend schreibt man die Elemente von $L \times M \times N$ auch als sogenannte Tripel

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

wobei $x \in L$, $y \in M$ und $z \in N$. 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 $t = z$. Analog 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).

Wir haben festgestellt, dass wir in einem Ausdruck wie $x + y + z$, in dem x, y und z natürliche Zahlen bedeuten, wegen des Assoziativgesetzes keine Klammern zu setzen brauchen. 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.

$$\sum_{i=7}^{236} x_i = \sum_{p=7}^{236} x_p.$$

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

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

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 29 Für alle natürlichen Zahlen $l \leq m < n$ und k gelten das Assoziativgesetz

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

und die Substitutionsregel

$$\sum_{i=m}^n x_{i+k} = \sum_{j=m+k}^{n+k} x_j$$

sowie die analogen Aussagen für das Produktzeichen. Außerdem gilt 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 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.

Die anderen Behauptungen sind in Übungsaufgabe 36 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, z. B. in Indien und China. Hier sind die chinesischen Zahlzeichen von Eins bis Neun:

??

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 diese Wörter durch je ein Zeichen notiert:

??

Damit kann man alle Zahlen kleiner als einhunderttausend bezeichnen. Die Maya bildeten auf jeder Ebene Zwanzigerbündel, deren Anzahl sie mit Hilfe der Zeichen . bis ≡ notierten.

Manche Kulturen (z. B. die babylonische und die chinesische) ließen oft die Zeichen für die Bündel weg, was natürlich zu Verwechslungen führte. Nur

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.

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:	•	١	٢	٣	٤	٥	٦	٧	٨	٩
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.

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

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 $A = 10, B = 11, \dots, F = 15$.

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.
- 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, warum und wie Stellenwertsysteme funktionieren. 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.

Satz 30 *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 viele 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,

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

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 Zahl 625 ins ternäre System umzuwandeln, dividieren wir entsprechend Satz 28 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 wir

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

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:

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

Bevor wir zum Beweis des Satzes kommen, erläutern wir eine neue Version der vollständigen Induktion. Um eine Aussage für alle natürlichen Zahlen zu beweisen, genügt es, ihre Gültigkeit für eine beliebige natürliche Zahl aus der Gültigkeit für *alle* kleineren natürlichen Zahlen zu folgern. Wenn es nämlich natürliche Zahlen gäbe, für die die Aussage nicht gilt, so gäbe es nach Satz 22 eine kleinste solche Zahl. Aus dem Beweisenen würde dann aber folgen, dass die Aussage auch für diese Zahl gilt, und das ist ein Widerspruch. Bei dieser Art vollständiger Induktion ist der Induktionsanfang offenbar ein Spezialfall des Induktionsschritts.

Beweis von Satz 30. Wir können annehmen, dass die Behauptung gilt, wenn wir n durch eine beliebige kleinere natürliche Zahl ersetzen. Nach Satz 28 gibt es natürliche Zahlen q und $r < g$, so dass

$$n = qg + r.$$

Nach Satz 23 ist $n \geq qg$, und nach Satz 25 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 28 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 29 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:

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

(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

$$212011_3 \cdot 122_3 = 112120112_3.$$

Durch Rückverwandlung ins Dezimalsystem kann man die Probe machen:

$$625 \cdot 17 = 10625.$$

Nachtrag zum vorigen Abschnitt

In Satz 29 fehlten noch zwei Rechenregeln.

Satz 31 Für alle natürlichen Zahlen $m \leq n$ gilt das weitere Assoziativgesetz

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

und wenn $x_i \leq y_i$ für alle $i \in \{m, m+1, \dots, n\}$, dann gilt

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

Dabei bezeichnen x_i und y_i natürliche Zahlen.

Der Beweis ist analog zu Aufgabe 41 unter Benutzung des Assoziativgesetzes (Satz 8) und von Satz 25.

Wir wenden uns nun der Frage zu, wie man einen zweigliedrigen Term (ein Binom) potenzieren und wie man eine Differenz von Potenzen mit gleichem Exponenten umformen kann.

Satz 32 (Binomische Formeln) Für beliebige natürliche Zahlen a, b und n gilt

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i$$

und, wenn $a \geq b$ ist,

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

Dies erklärt die Bezeichnung *Binomialkoeffizient* für die in Aufgabe 24 eingeführten Zahlen $\binom{n}{i}$.³⁰ Ohne Benutzung des Summenzeichens kann man die binomischen Formeln so schreiben:

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a b^{n-1} + b^n,$$
$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2} b + a^{n-3} b^2 + \dots + a b^{n-2} + b^{n-1}).$$

Beweis. Die erste binomische Formel gilt für $n = 0$, weil dann beide Seiten laut Definition gleich 1 sind.

³⁰Die Englische Bezeichnung „(from) n choose i “ ist natürlich durch die Definition in Aufgabe 24 motiviert.

Angenommen, die Formel gilt für eine Zahl n . Nach Definition der Potenz und nach Induktionsvoraussetzung ist

$$(a + b)^{n+1} = (a + b) \cdot (a + b)^n = (a + b) \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

Nach den Distributivgesetzen aus Satz 10 und Satz 29 sowie der Definition der Potenz ist die rechte Seite gleich

$$a \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i + b \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i = \sum_{i=0}^n \binom{n}{i} a^{(n-i)+1} b^i + \sum_{i=0}^n \binom{n}{i} a^{n-i} b^{i+1}.$$

In der zweiten Summe können wir $\binom{n}{i} = \binom{n}{(i+1)-1}$ und (im Exponenten) $n-i = ((n+1)-1) - i = (n+1) - (i+1)$ schreiben (vgl. Präsenzaufgabe 16). Unter Benutzung der Substitutionsregel aus Satz 29 wird unser Ausdruck zu

$$\sum_{i=0}^n \binom{n}{i} a^{(n-i)+1} b^i + \sum_{j=1}^{n+1} \binom{n}{j-1} a^{(n+1)-j} b^j.$$

Mit Hilfe von Satz 29 spalten wir von der ersten Summe den Term mit $i = 0$ 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 i auch in der ersten Summe bis $n + 1$ laufen lassen (und durch j ersetzen). Nach dem Assoziativgesetz aus Satz 31 erhalten wir

$$(a + b)^{n+1} = a^{n+1} + \sum_{j=1}^{n+1} \left(\binom{n}{j} + \binom{n}{j-1} \right) a^{(n+1)-j} b^j.$$

Mit Hilfe der Formel

$$\binom{n}{j} + \binom{n}{j-1} = \binom{n+1}{j}$$

aus Aufgabe 24 und nach Wiedereingliederung des Terms mit $j = 0$ folgt die Induktionsbehauptung.

Der Beweis der anderen binomischen Formel ist die Übungsaufgabe 43. \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, so wie wir sie in Aufgabe 24 definiert haben, 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 $a^{n-i}b^i$ entsteht dabei so oft, wie es Teilmengen der Mächtigkeit i gibt, also $\binom{n}{i}$ mal. Man kann diese Argumentation zu einem streng logischen Beweis ausbauen, was wir hier aber nicht tun werden.

Zurück zu Stellenwertsystemen

Wie kann man an der Zifferndarstellung zweier natürlicher Zahlen in einem Stellenwertsystem erkennen, welche von beiden die kleinere ist? Da wir die Ziffern links mit Nullen auffüllen, benötigen wir keine Fallunterscheidung in Abhängigkeit von der Stellenzahl.

Satz 33 *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 $c_j < c'_j$.*

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 und hat nach Aufgabe 28 (angewendet auf die \geq -Relation) ein größtes Element.

Beweis. Ist $n \neq n'$, so können diese Zahlen nach Satz 30 nicht die selbe Ziffernfolge haben. Nun sei j die größte natürliche Zahl, so dass $c_j \neq c'_j$ ist. Weil $c_i \leq g - 1$ und $c'_i \geq 0$ für $i \in \{0, 1, \dots, j - 1\}$ ist, gilt nach Satz 29 und 31

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

wobei wir zwar den Summationsindex i formal bis ∞ (gelesen „unendlich“) laufen lassen, aber in Wirklichkeit nur endlich viele Summanden nicht Null sind. Ersetzen wir in der zweiten binomischen Formel in Satz 32 die Zahlen a , b und n durch g , 1 und j , so erhalten wir³¹

$$(g - 1)(1 + g + g^2 + \dots + g^{j-1}) = g^j - 1,$$

also mit dem Assoziativgesetz aus Satz 29

$$\sum_{i=0}^{j-1} (g - 1)g^i < g^j,$$

und durch Einsetzen 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 $c_j < c'_j$, also $c_j + 1 \leq c'_j$, so folgt

$$n < c'_j g^j + \sum_{i=j+1}^{\infty} c_i g^i = \sum_{i=j}^{\infty} c'_i g^i \leq n',$$

also $n < n'$. Ist hingegen $c_j > c'_j$, so zeigt man analog, dass $n > n'$. \square

Die Kleiner-Gleich-Relation auf \mathbf{N} entspricht also der lexikographischen Ordnung (im Sinne von Aufgabe 30) auf der Menge der Ziffernfolgen, wenn wir diese als Abbildungen von \mathbf{N} in die Menge $\{0, 1, \dots, g - 1\}$ der Ziffern auffassen und den Definitionsbereich \mathbf{N} mit der Größer-Gleich-Relation versehen.

In der Musterlösung zu Aufgabe 30 haben wir gesehen, dass die lexikographische Ordnung auf N^M , die zu Wohlordnungen \leq auf M und \preceq auf N gehört, im Allgemeinen keine Wohlordnung ist. Der vorige Satz legt nahe, wie man trotzdem eine Potenz von Ordinalzahlen definieren kann. Man betrachtet nicht die Menge aller Abbildungen $f : M \rightarrow N$, sondern nur solcher, bei denen $f(x)$ mit Ausnahme endlich vieler Elemente x von M gleich dem kleinsten Element von N ist, und benutzt die lexikographische Ordnung, die zu \preceq und zur umgekehrten Ordnung von \leq gehört.

Vergisst man die Ordnung auf einer wohlgeordneten Menge, so erhält man eine Menge. Auf diese Weise kann man jeder Ordinalzahl eine Kardinalzahl zuordnen. Diese Zuordnung ist mit Summen und Produkten, aber nicht mit Potenzen verträglich.

