Einführung in das mathematische Arbeiten

Skriptum zur Vorlesung

Institut für Mathematik
Universität Wien

Hermann Schichl

Überarbeitet für die Vorlesung im Wintersemester 2003/04
von Roland Steinbauer

Inhaltsverzeichnis

KAPITEL 1

Einleitung

Im Vergleich mit vielen anderen Studien, selbst mit den anderen naturwissenschaftlichen, hat das Mathematikstudium eine höhere Drop-Out–Rate, und viele Studenten geben bereits im ersten Studienabschnitt auf.

Ein Hauptgrund für dieses Faktum liegt darin, dass sich die Art wie Mathematik an der Universität betrieben wird, grundlegend unterscheidet von dem, was man aus der Schule gewohnt ist. Während in der Schule das Hauptaugenmerk auf das Lösen von Beispielen gerichtet ist und für die meisten Lehrer das Algorithmische im Vordergrund steht (das Erlernen von Schemata zur Behandlung von Standardproblemen), tritt dies an der Universität merklich in den Hintergrund. Es ist in Wahrheit so, dass selbst die besten Fähigkeiten in diesem Gebiet nicht ausreichen, ein Mathematikstudium, sei es zum Lehramt oder zum Diplom, erfolgreich abzuschließen.

In der Vergangenheit hat die Erfahrung gezeigt, dass bereits in der Studieneingangsphase (in den ersten wenigen Wochen) zwei Fakten zu einer Fehleinschätzung des Studiums durch die Studenten führen.

(1) *Die scheinbare Einfachheit des zu Beginn gelehrten Stoffes* — der Stoff, der in den Vorlesungen zu Beginn vorgetragen wird, scheint den meisten wohlbekannt und leicht verständlich. Dies verführt dazu, sich zu Beginn auf dem in der Schule gelernten „auszuruhen“ und den Punkt zu verschlafen, an dem der sichere Hafen des bereits Erlernten verlassen wird. Der Stoff sieht nämlich nur auf den ersten Blick einfach aus, denn **die wahre Schwierigkeit liegt nicht darin *was* behandelt wird sondern *wie* es behandelt wird**. Jeder sollte also die scheinbare Einfachheit zu Beginn dazu nützen, zunächst zu verstehen, *wie* der Stoff präsentiert wird und warum das gerade *so* geschieht.

(2) Der *Abstraktionsschock* hängt unmittelbar mit dem zuvor gesagten zusammen. Während in der Schule die meisten Lehrer Mathematik an Hand von Beispielen erklären und weiterentwickeln, ja der gesamte Unterricht meist darauf fokussiert wird, dienen in der höheren Mathematik Beispiele vor allem dazu Sachverhalte zu illustrieren. Die wahre Entwicklung erfolgt innerhalb abstrakter Strukturen; diese werden durch möglichst wenige grundlegende Attribute **definiert**, und weitere gültige Eigenschaften sowie Querbeziehungen zu anderen Strukturen werden in **Beweisen** mittels logischer Schlussfolgerungen aus diesen Grundlagen und bereits bekannten Tatsachen abgeleitet.

Einer der häufigsten Fehler von Studienanfängern liegt darin, den Beweisen nicht die nötige Aufmerksamkeit zukommen zu lassen. Das heißt den wahren Geist der Mathematik zu verfehlen und die wahren Schwierigkeiten, besonders am Anfang, zu übersehen. Zusätzlich führt es dazu, dass bereits nach wenigen Wochen des Studiums die geschaffenen Strukturen einen Umfang und ein Abstraktionsniveau erreicht haben, das sich mit Schulwissen und Beispielen allein nicht mehr überblicken lässt. Mitlernen und Hinterfragen des Gehörten bereits zu Beginn des Studiums helfen, den Schock zu verringern oder gar zu verhindern.

Diese Lehrveranstaltung wurde im Studienplan mit der Absicht eingeführt, eine Brücke zwischen der Mittel- und der Hochschulmathematik zu schlagen. Sie soll also dazu dienen, die StudienanfängInnen an die abstrakte Art und Weise, in der Mathematik an Universitäten gelehrt wird, zu gewöhnen und außerdem die Studierenden auf ein annähernd einheitliches Wissensniveau zu führen, das auf Grund unterschiedlicher Lehrpläne in den verschiedenen Schultypen zu Studienbeginn nicht gegeben ist.

1.1. Hürden zu Studienbeginn

Das Mathematikstudium bietet den meisten Studienanfängern zu Beginn einige grundlegende Hürden, die in diesem Kapitel angesprochen werden sollen.