³¹Eigentlich erscheinen die Summanden in umgekehrter Reihenfolge. Dass man diese ändern kann, ist strenggenommen eine weitere Substitutionsregel, die man beweisen muss.

Wir können nun aus der g -adischen Darstellung

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

einer natürlichen Zahl leicht die h -adische Darstellung gewinnen, wenn h eine Potenz von g ist, sagen wir $h = g^k$. Wir fassen dazu immer k aufeinanderfolgende Terme zusammen und klammern die höchstmögliche Potenz von g aus:

$$\begin{aligned} n &= (c_0 + c_1g + c_2g^2 + \dots + c_{k-1}g^{k-1}) \\ &\quad + (c_k + c_{k+1}g + c_{k+2}g^2 + \dots + c_{2k-1}g^{k-1})g^{2k} \\ &\quad + (c_{2k} + c_{2k+1}g + c_{2k+2}g^2 + \dots + c_{3k-1}g^{k-1})g^{3k} \\ &\quad + \dots \\ &\quad + (c_{lk} + c_{lk+1}g + c_{lk+2}g^2 + \dots + c_{(l+1)k-1}g^{k-1})g^{lk} \\ &\quad + \dots \end{aligned}$$

Nach einem Potenzgesetz ist $g^{lk} = h^k$, und nach der zweiten binomischen Formel ist

$$\begin{aligned} c_{lk} + c_{lk+1}g + c_{lk+2}g^2 + \dots + c_{(l+1)k-1}g^{k-1} \\ \leq (g-1)(1 + g + g^2 + \dots + g^{k-1}) = g^k - 1 < h, \end{aligned}$$

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 Praxis für $g = 2$ und $h = 8$ oder $h = 16$ angewendet.

Begründung der schriftlichen Rechenverfahren

Bei der **schriftlichen Addition** von zwei natürlichen Zahlen, die im g -adischen System gegeben sind, können wir die Ziffern ihrer Summe nicht einfach dadurch ermitteln, dass wir ihre Ziffern Stelle für Stelle addieren, weil die dabei entstehenden Zahlen nicht immer kleiner als g sind. Die Summe zweier Ziffern a und b ist

$$a + b \leq (g-1) + (g-1) \leq 1 \cdot g + (g-2),$$

also nach Satz 33 höchstens zweistellig mit höchster Ziffer (genannt Übertrag) nicht größer als 1. Handelt es sich um die k -te Stelle, so ist der Beitrag zur Summe gleich

$$ag^k + bg^k \leq 1 \cdot g^{k+1} + (g-2)g^k,$$

der Übertrag ist also zur $(k + 1)$ ten Stelle hinzuzufügen. Darum muss man mit der Einerstelle, also $k = 0$, beginnen und zu immer höheren Stellen fortschreiten. Haben wir an einer Stelle bereits einen Übertrag $u \leq 1$ von der vorhergehenden Stelle, so erhalten wir

$$a + b + u \leq (g - 1) + (g - 1) + 1 \leq 1 \cdot g + (g - 1),$$

also entsteht auch hier höchstens der Übertrag 1. Darum funktioniert das schriftliche Additionsverfahren.

Versucht man mehr als zwei Zahlen gleichzeitig zu addieren, so können beliebig große (auch mehrstellige) Überträge 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.

Kommen wir nun zur **schriftlichen Subtraktion**. Bezeichnen wir die k te Ziffer des Minuenden mit a und die k te Ziffer des Subtrahenden mit b , so liefern sie im Fall $a \geq b$ den Beitrag $ag^k - bg^k$ 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^{k+1} verringert) und dafür die Zahl a 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^{k+1} das Selbe bewirkt wie eine Vergrößerung des Subtrahenden um g^{k+1} (siehe Präsenzaufgabe 16). Bei Anwendung dieser Technik ist der Übertrag 1 also der nächsthöheren Stelle des Subtrahenden zuzuschlagen.

Es kann vorkommen, dass bei der k ten Stelle bereits ein Übertrag $u \leq 1$ von der $(k - 1)$ ten Stelle zu berücksichtigen ist. Ist $a \geq b + u$, so erhalten wir als k te Ziffer der Differenz die Zahl $a - (b + u)$, die nicht größer als a , also kleiner als g ist. Ist hingegen $a < b + u$, so ergibt sich als k te Ziffer der Differenz

$$a + (g - (b + u)) = g - ((b + u) - a) = (a + g) - (b + u).$$

Der erste Ausdruck ist wegen $b + u \leq g$ wohldefiniert, der zweite ist wegen $a < b + u$ kleiner als g , also eine Ziffer. Der dritte zeigt, dass wir a durch $a + g$ ersetzt haben, also müssen wir wie beschrieben einen Übertrag zur nächsten Stelle vornehmen. Es pflanzt sich also höchstens ein Übertrag von 1 fort, und darum funktioniert das schriftliche Subtraktionsverfahren.

Für die **schriftliche Multiplikation** zerlegt man den zweiten Faktor (den Multiplikator) in Terme der Form bg^l und benutzt das Distributivgesetz. Damit wird die Multiplikation auf das Teilproblem zurückgeführt, den ersten

Faktor (den Multiplikanden) mit einer Zahl der Form bg^l zu multiplizieren. Nach dem Assoziativgesetz kann man erst mit b und dann mit g^l multiplizieren, wobei der zweite Schritt eine Verschiebung der Ziffern um l Stellen nach links und das Anhängen von ebenso vielen Nullen bewirkt. Diese Nullen werden im Zwischenergebnis meist nicht mitgeschrieben.

Um nun den Multiplikanden mit einer Ziffer b des Multiplikators zu vervielfachen, geht man stellenweise vor. Steht an der k ten Stelle des Multiplikanden die Ziffer a , so liefert sie den Beitrag abg^k . Man schreibt diese Produkte nicht auf, sondern addiert sie, beginnend mit der Einerstelle ($k = 0$). Die Zahl

$$ab \leq (g-1)(g-1) < (g-1)g$$

ist höchstens zweistellig mit höchster Stelle kleiner als $g-1$. Diese bewirkt einen Übertrag. Kommt von der $(k-1)$ ten Stelle bereits ein Übertrag $u < g-1$ hinzu, so erhalten wir

$$ab + u < (g-1)(g-1) + (g-1) = (g-1)g,$$

also entsteht auch hier ein Übertrag kleiner als $g-1$ zur $(k+1)$ ten Stelle, und das pflanzt sich durch alle Stellen fort. Deshalb funktioniert das schriftliche Multiplikationsverfahren.

Um die **schriftliche Division** zu begründen, merken wir an, dass sich der abgerundete Quotient q bei der Division einer natürlichen Zahl m durch eine natürliche Zahl n , der laut Satz 28 durch die Bedingungen

$$m = qn + r, \quad r < n$$

bestimmt ist, auch ohne Erwähnung des Restes r charakterisieren lässt. Die Zahl q ist nämlich die größte natürliche Zahl mit der Eigenschaft

$$qn \leq m.$$

In der Tat, jede größere Zahl ist von der Form $q+s$, wobei $s \geq 1$, und dann ist $(q+s)n = qn + sn \geq qn + n > qn + r = m$, d. h. $(q+s)n > m$.

Bei der schriftlichen Division von m durch n bestimmt man zunächst die größte natürliche Zahl k , so dass

$$ng^k \leq m.$$

Da die Multiplikation mit g^k eine Verschiebung der g -adischen Stellen bewirkt, ist der größte Wert von k leicht mit Hilfe von Satz 33 zu bestimmen. Nun bestimmt man den abgerundeten Quotienten c von m und ng^k , d. h.

$$m = cng^k + r, \quad r < ng^k,$$

wobei r natürlich eine andere Bedeutung als im vorigen Absatz hat. Wäre $c \geq g$, so hätten wir $m \geq ng^{k+1} + r \geq ng^{k+1}$, was der maximalen Wahl von k widerspräche. Somit gilt

$$c < g,$$

das heißt, c ist eine Ziffer. Da sie mit dem Faktor g^k auftritt, ist sie ein Beitrag zur k ten Stelle des Quotienten. Wenden wir das selbe Verfahren rekursiv auf den Rest r an, so erhalten wir wegen $r < ng^k$ nur Beiträge zu niedrigeren Stellen, und Überträge treten bei diesem Verfahren im Quotienten nicht auf. Damit ist c die endgültige k te Stelle des Quotienten.

Die Schwierigkeit des Verfahrens liegt in der Bestimmung des abgerundeten Quotienten c , wofür Satz 28 kein schnelleres Verfahren liefert als die wiederholte Subtraktion. In der Praxis genügt bei einstelligen Divisoren n die Kenntnis des kleinen Einmaleins, bei mehrstelligen Divisoren errät man c durch einen Überschlag, 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 nur die Zahlen 0 und 1 in Frage, und die Bestimmung von c läuft auf einen Vergleich an Hand von Satz 33 hinaus.

4 Ganze Zahlen

4.1 Motivation und Definition

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 möchte die Menge \mathbf{N} der natürlichen Zahlen zu einem größeren Zahlbereich \mathbf{Z} erweitern, in dem dieser Mangel nicht besteht. Genauer gesagt wollen wir eine Menge \mathbf{Z} mit Operationen Addition und Multiplikation finden, so dass \mathbf{N} eine Teilmenge von \mathbf{Z} ist und dass für natürliche Zahlen die Operationen mit den früher betrachteten Operationen übereinstimmen. Des weiteren wünschen wir, dass die für natürliche Zahlen bekannten Rechengesetze auch für beliebige Zahlen a , b und c in \mathbf{Z} gelten, nämlich die Kommutativ-, Assoziativ- und Distributivgesetze

$$\begin{aligned} a + b &= b + a, & a \cdot b &= b \cdot a, \\ (a + b) + c &= a + (b + c), & (a \cdot b) \cdot c &= a \cdot (b \cdot c), \\ a \cdot (b + c) &= a \cdot b + a \cdot c. \end{aligned} \tag{3}$$

Die uneingeschränkte Ausführbarkeit der Subtraktion bedeutet dann Folgendes: Für beliebige Zahlen a und b in \mathbf{Z} gibt es eine Zahl $c \in \mathbf{Z}$, so dass

$$a = b + c.$$

Diese Zahl c bezeichnet man dann als Differenz von a und b , abgekürzt $a - b$.

Wenn die genannten Rechengesetze gelten, dann folgen automatisch weitere, nämlich die Assoziativ- und Distributivgesetze der Subtraktion:

$$\begin{aligned} (a + b) - c &= a + (b - c), & (a - b) - c &= a - (b + c), \\ (a - b) + c &= a - (b - c), & a \cdot (b - c) &= a \cdot b - a \cdot c. \end{aligned} \tag{4}$$

Der Beweis ist ähnlich wie für natürliche Zahlen, nur einfacher, weil man jetzt keine Bedingungen für die Existenz der Differenzen nachprüfen muss. Bezeichnen wir z. B. $b - c$ mit d , so ist d nach Definition diejenige Zahl, für die gilt $b = c + d$. Dann gilt aber nach Kommutativ- und Assoziativgesetz der Addition

$$a + b = a + (c + d) = a + (d + c) = (a + d) + c, \tag{6}$$

also $(a + b) - c = a + d$, und durch Einsetzen folgt das erste Distributivgesetz der Subtraktion. Ähnlich beweist man die anderen. Mit Hilfe der Kommutativgesetze folgert man schließlich aus den angegebenen (linken) Distributivgesetzen die rechten Distributivgesetze

$$(b + c) \cdot a = b \cdot a + c \cdot a, \quad (b - c) \cdot a = b \cdot a - c \cdot a.$$

All das ist natürlich nur eine Wunschliste. Wir wissen noch nicht, ob eine solche Menge \mathbf{Z} mit Operationen $+$ und \cdot existiert. Wir nehmen das zunächst einmal an und folgern daraus weitere Eigenschaften von \mathbf{Z} , die uns hoffentlich auf eine Idee bringen, wie wir eine solche Menge konstruieren könnten.

Jede Teilmenge von \mathbf{Z} , die die Menge \mathbf{N} enthält und abgeschlossen³² unter Addition, Multiplikation und Subtraktion ist, erfüllt bereits alle Wünsche, die wir an die Menge \mathbf{Z} hatten. Jede solche Menge muss alle Differenzen $m - n$ von natürlichen Zahlen m und n enthalten. Die Menge aller solcher Differenzen ist bereits abgeschlossen unter Addition, Multiplikation und Subtraktion, denn nach den Rechengesetzen gilt

$$\begin{aligned} (k - l) + (m - n) &= (k + m) - (l + n), \\ (k - l) - (m - n) &= (k + n) - (l + m), \\ (k - l) \cdot (m - n) &= (k \cdot m + l \cdot n) - (k \cdot n + l \cdot m). \end{aligned} \tag{7}$$

Wir führen den Beweis nur im Fall der Subtraktion vor: Indem wir nacheinander das dritte und das zweite Assoziativgesetz der Subtraktion, das Kommutativgesetz der Addition, das erste **Assoziativgesetz** der Subtraktion und wieder das Kommutativgesetz der Addition anwenden, erhalten wir

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

An Stelle von \mathbf{Z} können wir also die Teilmenge aller Differenzen natürlicher Zahlen nehmen. Mit anderen Worten, wir können annehmen, dass jedes Element der Menge \mathbf{Z} eine Differenz natürlicher Zahlen ist.

In diesem Fall 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

$$k - l = m - n.$$

³²Dieser Begriff der Abgeschlossenheit ist analog zu dem in Definition 21 betrachteten.

Nach Definition der Differenz und nach den Rechengesetzen folgt

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

also

$$k + n = l + m. \tag{8}$$

Da wir die Umformungen auch in umgekehrter Reihenfolge vornehmen können, ist die letzte Bedingung 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

$$\{(m, n) \in \mathbf{N} \times \mathbf{N} \mid f(m, n) = a\}, \tag{9}$$

die wegen der Surjektivität von f nicht leer ist.

Wenn wir auf der Menge $\mathbf{N} \times \mathbf{N}$ die Relation der Differenzgleichheit, abgekürzt³³ \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. Genau wie für die Relation der Gleichmächtigkeit folgt daraus, dass die Menge $\mathbf{N} \times \mathbf{N}$ in Äquivalenzklassen zerfällt, und diese sind genau die Mengen in (9).

All unsere Betrachtungen stehen auf tönernen Füßen, solange wir nicht wissen, ob die erhoffte Menge \mathbf{Z} mit den Operationen $+$ und \cdot überhaupt existiert. Glücklicherweise können wir die Relation \sim mittels (8) und die Rechenoperationen mittels (7) beschreiben, ohne die gesuchte Menge \mathbf{Z} zu benutzen.

Definition 30 *Wir definieren eine 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:

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

³³Da 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.

Satz 34 (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.

$$\text{wenn } (k, l) \sim (m, n), \text{ dann } (m, n) \sim (k, l),$$

denn nach dem Kommutativitätsgesetz der Addition gilt

$$\text{wenn } k + n = l + m, \text{ dann } m + l = n + k.$$

Die Relation \sim ist *transitiv*, d. h.

$$\text{wenn } (k, l) \sim (m, n) \text{ und } (m, n) \sim (p, q), \text{ dann } (k, l) \sim (p, q).$$

Diese Aussage bedeutet:

$$\text{Wenn } k + n = l + m \text{ und } m + q = n + p, \text{ dann } k + q = l + p.$$

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 8) können wir beide Seiten umformen und erhalten

$$(k + q) + (m + n) = (l + p) + (m + n),$$

und nach der Kürzungsregel (Satz 26) 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, dass gilt

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

Diese Aussage ist nach den Rechengesetzen der Addition äquivalent zu

$$(k + l') + (m + n') = (l + k') + (n + m'),$$

und Letztere folgt unmittelbar aus unseren Voraussetzungen.

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. Das ist ganz analog zu den Mächtigkeitsklassen von Mengen, vgl. S. 19. 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 31 Die Menge \mathbf{Z} ist die Menge der Äquivalenzklassen von geordneten Paaren natürlicher Zahlen bezüglich der Relation der Differenzgleichheit. Die Elemente von \mathbf{Z} nennen wir ganze Zahlen, 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 35 (i) Für beliebige ganze Zahlen a, b und c gelten die Rechengesetze (3).

(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 $m, n \in \mathbf{N}$ 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:

$$\begin{aligned} (km + ln)p + (kn + lm)q &= (kmp + lnq) + (knq + lmq) \\ &= (kmp + knq) + (lnq + lmq) = k(mp + nq) + l(mq + np), \end{aligned}$$

und für die hinteren Komponenten prüft man es analog.

Ähnlich beweist man die anderen Rechengesetze.

(ii) Ist $a = [k, l]$, und $b = [n, m]$, so bringt uns die mittlere Gleichung in (7) auf die Idee, $c = [k + m, l + n]$ zu setzen, und dann ist nach der Definition der Addition und den Rechengesetzen für natürliche Zahlen

$$\begin{aligned} b + c &= [n, m] + [k + m, l + n] = [n + (k + m), m + (l + n)] \\ &= [k + (m + n), l + (m + n)]. \end{aligned}$$

Diese Klasse ist die selbe wie $[k, l] = a$, weil

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

also $(k + (m + n), l + (m + n)) \sim (k, l)$.

(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. \square

Aussage (i) rechtfertigt unsere eingangs gezogenen Schlüsse, bei denen wir die Existenz der ganzen Zahlen und die Gültigkeit der Rechengesetze zunächst angenommen hatten. Aufgrund von Aussage (ii) ist auch die Differenz $a - b$ von ganzen Zahlen definiert.

Folgerung 11 Für alle ganzen Zahlen gelten die Rechengesetze (4) der Subtraktion und die rechten Distributivgesetze (6). Außerdem gelten für alle ganzen Zahlen a, b, c und d die weiteren Rechengesetze

$$\begin{aligned} (a - b) + (c - d) &= (a + c) - (b + d), \\ (a - b) - (c - d) &= (a + d) - (b + c), \\ (a - b) \cdot (c - d) &= (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c). \end{aligned} \tag{10}$$

Die letztgenannten Rechengesetze hatten wir zwar nur für natürliche Zahlen bewiesen, siehe Gleichungen (7), aber der Beweis ist für alle ganzen Zahlen richtig (vgl. Aufgabe 48).

Zwar hat sich unser Wunsch, dass \mathbf{Z} die Menge \mathbf{N} als Teilmenge enthält, nicht erfüllt, aber die Aussage (iii) des Satzes ist ein hinreichender Ersatz, weil wir mit den Bildern der natürlichen Zahlen unter der Abbildung i genau so rechnen können wie mit diesen Zahlen selbst.³⁴ 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. Insbesondere sind 0 und 1 jetzt ganze Zahlen, und es folgt aus den Definitionen, dass für alle ganzen Zahlen a gilt

$$a + 0 = a, \quad a - 0 = a, \quad a \cdot 0 = 0, \quad a \cdot 1 = a.$$

Es hat sich eingebürgert, für den Ausdruck $0 - a$ die Abkürzung $-a$ zu verwenden. Man nennt $-a$ die zu a *entgegengesetzte Zahl*. Ebenso kann man anstelle von $0 + a$ auch $+a$ schreiben, was aber das selbe wie a ist und darum kaum vorkommt. Wenn wir in den Rechengesetzen (10) für je zwei Variablen Null einsetzen, ergeben sich folgende Regeln:

$$\begin{aligned} a + (-d) &= a - d, & (-b) + c &= c - b, & (-b) + (-d) &= -(b + d), \\ a - (-d) &= a + d, & (-b) - c &= -(b + c), & (-b) - (-d) &= d - b, \\ & & -(c - d) &= d - c, & & \\ a \cdot (-d) &= -a \cdot d, & (-b) \cdot c &= -b \cdot c, & (-b) \cdot (-d) &= b \cdot d. \end{aligned}$$

Insbesondere sehen wir, dass die entgegengesetzte Zahl zu $m - n$ gleich $n - m$ ist. Setzen wir drei Variablen gleich Null, so folgt

$$-(-d) = d.$$

Das Zeichen $-$ in einem Ausdruck $-n$, wobei n eine natürliche Zahl ist, nennt man ein *Vorzeichen*.³⁵

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

³⁴Man 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.