1.1.1. „Buchstabenrechnen“ versus „Zahlenrechnen“ — Abstraktion. Zahlen spielen im Mathematikstudium eine gegenüber der Schule untergeordnete Bedeutung. Reines Rechnen ist kein grundlegender Bestandteil des Lehrstoffs, es ist allerdings Voraussetzung und wird nicht wiederholt. Im Rahmen von *Beispielen* wird das Rechnen mit Zahlen dazu herangezogen, die abgeleiteten Theoreme zu illustrieren.
ACHTUNG: Das bedeutet nicht, dass richtiges Rechnen im Mathematikstudium zweitrangig ist! Es ist unverzichtbare Grundlage.

Ein großer Teil der mathematischen Theorie wird durch abstrakteres Ableiten gewonnen. Dabei spielen mitunter auch Rechenvorgänge eine wichtige Rolle, diese Ableitungen zielen jedoch meist darauf ab, möglichste Allgemeinheit in den Aussagen zu erzielen.

Das „Buchstabenrechnen“ steht also im Mathematikstudium im Vordergrund.

1.1.2. „Ich habe genau einen Bruder“ — Sprache. Die Sprache dient in der Mathematik, wie auch im täglichen Leben, der Informationsübermittlung. Die Aufgabe des Sprechers ist es dabei, durch geeignete Sprachwahl dem Hörer möglichst wenig Mühe beim Verstehen zu verursachen. Der Beruf des Mathematikers prägt die verwendete Sprache, wie das bei jedem Beruf der Fall ist.

Genauso wie von einem Arzt in der Regel anstelle des Wortes „Ellenbogenbruch“ meist „Olekranonfraktur“ verwendet wird, kann man von Mathematikern mitunter „ich habe genau einen Bruder“ hören. Während jedoch ein Mediziner einige Monate Zeit hat, seine Sprache an das Berufsbild anzupassen, ist es für Mathematikstudenten notwendig, die grundlegenden Sprechweisen äußerst rasch zu erlernen. Ohne diese Fähigkeit gehen viel wesentliche Information und das Grundverständnis der mathematischen Aussagen verloren.

Nachdem die Mathematik ein Gebiet ist, in dem es auf Exaktheit ankommt, ist die mathematische Sprache Regeln unterworfen, die über jene hinausgehen, die für Umgangssprache (Hochsprache) und Literatur gelten.

In dieser Vorlesung werden sprachliche Regeln durch grau hinterlegte Schrift hervorgehoben. Viele der hier zitierten Regeln sind ebenso wie viele dazu gehörende Beispiele dem Buch [**Beutelspacher 1999**] entnommen.

Man beachte, dass mathematische Sprache als Grundlage die Hochsprache bzw. die Literatur hat. Grundsätzlich kann man daher davon ausgehen, dass mathematische Texte zwar Gebrauchsliteratur aber immerhin Literatur sind. Wenn Sie also die Lösungen von Übungsbeispielen, Seminar- oder Diplomarbeiten, gar Dissertationen verfassen, so halten sie wenigstens die folgenden literarischen Grundregeln zusätzlich zu den in dieser Vorlesung behandelten mathematischen Konventionen ein.

Schreiben Sie in vollständigen Sätzen und formulieren Sie überschaubar und klar: Bedenken Sie, dass ein Satz zumindest Subjekt und Prädikat enthalten sollte. Lange, verschachtelte Sätze sind schwer verständlich und lassen weder den Verfasser intelligenter wirken noch den Text glaubwürdiger werden.

Jeder Satz, den Sie schreiben, muss (zumindest für Sie) einen Sinn haben: Vermeiden Sie, durch übertriebene Symbolsetzung und logische Formalismen Ihre Aussagen so zu verschlüsseln, dass am Ende nicht einmal Sie selbst auf Anhieb ihren Inhalt verstehen.

Schließlich die wichtigste Regel: Brechen Sie ruhig alle in diesem Skriptum vorgestellten Regeln, wenn Sie sich durch sie eingeengt fühlen, und wenn Sie wissen, was Sie tun.

1.1.3. „Q.E.D.“ — Beweise. Seit Euklid im dritten Jahrhundert vor Christus seine *Elemente* geschaffen hat, in der er die gesamte damals bekannte Mathematik zusammengefasst hat, ist die logische Struktur, das Fundament der Mathematik, auf Beweisen errichtet.