³⁵In mathematikdidaktischen Schriften kommt die irrige Auffassung vor, Vorzeichen seien grundsätzlich von Operationszeichen zu unterscheiden, es werden sogar Bezeichnungen wie n^- oder ^-n vorgeschlagen.

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“).

4.2 Vergleich von ganzen Zahlen

Wir wollen die für natürliche Zahlen definierte Kleiner-Gleich-Relation so zu einer Ordnungsrelation auf der Menge der ganzen Zahlen fortsetzen, dass die erste Rechenregel aus Satz 25 auch für ganze Zahlen a , b , c und d gilt, nämlich

$$\text{Wenn } a \leq b \text{ und } c \leq d, \text{ dann } a + c \leq b + d.$$

Nehmen wir einmal an, das wäre möglich. Da sich ganze Zahlen als Differenzen natürlicher Zahlen darstellen lassen, geht es um Aussagen der Form

$$k - l \leq m - n, \tag{11}$$

wobei k , l , m und n natürliche Zahlen sind. Aus der genannten Aussage folgt nach den obigen Regeln, wenn wir für c und d jeweils die Zahl $l + n$ wählen, dass

$$(k - l) + (l + n) \leq (m - n) + (l + n).$$

Unter Benutzung der Rechenregeln können wir beide Seiten vereinfachen und erhalten

$$k + n \leq l + m. \tag{12}$$

Aus dieser Ungleichung folgert man umgekehrt die Ungleichung (11), indem man auf beiden Seiten die ganze Zahl $-(l + n)$ addiert, was ja nach der angenommenen Regel möglich ist. Die Ungleichungen (11) und (12) sind also äquivalent, wenn unsere Annahme stimmt. Da in der Ungleichung (12) nur natürliche Zahlen vorkommen, für die die Kleiner-Gleich-Relation mit der bisher betrachteten übereinstimmen soll, können wir diese Ungleichung zur Definition der genannten Relation auf ganzen Zahlen benutzen, vorausgesetzt, die Wahrheit der Ungleichung (12) hängt nicht von der Wahl von Repräsentanten ab. Wir erinnern daran, dass der Repräsentant einer ganzen

Zahl nur bis auf Differenzgleichheit bestimmt ist, die wir mit \sim abkürzen.

Satz 36 *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 Differenzgleichheit $(k, l) \sim (k', l')$ 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 25 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 Satz 23 und der Kürzungsregel (Satz 26) folgt

$$n + k' \leq m + l'.$$

Aus der ursprünglichen Ungleichung folgt also diejenige mit (k', l') anstelle 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 25 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 32 Wir definieren eine Relation \leq auf der Menge \mathbf{Z} , indem wir für beliebige natürliche Zahlen k, l, m und n setzen

$$[k, l] \leq [m, n], \text{ wenn } k + n \leq l + m.$$

Hier verzichten wir zeitweilig auf die Gleichsetzung der Menge \mathbf{N} der natürlichen Zahlen mit einer Teilmenge der Menge \mathbf{Z} der ganzen Zahlen, so dass \mathbf{N} und \mathbf{Z} disjunkt sind und wir die neue Relation auf \mathbf{Z} mit dem gleichen Symbol \leq bezeichnen können, ohne Verwechslungen befürchten zu müssen.

Satz 37 (i) Die Relation \leq auf der Menge \mathbf{Z} ist eine Ordnung.

(ii) Ist $i : \mathbf{N} \rightarrow \mathbf{Z}$ die Abbildung aus Satz 35, so gilt für beliebige natürliche Zahlen m und n

$$\text{genau dann } i(m) \leq i(n), \text{ wenn } m \leq n.$$

(iii) 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

$$a + i(p) = b.$$

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 Definition 32:

$$\text{Wenn } k + n \leq l + m \quad \text{und} \quad m + l \leq n + k, \quad \text{dann } k + n = l + m.$$

Letzteres gilt wegen der Antisymmetrie der Kleiner-Gleich-Relation auf \mathbf{N} , die sogar für Kardinalzahlen in Satz 16 bewiesen wurde.

Die *Transitivität* besagt, dass für ganze Zahlen a, b und c gilt:

Wenn $a \leq b$ und $b \leq c$, dann $a \leq c$.

Dies bedeutet:

Wenn $k + n \leq l + m$ und $m + s \leq n + r$, dann $k + s \leq l + r$.

Wenden wir Satz 25 auf die ersten beiden Ungleichungen an, so erhalten wir

$$(k + n) + (m + s) \leq (l + m) + (n + r),$$

und mit der Kürzungsregel folgt die dritte Ungleichung. Die behauptete Implikation ist also wahr.

(ii) Mit Hilfe der Definition der Abbildung i wird die Aussage $i(m) \leq i(n)$ zu $[m, 0] \leq [n, 0]$. Nach Definition 32 bedeutet dies $m + 0 \leq 0 + n$, und das ist äquivalent zu $m \leq n$.

(iii) Mit denselben Bezeichnungen wie im Beweis von (i) bedeutet $a \leq b$, dass $k + n \leq l + m$. Wegen $-a = [l, k]$ und $-b = [n, m]$ bedeutet $-b \leq -a$, dass $n + k \leq m + l$. Beide Aussagen sind aufgrund der Kommutativität der Addition äquivalent. Außerdem sind sie nach Satz 24 äquivalent zu der Aussage, dass es eine natürliche Zahl p mit der Eigenschaft

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

gibt. Letzteres ist gleichbedeutend mit $(k + p) + n = l + m$, also nach Definition 32 mit

$$[k + p, l] = [m, n]$$

und nach Definition 31 mit

$$[k, l] + [p, 0] = [m, n]. \quad \square$$

Aufgrund von Aussage (ii) führt es nicht zu Widersprüchen, wenn wir die Menge \mathbf{N} wie am Ende des vorigen Abschnitts mit einer Teilmenge von \mathbf{Z} gleichsetzen, also eine natürliche Zahl n mit der ganzen Zahl $i(n)$ identifizieren. Wir haben dann laut (i) die Kleiner-Gleich-Relation von \mathbf{N} zu einer Ordnung auf dem größeren Zahlbereich \mathbf{Z} fortgesetzt, die wir wieder Kleiner-Gleich-Relation nennen. Teil (iii) besagt u. a., dass genau dann $a \leq b$ gilt, wenn es eine natürliche Zahl³⁶ n gibt, so dass $a + n = b$. Diese Aussage 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.*

³⁶Wir hatten die Variable p gewählt, weil n im Beweis schon besetzt war.

Wenden wir die andere Aussage aus Teil (iii) auf die Zahlen a und 0 an, so erhalten wir:

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 25, 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 vom Ende des vorigen Abschnitts.

Diese Aussage ist äquivalent zu ihrer Kontraposition, nämlich:

Folgerung 14' *Gilt $a \cdot b = 0$ für ganze Zahlen a und b , so ist $a = 0$ oder $b = 0$.*

Hier ist eine weitere Umformulierung:

Folgerung 14'' *Es gibt keine von Null verschiedenen ganzen Zahlen a und b , so dass $a \cdot b = 0$ ist.³⁷*

Wir müssen noch die Rechenregeln für die Kleiner-Gleich-Relation nachprüfen.

Satz 38 (i) *Für beliebige ganze Zahlen a , b , c und d gilt:*

$$\text{Wenn } a \leq b \text{ und } c \leq d, \text{ dann } a + c \leq b + d.$$

(ii) *Für beliebige natürliche Zahlen m und ganze Zahlen c , d gilt:*

$$\text{Wenn } c \leq d, \text{ dann } m \cdot c \leq m \cdot d.$$

³⁷Aus diesem Grunde sagt man traditionell, dass es unter den ganzen Zahlen keine Nullteiler gibt. Nach unserer Definition 29 ist allerdings jede ganze Zahl Teiler der Null.

Beweis. (i) Zusätzlich zu den Bezeichnungen aus dem Beweis des vorigen Satzes 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 25 auf die beiden vorangehenden Ungleichungen anwenden.

Teil (ii) ist Gegenstand von Aufgabe 51. □

4.3 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.³⁸ 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 Teilmengen der Mächtigkeit k in einer Menge der Mächtigkeit n wird laut Aufgabe 24 mit $\binom{n}{k}$ bezeichnet. Die selben Zahlen treten in der binomischen Formel auf.
- 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. 54. Die Aussage lautet dann

$$|M^n| = m^n.$$

In der Schule wird die Potenz natürlicher Zahlen, wie wir schon bemerkt haben, anders definiert, nämlich rekursiv. Dann wird Definition 17 zu einem Satz, den man beweisen muss.

³⁸Wir kommen hier noch einmal darauf zurück, weil wir für den folgenden Satz 39 ganze Zahlen benötigen.

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.

Definition 33 *Wir definieren das Pochhammer-Symbol für alle natürlichen Zahlen m und n rekursiv durch*

$$(m)_0 = 1, \quad (m)_{n+1} = (m)_n \cdot (m - n) \quad \text{für alle } n \in \mathbf{N}.$$

Es gilt

$$(m)_n = \prod_{i=0}^{n-1} (m - i),$$

denn für festes m definieren die beiden Seiten Funktionen von n , die den selben Anfangswert 1 haben und der selben Rekursionsformel genügen. Somit müssen sie nach Satz 17 übereinstimmen. In einer weniger exakten Schreibweise ist

$$(m)_n = \underbrace{m(m-1)(m-2)\dots(m-n+1)}_{n \text{ Faktoren}},$$

also insbesondere

$$(n)_n = n!$$

im Spezialfall $m = n$. Der strenge Beweis der letzten Identität ist etwas umständlich (siehe Aufgabe 54).

Satz 39 *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 $n + 1$. Wegen $n + 1 \neq 0$ ist $N' \neq \emptyset$, also gibt es ein Element $a \in N'$. Wir setzen $N = N' \setminus \{a\}$, 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. Der 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' , also ist die Anzahl injektiver Abbildungen $N' \rightarrow M$ gleich

$$(m)_n \cdot (m - n).$$

Nach der rekursiven Definition ist das gleich $(m)_{n+1}$. Somit gilt die Behauptung auch für die Menge N' .

Man beachte, dass dieses Argument auch funktioniert, wenn es keine injektiven Abbildungen $N \rightarrow M$ gibt³⁹. In diesem Fall ist nach Induktionsvoraussetzung $(m)_n = 0$, und wir erhalten $0 \cdot (m - n)$ Fortsetzungen $N' \rightarrow M$. \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.

³⁹was nach Definition 19 für $n > m$ eintritt

In der klassischen kombinatorischen Terminologie nennt man Abbildungen oder n -Tupel *Variationen mit Wiederholung*, und injektive Abbildungen nennt man *Variationen ohne Wiederholung*.⁴⁰ Der Begriff von Elementen einer Menge war damals nicht geläufig, man sprach von Dingen. Durch Abzählen unserer Liste sehen wir, dass

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 Möglichkeiten, n Elektrogeräte an m Steckdosen anzuschließen, sind die Variationen ohne Wiederholung von m Dingen zur Klasse n .

Die bijektiven Abbildungen einer Menge in sich selbst nennt man *Permutationen*. Da nach Satz 20 jede injektive Abbildung einer endlichen Menge in sich selbst auch surjektiv und somit bijektiv ist, erhalten wir als Spezialfall von Satz 39:

Folgerung 15 *Die Anzahl der Permutationen einer endlichen Menge der Mächtigkeit n ist gleich $n!$.*

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 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, so dass $g = f \circ p$ ist. Als p kann man z. B. die Transposition von 1 und 2 nehmen.

⁴⁰Man beachte, dass bei den Variationen mit Wiederholung die Variationen ohne Wiederholung mitgezählt werden.

Definition 34 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 (Präsenzaufgabe 31).

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 Wiederholung von 7 Dingen ($\square, \blacksquare, \dots, \boxtimes$) zur Klasse 2.

Satz 40 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

$$(m)_n = n! \binom{m}{n}.$$

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. Auf diese Weise erhalten wir 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 insgesamt $n! \binom{m}{n}$ solche Abbildungen. Vergleichen wir dieses Ergebnis mit Satz 39, so erhalten wir die behauptete Gleichung. \square

Mit Hilfe der Aussage (ii) kann man Binomialkoeffizienten berechnen:

Folgerung 16 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 Augen durch Zahlen 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 41 Die Anzahl der Kombinationen mit Wiederholung von m Dingen zur Klasse n ist gleich $\binom{m+n-1}{n}$.

Die Beweismethode von Satz 40 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 Äquivalenzklasse 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

$$(2, 2, 2, 3, 4, 4, 6)$$

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 Folgen von Zeichen 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 (Aufgabe 24) gleich $\binom{(m-1)+n}{n}$. \square

4.4 Gemeinsame Teiler und gemeinsame Vielfache

Die Definition der Teilbarkeit ganze Zahlen unterscheidet sich nicht von der für natürliche Zahlen.

Definition 35 *Es seien a und b natürliche Zahlen. Man nennt b ein Vielfaches von a und nennt a einen Teiler von b , wenn es eine natürliche Zahl c gibt, so dass $b = a \cdot c$. Als Abkürzung schreibt man $a \mid b$.*

Ist außerdem $a \neq 0$, so ist c eindeutig bestimmt und heißt Quotient von b und a , abgekürzt $b : a$.

Falls $a \geq 0$ und $b > 0$, dann muss nach den Vorzeichenregeln auch $c > 0$ sein, und im Fall $b = 0$ können wir $c = 0$ nehmen. Wenn also eine natürliche Zahl im Sinne von Definition 35 Teiler einer natürlichen Zahl ist, so liegt auch Teilbarkeit auch im Sinne von Definition 29 vor, und die Umkehrung ist offensichtlich. Also brauchen wir nicht zwischen beiden Begriffen der Teilbarkeit zu unterscheiden.

Es ist klar, dass für ganze Zahlen a und b gilt genau dann $a \mid b$, wenn $-a \mid b$, und genau dann, wenn $a \mid -b$, und genau dann, wenn $-a \mid -b$. Darum kann man sich oft auf natürliche Zahlen beschränken.

Lemma 2 *Es seien a, b, c, x und y ganze Zahlen.*

(i) *Es gilt genau dann $ac \mid bc$, wenn $a \mid b$.*

(ii) *Wenn $c \mid a$ und $c \mid b$, dann $c \mid ax + by$.*

Beweis. (i) Ist $a \mid b$, so gibt es eine ganze Zahl x , so dass $ax = b$, und es folgt $bc = (ax)c = (ac)x$, also $ac \mid bc$. Die Umkehrung ist Gegenstand von Aufgabe 56.

(ii) Die Voraussetzungen $c \mid a$ und $c \mid b$ bedeuten, dass es ganze Zahlen u und v gibt, so dass $a = cu$ und $b = cv$, so dass nach Kommutativ- und Distributivgesetz folgt

$$ax + by = (cu)x + (cv)y = c(ux) + c(vy) = c(ux + vy).$$

□

Da ein Teiler einer von Null verschiedenen natürlichen Zahl nach Satz 25 nicht größer sein kann als die Zahl selbst, hat jede von Null verschiedene ganze Zahl nur endlich viele Teiler. Man kann sie finden, indem man alle kleineren Zahlen durchprobiert. So hat z. B. 12 die Teiler 1, 2, 3, 4, 6 und 12, und die Zahl 20 hat die Teiler 1, 2, 4, 5, 10, 20. Die gemeinsamen Teiler von 12 und 20 sind 1, 2 und 4. Haben zwei Zahlen den einzigen (positiven) gemeinsamen Teiler 1, so heißen sie *teilerfremd*.

Sind zwei ganze Zahlen a und b gegeben, die nicht beide gleich Null sind, so ist die Menge ihrer gemeinsamen Teiler endlich, also gibt es unter diesen nach Aufgabe 28 einen *größten gemeinsamen Teiler*, abgekürzt $\text{ggT}(a, b)$. Wie findet man ihn möglichst effektiv?

Offensichtlich ist $\text{ggT}(a, 0) = a$. Wir brauchen also nur den Fall $a \geq b > 0$ zu behandeln. Aus Lemma 2(ii) wissen wir, dass jeder gemeinsame Teiler von a und b auch ein Teiler der natürlichen Zahl $c = a - b$ ist. Ebenso ist jeder gemeinsame Teiler von b und c auch ein Teiler von $b + c = a$. Es folgt, dass jeder gemeinsame Teiler von a und b ein gemeinsamer Teiler von b und c ist und umgekehrt, also $\text{ggT}(a, b) = \text{ggT}(b, c)$. Wir haben das Problem auf ein leichteres zurückgeführt, denn die größere der Zahlen b und c ist kleiner als die größere der Zahlen a und b . Wenn wir so fortfahren, kommen wir irgendwann zu einem Paar, bei dem eine der beiden Zahlen gleich Null ist, und dann sind wir fertig. Die eben beschriebene Methode heißt *Euklidischer Algorithmus*.

Beispiel. Wir wollen den größten gemeinsamen Teiler von 247 und 91 finden.

$$\begin{aligned} \text{ggT}(247, 91) &= \text{ggT}(156, 91) = \text{ggT}(65, 91) = \text{ggT}(65, 26) \\ &= \text{ggT}(39, 26) = \text{ggT}(13, 26) = \text{ggT}(13, 13) = \text{ggT}(13, 0) = 13. \end{aligned}$$

Zur Beschleunigung subtrahieren wir in einem Schritt die kleinere von der größeren Zahl so oft wie möglich, d. h. wir teilen mit Rest:

$$\begin{aligned} 247 &= 2 \cdot 91 + 65 \\ 91 &= 1 \cdot 65 + 26 \\ 65 &= 2 \cdot 26 + 13 \\ 26 &= 2 \cdot \underline{13} \end{aligned}$$

Haben wir $d = \text{ggT}(a, b)$ mit dem Euklidischen Algorithmus berechnet, so können wir eine ganzzahlige Lösung der Gleichung

$$ax + by = d$$

finden, indem wir die Gleichungen nach den Resten auflösen und von unten beginnend die Zwischenergebnisse eliminieren. In unserem Beispiel:

$$\begin{aligned} 13 &= 65 - 2 \cdot 26 = 65 - 2(91 - 65) \\ &= 3 \cdot 65 - 2 \cdot 91 = 3(247 - 2 \cdot 91) - 2 \cdot 91 \\ &= 3 \cdot 247 - 8 \cdot 91 \end{aligned}$$

Die Gleichung $247x + 91y = 13$ hat also u. a. die Lösung $x = 3, y = -8$.

Beispiel. Finde $\text{ggT}(111, 77)$.

$$\begin{aligned}111 &= 1 \cdot 77 + 34 \\77 &= 2 \cdot 34 + 9 \\34 &= 3 \cdot 9 + 7 \\9 &= 1 \cdot 7 + 2 \\7 &= 2 \cdot 3 + 1 \\3 &= 3 \cdot 1\end{aligned}$$

Es folgt $\text{ggT}(111, 77) = 1$, d. h. 111 und 77 sind teilerfremd.

$$\begin{aligned}1 &= 7 - 3 \cdot 2 = 7 - 3 \cdot (9 - 7) \\&= 4 \cdot 7 - 3 \cdot 9 = 4 \cdot (34 - 3 \cdot 9) - 3 \cdot 9 \\&= 4 \cdot 34 - 15 \cdot 9 = 4 \cdot 34 - 15(77 - 2 \cdot 34) \\&= 34 \cdot 34 - 15 \cdot 77 = 34 \cdot (111 - 77) - 15 \cdot 77 \\&= 34 \cdot 111 - 49 \cdot 77\end{aligned}$$

Die Gleichung $111x + 77y = 1$ hat also u. a. die Lösung $x = 34, y = -49$.

Satz 42 *Ist d der größte gemeinsame Teiler der natürlichen Zahlen a und b , die nicht beide gleich Null sind, so gibt es ganze Zahlen x und y , so dass*

$$d = ax + by.$$

Jeder gemeinsame Teiler von a und b ist ein Teiler von d .