Auf diese Weise wird sichergestellt, dass in der mathematischen Welt die gemachten Aussagen rein logisch nachgewiesen oder widerlegt werden können. Sie müssen nicht durch „Experimente“ oder „Expertengutachten“ gestützt werden. Auch der in vielen Wissenschaften wohlbekannte philosophische Kampf zwischen verschiedenen Schulen und Lehrmeinungen findet in der Mathematik nicht statt, oder beschränkt sich zumindest darauf, ob ein bestimmtes Gebiet interessant bzw. modern ist oder eben nicht.

Das Beweisen ist für StudienanfängerInnen ungewohnt, die aus der Schule gewöhnt sind, die Aussagen ihres Lehrers aufzunehmen und die vorgestellten Methoden nachzuvollziehen. Es ist in der Schule unökonomisch, alle Aussagen des Lehrers zu hinterfragen. Auf der Universität wird dies anders. Grundsätzlich sollte man scheinbar sein gesamtes Vorwissen hinter sich lassen und sich von neuem von den bisher geglaubten Tatsachen überzeugen (lassen).

Ein großer Fehler von Studienanfängern besteht darin, bei Übungsbeispielen von bis dahin unbewiesenen Tatsachen auszugehen und Beispiele oder Beweise dadurch fälschlicherweise abzukürzen oder gar zu verderben. Darum

> **Unterscheiden Sie im Rahmen eines Beweises oder einer Übungsaufgabe immer genau zwischen den Resultaten, die sie verwenden dürfen und denen die Sie kennen, oder zu kennen glauben.**

Das scheint nur auf den ersten Blick sinnlos. In Wahrheit wird damit ein zweifacher Zweck verfolgt. Zum einen wird der Blick dafür geschult, keine „Lücken im mathematischen Gebäude“ zu hinterlassen. Oft ist das der Sinn hinter einem scheinbar einfachen Übungsbeispiel. Zum anderen wird darauf vorbereitet, auch Beweise in mathematischen Strukturen zu finden, die ärmer an Eigenschaften sind und für die manche Resultate nicht gelten.

Zuletzt noch einige sprachliche Hinweise:

Stellen Sie ihre Beweise sorgfältig dar: Dadurch vermeiden Sie es, Lücken in der Kette logischer Schlüsse zu übersehen. Wesentlich bei der Erstellung von Beweisen ist eine sinnvolle Gliederung und sinnvolle Untergliederungen.

Beachten Sie beim Beweisen zu Beginn die folgenden Prinzipien:

Sagen Sie, was Sie beweisen: Außerdem sollten Sie an jeder Stelle im Beweis sicherstellen, dass die Hörerin oder der Leser genau weiß, welche Teilbehauptung Sie gerade untersuchen. Folgen Sie dem folgenden Grundprinzip:

> **Sagen Sie immer, was Sie als nächstes vorhaben, führen Sie es durch, und sagen Sie danach, dass Sie es getan haben.**

Es empfiehlt sich auch, zu Beginn die zu beweisende Aussage in mathematische Form zu übersetzen.

Gliedern Sie ihren Beweis: Alle Beweise, die länger als etwa eine halbe Seite sind, sollten in Teilabschnitte unterteilt werden. Zerlegen Sie den Beweis in eine Reihe von Teilbehauptungen oder Fällen. Kennzeichnen Sie diese mit Einschüben wie *Schritt 1:*, *Schritt 2:*, bzw. *Fall 1:*, *Fall 2:*, etc. Achten Sie besonders bei der Unterteilung in Fälle, dass Sie keinen Fall vergessen. Führen Sie niemals Fälle ein, die nicht gesondert behandelt werden müssen.

Kennzeichnen Sie den Schluss eines Beweises: Es ist äußerst ermüdend für einen Leser, wenn er sich nie sicher sein kann, wo ein Beweis beginnt und wo er genau endet. Als Kennzeichen für das Ende eines Beweises dienen manchmal Phrasen wie

- *Damit ist alles gezeigt.* oder
- *... was wir behauptet hatten.*

und ähnliche Sätze. Das zwingt den Leser dazu, den Beweis bis zum Ende zu lesen und erschwert es, sich einen schnellen Überblick zu verschaffen, speziell wenn mehrere Resultate und Zwischentexte aufeinander folgen. übersichtlicher sind die Standardabkürzungen

- *w.z.z.w* — was zu zeigen war — oder die lateinische Variante
- *Q.E.D.* (auch *q.e.d.* oder *qed.*) — quod erat demonstrandum.

In modernen Büchern hat sich das ökonomische Beweisabschlusszeichen, das meist am Ende der letzten Beweiszeile steht,

... $\square$

durchgesetzt.