Beweis. Die Zahlen x und y ergeben sich aus dem Euklidischen Algorithmus. Strenggenommen muss man ihre Existenz beweisen, z. B. durch vollständige Induktion nach der größeren der beiden Zahlen:

Ist die kleinere, sagen wir b , gleich Null, so ist die Behauptung offensichtlich wahr, denn wir können $x = 1$ und $y = 0$ setzen. Nun seien natürliche Zahlen a und b gegeben, deren kleinere nicht Null ist. Angenommen, die Behauptung gilt für alle Paare, deren größeres Element kleiner ist als das größere von a und b . Wenn wir annehmen, dass a das größere ist, so gilt die Behauptung insbesondere für b und $c = a - b$. Da b und c nach Lemma 2(ii) ebenfalls den größten gemeinsamen Teiler d haben, gibt es ganze Zahlen u und v , so dass

$$d = bu + cv.$$

Es folgt

$$d = bu + (a - b)v = av + b(u - v),$$

also können wir $x = v$ und $y = u - v$ setzen. Damit ist der Induktionsschritt abgeschlossen.

Ist e ein gemeinsamer Teiler von a und b , so folgt aus dem Bewiesenen mittels Lemma 2(iii), dass $e \mid d$. \square

Folgerung 17 *Ganze Zahlen a und b sind genau dann teilerfremd, wenn es ganze Zahlen x und y gibt, so dass $ax + by = 1$.*

In der Tat, sind a und b teilerfremd, so ist $\text{ggT}(a, b) = 1$, und nach Satz 42 existieren die behaupteten Zahlen x und y . Umgekehrt gelte $ax + by = 1$ für ganze Zahlen x und y . Ist nun $e \in \mathbf{N}$ ein gemeinsamer Teiler von a und b , so ist nach Lemma 2(ii) e auch Teiler von $ax + by$, also von 1. Daraus folgt $e = 1$.

Man sollte den Euklidischen Algorithmus nicht mit dem Algorithmus zur Bestimmung der g -adischen Ziffern einer Zahl verwechseln. Bei letzterem wird der abgerundete Quotient des vorigen Schrittes immer durch die selbe Grundzahl g geteilt, beim Euklidischen Algorithmus hingegen wird der abgerundete Quotient des vorigen Schrittes durch den Rest des vorigen Schrittes geteilt.

Satz 43 *Es seien a, b und c ganze Zahlen, wobei a und b nicht beide gleich Null sind.*

(i) *Für jedes $n \in \mathbf{N}$ gilt $\text{ggT}(na, nb) = n \cdot \text{ggT}(a, b)$.*

(ii) *Sind a und b teilerfremd und gilt $a \mid bc$, so gilt $a \mid c$.*

(iii) *Sind a und b teilerfremd und gilt $a \mid c$ und $b \mid c$, so gilt $ab \mid c$.*

Beweis. (i) Es sei $d = \text{ggT}(a, b)$ und $e = \text{ggT}(na, nb)$. Nach Lemma 2(i) ist nd ein gemeinsamer Teiler von na und nb , und nach der letzten Aussage von Satz 42 ist $nd \mid e$.

Andererseits ist n ein gemeinsamer Teiler von na und nb , nach Satz 42 also $n \mid e$, so dass es eine natürliche Zahl k mit der Eigenschaft $e = nk$ gibt. Aus $e \mid na$ und $e \mid nb$ folgt nun mit Lemma 2(i), dass $k \mid a$ und $k \mid b$, und nach Satz 42 folgt $k \mid d$. Wiederum mit Lemma 2(i) ergibt sich $nk \mid nd$.

Wir haben also gezeigt, dass $nd \mid e$ und $e \mid nd$, so dass $e = nd$.

(ii) Nach Folgerung 17 gibt es $x, y \in \mathbf{Z}$, so dass $ax + by = 1$. Multiplizieren wir beide Seiten mit c , so erhalten wir

$$c = a(cx) + (bc)y.$$

Wegen $a \mid bc$ folgt aus Satz 1(iii), dass $a \mid c$.

(iii) Nach Voraussetzung gibt es $d, e \in \mathbf{Z}$, so dass $c = ad = be$. Multiplizieren wir wieder die Gleichung $ax + by = 1$ mit c , so erhalten wir

$$c = acx + bcy = a(be)x + b(ad)y = ab(ex + dy).$$

Daraus folgt $ab \mid c$. □

Aussage (ii) des Satzes benötigt man zum Beweis, dass die Primfaktorzerlegung einer natürlichen Zahl eindeutig bestimmt ist. Darauf werden wir hier allerdings nicht eingehen.

Sind a und b positive natürliche Zahlen, so gibt es positive gemeinsame Vielfache (z. B. ab), und unter diesen gibt es nach Folgerung 7 ein *kleinstes gemeinsames Vielfaches*, abgekürzt $\text{kgV}(a, b)$.

Satz 44 *Ist d der größte gemeinsame Teiler und m das kleinste gemeinsame Vielfache der natürlichen Zahlen a und b , die nicht beide gleich Null sind, so gilt*

$$ab = dm.$$

Jedes gemeinsame Vielfache von a und b ist ein Vielfaches von m .

Beweis. Wegen $d \mid a$, $d \mid b$ und $d \mid ab$ gibt es natürliche Zahlen u, v und w , so dass

$$a = du, \quad b = dv, \quad ab = dw.$$

Nach Satz 43(i) ist

$$d = \text{ggT}(a, b) = d \text{ggT}(u, v),$$

also ist nach der Kürzungsregel (Satz 26) $\text{ggT}(u, v) = 1$, d. h. u und v sind teilerfremd. Außerdem gilt $dw = adv = dub$, also

$$w = av = bu,$$

d. h. w ist ein gemeinsames Vielfaches von a und b .

Nun sei c ein beliebiges gemeinsames Vielfaches von a und b , das heißt $a \mid c$ und $b \mid c$ und folglich auch $d \mid c$. Das bedeutet, dass es natürliche Zahlen x, y und z gibt, so dass

$$c = ax, \quad c = by, \quad c = dz.$$

Es folgt $dz = dux = dvy$, also nach der Kürzungsregel

$$z = ux = vy,$$

d. h. $u \mid z$ und $v \mid z$. Da u und v teilerfremd sind, folgt nach Satz 43(iii), dass $uv \mid z$, also $duv \mid dz$. Wir haben bewiesen, dass $w \mid c$, und nach Satz 25 folgt $w \leq c$.

Laut Definition ist das kleinste gemeinsame Vielfache m von a und b also gleich w , und alle Behauptungen sind bewiesen. \square

Man kann den Beweis auch mit Hilfe der Primfaktorzerlegung führen, wozu man aber ihre Eindeutigkeit beweisen muss.

Der Satz gibt uns eine effektive Methode zur Berechnung des kleinsten gemeinsamen Vielfachen:

Folgerung 18 *Sind die natürlichen Zahlen a und b nicht beide gleich Null, so ist*

$$\text{kgV}(a, b) = (a \cdot b) : \text{ggT}(a, b).$$

(Eigentlich ist die Klammersetzung hier egal.)

5 Rationale Zahlen

5.1 Motivation und Definition

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 zu einem Bereich \mathbf{Q} vornehmen, um auch die Division uneingeschränkt ausführbar zu machen. Dabei soll die Subtraktion uneingeschränkt ausführbar bleiben, und die gewohnten Rechengesetze sollen auch für beliebige Zahlen r , s und t in \mathbf{Q} gelten, nämlich die Kommutativ-, Assoziativ- und Distributivgesetze

$$\begin{aligned} r + s &= s + r, & r \cdot s &= s \cdot r, \\ (r + s) + t &= r + (s + t), & (r \cdot s) \cdot t &= r \cdot (s \cdot t), \\ r \cdot (s + t) &= r \cdot s + r \cdot t. \end{aligned} \tag{13}$$

Mit der uneingeschränkten Ausführbarkeit der Division meint man, dass es für beliebige Zahlen r und $s \neq 0$ in \mathbf{Q} genau eine Zahl $t \in \mathbf{Q}$ geben soll, so dass $r = s \cdot t$ gilt. Diese Zahl t nennt man dann den Quotienten von r und s , abgekürzt $r : s$. Für $s = 0$ kann man die Existenz von t nicht verlangen, denn für jedes $t \in \mathbf{Q}$ wird wegen

$$0 \cdot t = (0 + 0) \cdot t = 0 \cdot t + 0 \cdot t$$

gelten $0 \cdot t = 0$. Man bekäme also im Falle $r \neq 0$ keine Lösung, während im Fall $r = 0$ jedes t eine Lösung wäre. Direkt aus der Definition folgt

$$r : 1 = r, \quad r : r = 1.$$

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:

$$\begin{aligned} (r \cdot s) : t &= r \cdot (s : t), & (r : s) : t &= r : (s \cdot t), & (r : s) \cdot t &= r : (s : t), \\ (r + s) : t &= r : t + s : t, & (r - s) : t &= r : t - s : t, \\ r : (-s) &= -r : s, & (-r) : s &= -r : s, & (-r) : (-s) &= r : s. \end{aligned} \tag{14}$$

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 (4) 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.

Wir wissen noch nicht, ob es eine Menge \mathbf{Q} mit Operationen $+$ und \cdot gibt, die den eingangs genannten Wünschen entspricht. Wir nehmen das zunächst einmal an und folgern weitere Eigenschaften, die uns auf eine Idee für die Konstruktion bringen sollen.

Jede Teilmenge von \mathbf{Q} , die \mathbf{Z} enthält und abgeschlossen unter Addition, Multiplikation, Subtraktion und Division ist, erfüllt bereits alle Anforderungen. Jede solche Teilmenge muss alle Quotienten $a : b$ von ganzen Zahlen a und $b \neq 0$ enthalten. Die Menge aller solcher Differenzen ist aber schon abgeschlossen unter den vier Rechenoperationen, denn aus den Rechengesetzen folgt

$$\begin{aligned} (a : b) \cdot (c : d) &= (a \cdot c) : (b \cdot d), \\ (a : b) : (c : d) &= (a \cdot d) : (b \cdot c). \end{aligned} \tag{15}$$

Der Beweis ist wieder eine Kopie der analogen Regeln (7) für Differenzen ganzer Zahlen, wobei man $+$ durch \cdot und $-$ durch $:$ ersetzt. Als Spezialfall dieser Regeln erhalten wir

$$\begin{aligned} a : b &= (a : b) \cdot 1 = (a : b) \cdot (d : d) = (a \cdot d) : (b \cdot d), \\ c : d &= 1 \cdot (c : d) = (b : b) \cdot (c : d) = (b \cdot c) : (b \cdot d). \end{aligned}$$

Die Regeln für die Addition und Subtraktion

$$\begin{aligned} (a : b) + (c : d) &= (a \cdot d + b \cdot c) : (b \cdot d), \\ (a : b) - (c : d) &= (a \cdot d - b \cdot c) : (b \cdot d) \end{aligned} \tag{16}$$

folgen nun mit Hilfe der Distributivgesetze, z. B.

$$(a : b) + (c : d) = (a \cdot d) : (b \cdot d) + (b \cdot c) : (b \cdot d) = (a \cdot d + b \cdot c) : (b \cdot d).$$

Ähnlich beweist man die Regel für die Subtraktion.

Damit haben wir gezeigt, dass die Menge der Quotienten ganzer Zahlen abgeschlossen unter allen vier Rechenoperationen ist, also die Rolle von \mathbf{Q} spielen kann. Wir können somit annehmen, dass jedes Element der Menge \mathbf{Q} ein Quotient ganzer Zahlen ist.⁴¹ In diesem Fall ist die durch

$$q(a, b) = a : b$$

gegebene Abbildung $q : \mathbf{Z} \times (\mathbf{Z} \setminus \{0\}) \rightarrow \mathbf{Q}$ 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 der Definition der Division und den Rechengesetzen folgt

$$a = b \cdot (c : d) = (b \cdot c) : d,$$

also

$$a \cdot d = b \cdot c. \tag{17}$$

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. $q(1, 1) = q(2, 2)$. Für jedes Element r von \mathbf{Q} haben wir die Menge

$$\{(a, b) \in \mathbf{Z} \times (\mathbf{Z} \setminus \{0\}) \mid q(a, b) = r\}, \tag{18}$$

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 (18).

Wir erinnern daran, dass die Existenz der erhofften Menge \mathbf{Q} noch nicht bewiesen ist. Glücklicherweise können wir die Relation \approx mittels (17) und die Rechenoperationen mittels (15) und (16) beschreiben, ohne die gesuchte Menge \mathbf{Q} zu benutzen.

Definition 36 *Wir definieren die Relation der Quotientengleichheit, abgekürzt \approx , auf der Menge $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ wie folgt:*

⁴¹Daher die Wahl des Buchstabens \mathbf{Q} .

$(a, b) \approx (c, d)$ 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 45 (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. Der Beweis von Aussage (i) erhalten wir aus dem Beweis der analogen Aussage von Satz 34, 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 (3)

$$(a \cdot f) \cdot (c \cdot d) = (b \cdot e) \cdot (c \cdot d).$$

Wir haben zwar keine Kürzungsregel formuliert, aber man kann die erhaltene Aussage umformen in

$$(a \cdot f - b \cdot e) \cdot c \cdot d = 0.$$

Da d nach Voraussetzung nicht Null ist, gilt mit Folgerung 14', dass

$$a \cdot f - b \cdot e = 0 \quad \text{oder} \quad c = 0.$$

Im ersten Fall sind wir fertig. Im zweiten Fall erhalten wir mit der selben Folgerung, 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 34(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 (3). \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 37 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. Nun können wir auch die Rechengesetze beweisen.

Satz 46 (i) Für beliebige rationale Zahlen r , s und t gelten die Rechengesetze (13).

(ii) Die Subtraktion von rationalen Zahlen ist uneingeschränkt ausführbar.

(iii) Die Division von rationalen Zahlen ist uneingeschränkt (mit Ausnahme der Division durch $\frac{0}{1}$) 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

$$r \cdot (s + t) = \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f} \right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{a(cf + de)}{b(df)}$$

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 35, indem man $+$ durch \cdot ersetzt. Das Kommutativgesetz der Addition ist offensichtlich, und der Beweis des Assoziativgesetzes ist Gegenstand von Aufgabe 61.

(ii) Für gegebene rationale Zahlen $r = \frac{a}{b}$ und $s = \frac{c}{d}$ suchen wir nach t , so dass $r = s + t$. Laut (15) kommt nur $t = \frac{ad-bc}{bd}$ in Frage, und die umgekehrte Ausführung der beim Beweis dieser Gleichung vorgenommenen Umformungen liefert die Bestätigung.

(iii) Für gegebene rationale Zahlen $r = \frac{a}{b}$ und $s = \frac{c}{d}$ suchen wir nach t , so dass $r = s \cdot t$. Laut (15) kommt nur $t = \frac{ad}{bc}$ in Frage. Ist $c = 0$, so ist $(c, d) \approx (0, 1)$, also $s = \frac{0}{1}$. Andernfalls ist $(ad, bc) \in \mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$, also ist die Formel für t korrekt, und die umgekehrte Ausführung der beim Beweis von (15) vorgenommenen Umformungen liefert die Bestätigung.

(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 $a = b$. Damit ist j injektiv. \square

Aussage (i) rechtfertigt die eingangs gezogenen Schlüsse, bei denen wir die Existenz der rationalen Zahlen und die Gültigkeit der Rechengesetze zunächst angenommen hatten.

Folgerung 19 *Für alle rationalen Zahlen gelten die Rechengesetze der Subtraktion (vgl. (4)) und der Division (14). Außerdem gelten die Regeln (15) und (16) für rationale Zahlen an Stelle von ganzen Zahlen.*

Die damaligen Beweise sind unverändert in dem allgemeineren Fall richtig.

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 der Aussage (iv) 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} . In diesem Sinne bezeichnen $a : b$ und $\frac{a}{b}$ dann die selbe rationale Zahl.⁴²

⁴²Dies hat dazu geführt, dass der Bruchstrich allgemein als Ersatz für das Divisionszeichen verwendet wird, und zwar nicht nur für ganze Zahlen. So schreibt man z. B. für $\frac{a}{b} : \frac{c}{d}$ auch den Doppelbruch $\frac{\frac{a}{b}}{\frac{c}{d}}$.

Wir können die Regeln (15) und (16) für die Subtraktion und die Division auch so umschreiben:

$$\frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d},$$

$$\frac{a}{b} : \frac{c}{d} = \frac{a \cdot d}{b \cdot c}.$$

Vergleicht man dies mit der Definition der Multiplikation, so erhält man die Regel, dass man durch eine von Null verschiedene rationale Zahl $s = \frac{c}{d}$ dividieren kann, indem man mit ihrem *Kehrwert*⁴³ $1 : s = \frac{d}{c}$ multipliziert.

Traditionell spricht man von äquivalenten Brüchen, die die selbe Zahl darstellen. In Rechenausdrücken benutzt man das Symbol des Bruches aber als Bezeichnung der Zahl, was z. B. in Gleichungen wie $\frac{1}{2} = \frac{2}{4}$ deutlich wird. Für eine korrekte Darlegung braucht man ein weiteres Symbol, um einen Bruch im Unterschied von der durch ihn dargestellten Zahl zu bezeichnen. 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 .

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, 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 dieser ist eindeutig bestimmt.

Haben die Nenner zweier Brüche (a, b) und (c, d) einen gemeinsamen Teiler e , so findet man einen Vertreter für die Summe mit einem kleineren Nenner als bd . Es gibt dann nämlich ganze Zahlen x und y , so dass $b = ex$ und $d = ey$, und nach dem Distributivgesetz der Division gilt

$$\frac{a}{b} + \frac{c}{d} = \frac{ay}{by} + \frac{cx}{dx} = \frac{ay + cx}{exy}.$$

Der *Hauptnenner* $by = dx = exy$ ist dann ein gemeinsames Vielfaches der Nenner b und d . Insbesondere kann man für e den größten gemeinsamen Teiler nehmen, dann ist der Hauptnenner nach Satz 44 das kleinste gemeinsame Vielfache von b und d .

5.2 Vergleich von rationalen Zahlen

Wir wollen die für ganze Zahlen definierte Kleiner-Gleich-Relation so zu einer Ordnungsrelation auf der Menge der rationalen Zahlen fortsetzen, dass die

⁴³lat.: ihrem *Reziproken*

Rechenregeln aus Satz 38 auch für rationale Zahlen r, s, t und u gelten, nämlich:

Wenn $r \leq t$ und $t \leq u$, dann $r + t \leq s + u$,
wenn $r \leq t$ und $u \geq 0$, dann $r \cdot u \leq s \cdot u$.

Wenn das möglich sein sollte, dann müsste u. a. der Kehrwert einer positiven Zahl u positiv sein, denn sonst würde aus der zweiten Regel mit $r = 1 : u$ und $t = 0$ folgen, dass $1 \leq 0$. Außerdem müsste auch folgendes gelten:

Lemma 3 Für alle ganzen Zahlen a, b und c gilt:

Wenn $a \cdot c \leq b \cdot c$ und $c > 0$, dann $a \leq b$.

Wir könnten zum Beweis nämlich beide Seiten mit $\frac{1}{c}$ multiplizieren. Aber auch ohne unbewiesene Annahmen ist der Beweis möglich.

Beweis. Es gibt zwei Fälle. Ist $a \cdot c = b \cdot c$, so gilt

$$(a - b) \cdot c = 0,$$

und wegen $c \neq 0$ erhalten wir mit Folgerung 14', dass $a - b = 0$, also $a = b$. Ist hingegen $a \cdot c < b \cdot c$, so behaupten wir, dass sogar $a < b$ folgt. Wäre nämlich $a \geq b$, so würde mit Satz 38(ii) folgen, dass $a \cdot c \geq b \cdot c$ entgegen unserer Voraussetzung. \square

Dieses Lemma ist eine Kürzungsregel für Ungleichungen. Im Beweis haben wir nebenbei eine Kürzungsregel für Gleichungen bewiesen, die wir schon viel früher (nach Folgerung 14') hätten formulieren sollen:

Folgerung 20 Für alle ganzen Zahlen a, b und c gilt:

Wenn $a \cdot c = b \cdot c$ und $c \neq 0$, dann $a = b$.

Nun kommen wir auf unser Thema zurück. Nehmen wir wieder an, es wäre möglich, die Relation \leq wie gewünscht auf \mathbf{Q} fortzusetzen. Da sich rationale Zahlen als Quotienten ganzer Zahlen darstellen lassen, geht es um Aussagen der Form

$$a : b \leq c : d \tag{19}$$

wobei a, b, c und d ganze Zahlen sind und wir annehmen können, dass b und d positiv sind. Aus dieser Aussage folgt nach der zweiten Regel, wenn wir für u die Zahl $b \cdot d$ wählen, dass

$$(a : b) \cdot (b \cdot d) \leq (c : d) \cdot (b \cdot d).$$

Unter Benutzung der Rechengesetze können wir beide Seiten vereinfachen und erhalten

$$a \cdot d \leq b \cdot c. \quad (20)$$

Aus dieser Ungleichung folgert man umgekehrt die Ungleichung (19), indem man beide Seiten mit der positiven Zahl $\frac{1}{b \cdot d}$ multipliziert, was ja nach der angenommenen Regel möglich ist. Die Ungleichungen (19) und (20) sind also äquivalent, wenn unsere Annahme stimmt. Da in der Ungleichung (20) 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 der Ungleichung (20) hängt nicht von der Wahl der Repräsentanten ab.

Satz 47 *Es seien a, b, c, d, a', b', c' und d' ganze Zahlen, wobei $b > 0, b' > 0, d > 0$ und $d' > 0$. Ist $(a, b) \approx (a', b')$ und $(c, d) \approx (c', d')$, so gilt*

$$\textit{genau dann } a \cdot d \leq b \cdot c, \textit{ wenn } a' \cdot d' \leq b' \cdot c'.$$

Beweis. 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 38(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 3 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 38 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:

$$\frac{a}{b} \leq \frac{c}{d}, \text{ wenn } a \cdot d \leq b \cdot c.$$

Eine rationale Zahl r heißt positiv, wenn $r > 0$ ist, und negativ, wenn $r < 0$ ist.

Hier verzichten wir zeitweilig auf die Gleichsetzung der Menge \mathbf{Z} der natürlichen Zahlen mit einer Teilmenge der Menge \mathbf{Q} der ganzen Zahlen, so dass \mathbf{Z} und \mathbf{Q} disjunkt sind und wir die neue Relation auf \mathbf{Q} mit dem gleichen Symbol \leq bezeichnen können, ohne Verwechslungen befürchten zu müssen.

Satz 48 (i) Die Relation \leq auf der Menge \mathbf{Q} ist eine Ordnung.

(ii) Ist $j : \mathbf{Z} \rightarrow \mathbf{Q}$ die Abbildung aus Satz 46, so gilt für beliebige ganze Zahlen a und b

$$\text{genau dann } j(a) \leq j(b), \text{ wenn } a \leq b.$$

(iii) Für rationale Zahlen r und s gilt genau dann $r \leq s$, wenn $-s \leq -r$.

(iv) Für positive rationale Zahlen r und s gilt genau dann $r \leq s$, wenn $1 : s \leq 1 : r$.

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 37) und der Kommutivität.

Die *Antisymmetrie* besagt, dass für alle rationalen Zahlen r und s gilt:

$$\text{Wenn } r \leq s \text{ und } s \leq r, \text{ dann } r = s.$$

Dies bedeutet laut Definition 38:

$$\text{Wenn } a \cdot d \leq b \cdot c \quad \text{und} \quad c \cdot b \leq d \cdot a, \quad \text{dann } a \cdot d = b \cdot c.$$

Letzteres gilt wegen der Antisymmetrie der Kleiner-Gleich-Relation auf \mathbf{Z} (Satz 37) 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 38(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 3 folgt wegen $d > 0$ die dritte Ungleichung. Die behauptete Implikation ist also wahr.

(ii) 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 38 bedeutet dies $a \cdot 1 \leq 1 \cdot b$, und das ist äquivalent zu $a \leq b$.

(iii) Mit denselben Bezeichnungen wie im Beweis von (i) bedeutet $r \leq s$, dass $a \cdot d \leq b \cdot d$. Wegen $-r = \frac{-a}{b}$ und $-s = \frac{-c}{d}$ bedeutet $-s \leq -r$, dass $(-c) \cdot b \leq d \cdot (-a)$, also nach den Vorzeichenregeln und Kommutativität $-b \cdot c \leq -a \cdot d$. nun folgt die Behauptung aus Satz 37(iii).

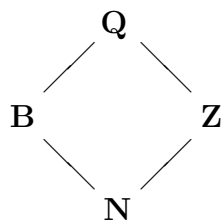
(iv) Wegen $1 : r = \frac{b}{a}$ und $1 : s = \frac{d}{c}$ gilt $1 : s \leq 1 : r$ genau dann, wenn $d \cdot a \leq c \cdot b$, und das ist nach Kommutativität äquivalent zu $r \leq s$. \square

Aufgrund von Aussage (ii) führt es nicht zu Widersprüchen, wenn wir die Menge \mathbf{Z} wie am Ende des vorigen Abschnitts mit einer Teilmenge von \mathbf{Q} gleichsetzen, also eine ganze Zahl a mit der rationalen Zahl $j(a) = \frac{a}{1}$ identifizieren. Wir haben dann laut (i) die Kleiner-Gleich-Relation von \mathbf{N} zu einer Ordnung auf dem größeren Zahlbereich \mathbf{Z} fortgesetzt, die wir wieder Kleiner-Gleich-Relation nennen.

Eine rationale Zahl ist genau dann nichtnegativ, wenn sie sich in der Form $\frac{a}{b}$ mit natürlichen Zahlen a und $b \neq 0$ schreiben lässt. Solche Zahlen nennt man *Bruchzahlen*. Für viele Autoren ist die Null keine natürliche Zahl und auch keine Bruchzahl. Brüche, in denen der Zähler kleiner als der Nenner ist, nennt man *echte Brüche*. Sie stellen die 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 unbeschränkt 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. Manche Schulbuchautoren benutzen für die Menge der Bruchzahlen das Symbol **B**, das in der mathematischen Fachliteratur allerdings nicht vorkommt.



Index

- f -Abschluss, 30
- f -abgeschlossen, 30
- Äquivalenz, 3
- Äquivalenzrelation, 72
- Übertrag, 67

- Abbildung, 13
- Abbildung auf, 14
- abgerundeter Quotient, 49
- Addition, 22
- Alternative, 6
- antisymmetrisch, 33
- Antivalenz, 6
- assoziativ, 5, 10, 23, 24
- Aussage, 1
- Aussageform, 7
- Axiom, 29

- bündeln, 56
- bijektiv, 15
- Binom, 62
- Binomialkoeffizient, 62
- binomische Formel, 62
- Bisubjunktion, 3
- Bruch, 102
- Bruchzahl, 106

- Cartesisches Produkt, 11

- das Kleinste, 31, 42
- Definitionsbereich, 13
- Differenz, 46
- differenzgleich, 72
- disjunkt, 21
- Disjunktion, 2
- distributiv, 5, 10, 24
- Division, 48
- Division mit Rest, 49
- Durchschnitt, 9

- echte Teilmenge, 30
- Eigenschaft, 9
- eindeutig, 14
- Element, 7
- elementfremd, 21
- endliche Menge, 35
- entgegengesetzte Zahl, 76
- entweder ... oder, 6
- erweitern, 102
- Euklidischer Algorithmus, 90

- Fakultät, 51
- Funktion, 13

- ganze Zahl, 74
- genau dann, wenn, 4
- genau ein, 13
- geordnetes Paar, 11
- ggT, 90
- gleichmächtig, 18
- größter gemeinsamer Teiler, 90
- Graph, 14
- Grundbegriff, 7
- Grundzahl, 57

- Halbordnung, 45
- Hauptnenner, 102

- identische Abbildung, 15
- Implikation, 3
- Index, 53
- Induktionsanfang, 37
- Induktionsbehauptung, 37
- Induktionsschritt, 37
- Induktionsvoraussetzung, 37
- injektiv, 14
- isomorph, 77

- kürzen, 102

Kardinalzahl, 20
 Kehrwert, 102
 kgV, 93
 Klasse, 19
 kleiner, 29, 33
 kleinstes gemeinsames Vielfaches, 93
 Kombinationen, 86
 kommutativ, 5, 10, 23, 24
 Konjunktion, 2
 Kreuzprodukt, 11
 Kürzungsregel, 47

 Lemma, 31
 lexikographische Ordnung, 45
 logisches Gesetz, 4

 Mächtigkeit, 20
 Mächtigkeitsklasse, 19
 Menge, 7
 Mengenoperationen, 10
 Multiplikation, 24

 n -Tupel, 53
 Nachfolger, 34
 Nachfolgerabbildung, 34
 natürliche Zahl, 35
 Negation, 1
 Nenner, 102
 Null, 57

 oder, 2
 Ordinalzahl, 46
 Ordnung, 44

 Permutationen, 85
 Pochhammer-Symbol, 83
 Potenz von Kardinalzahlen, 26
 Potenzgesetze, 26, 52
 Prädikat, 7
 Produkt von Kardinalzahlen, 24
 Produktzeichen, 54

 quod erat demonstrandum, 9
 Quotient, 46
 quotientengleich, 97

 rationale Zahl, 99
 reflexiv, 18, 45
 Rekursionsatz, 35
 rekursiv, 52
 Relation, 32
 Rest, 49
 reziprok, 102

 Schnittmenge, 9
 schriftliche Rechenverfahren, 66
 Stellenwertsystem, 57
 Subjunktion, 3
 Substitutionsregel, 55
 Subtraktion, 48
 Summationsgrenze, 54
 Summe von Kardinalzahlen, 22
 Summenzeichen, 54
 surjektiv, 14
 symmetrisch, 18

 teilbar, 48
 Teiler, 48
 teilerfremd, 89
 Teilmenge, 8
 total, 33
 transitiv, 18, 33
 Transposition, 39
 Tripel, 53

 Umkehrabbildung, 15
 umkehrbar eindeutig, 15
 und, 2
 unkürzbar, 102

 Variationen, 85
 Vereinigung, 9
 Vereinigungsmenge, 9
 Verkettung, 15

verknüpfen, 2
Vielfaches, 48
vollständige Induktion, 37, 59
Vorzeichen, 76

Wahrheitstafel, 1
Wahrheitswert, 1
wenn ... dann, 3
Wertebereich, 15
Wertevorrat, 15
Wohlordnung, 44

Zähler, 102
Zielbereich, 13
Ziffer, 58
Zuordnung, 12