Achten Sie im Verlauf der Vorlesung auf die Struktur der vorgetragenen Beweise, nehmen Sie sie als Beispiele und achten Sie auf die grau hinterlegten Textstellen, mit denen typische Redewendungen und die Struktur hervorgehoben werden.

1.2. Schulstoff

Parallel zu dieser Vorlesung werden wichtige Aspekte des AHS–Schulstoffs im Rahmen von Workshops wiederholt. Ein Großteil dieses Stoffes wird in nicht exakter Form vorgetragen. Die Darstellung orientiert sich am Lehrstoff, der für Realgymnasien vorgesehen ist.

Die Wiederholung des Schulstoffs soll hauptsächlich dazu dienen, die Studenten auf vorhandene Wissenslücken hinzuweisen und die grundlegenden *algorithmischen Fertigkeiten* zu Beginn des Studiums nochmals darzustellen.

> **Es seien alle Studierenden dazu angehalten, den Schulstoff erneut zu lernen, denn die vollständige Beherrschung der dort vermittelten Fakten und Fertigkeiten wird im gesamten folgenden Studium kommentarlos vorausgesetzt werden.**
> **Fehler, auch Rechenfehler, deren Grundlage der Schulstoff ist, sind keine Kavaliersdelikte. Sie zählen bei Übungen und Prüfungen grundsätzlich als *schwere Fehler* und entwerten ein Beispiel vollständig.**

Arbeiten Sie also bei Prüfungen und Übungen sorgfältig und üben Sie den Schulstoff gut ein.

Einige abschreckende Beispiele aus Prüfungen der jüngeren Vergangenheit, die im Mathematikstudium nicht toleriert werden.

- $\frac{a}{b} + \frac{c}{d} = \frac{a+b}{c+d}$.
- $\frac{3x+1}{3y+1} = \frac{x+1}{y+1}$.
- $(e^x)' = x\,e^{x-1}$ bei Ableitung nach x.
- $\int_0^1 e^x\,dx = e$.

- Wenn man mit zwei Würfeln wirft, dann errechnet sich die Wahrscheinlichkeit, dass dabei eine 6 geworfen wird: $\frac{1}{6} + \frac{1}{6} = \frac{1}{3}$.
- $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$.
- $\log ab = \log a \log b$, $\log 0 = 0$.

1.3. Aufbaustoff

Einige Teile des Schulstoffs und die darüber hinaus gehenden Fakten werden in der Vorlesung selbst mit „voller mathematischer Exaktheit" vorgetragen. Sie bilden gemeinsame Grundlage der nachfolgenden Vorlesungen *Analysis 1* und *Lineare Algebra und Geometrie 1*. Im Rahmen dieses Erweiterungsstoffs werden außerdem weitere Sprachregeln und Sprechweisen erklärt, sowie das Beweisprinzip illustriert.

Einige Teile des Erweiterungsstoffs sind nicht Gegenstand der Prüfung und nur gedacht als Hinweise und Informationen für die besonders Interessierten. Die Teile des Skriptums, die gekennzeichnet sind wie dieser Absatz, bilden diesen Zusatzstoff.

Abschließend noch ein Wort zur Exaktheit: Im Prinzip wäre es möglich, den Stoff der Vorlesung zu entwickeln, ohne irgendwelche mathematische Vorkenntnisse vorauszusetzen. Dann würde allerdings Ihr Vorwissen über weite Strecken brach liegen und viele der vorgestellten Konstruktionen würden blutleer und gekünstelt wirken. Um Sie nicht so in eine Motivationskrise zu treiben, werden wir während wir die Inhalte der Vorlesung exakt aufbauen auf den reichen Fundus der Schulmathematik zurückgreifen, um so den Stoff anhand von Beispielen zu motivieren und zu untermalen. Das macht es allerdings nötig, einige mathematische Begriffe und Objekte zu verwenden, bevor sie im Rahmen der Vorlesung exakt definiert wurden, d.h. sie *naiv* zu verwenden und an Ihre bisherige mathematische Erfahrung zu appellieren.

Denken Sie z.B. an Ihre Kenntnisse über Zahlen. Schon seit der Volksschule „wissen" Sie, dass $1 + 1 = 2$ ist. Allerdings, ohne genau sagen zu können, was die einzelnen Symbole 1, + und = eigentlich „sind". Die hier vorkommenden Zahlen $1, 2, \ldots$, also jene Zahlen die man zum Zählen verwendet, heißen die *natürlichen Zahlen*. Per Konvention wollen wir auch die Null zu den natürlichen Zahlen zählen und diese mit $\mathbb{N}$ bezeichnen. Nehmen wir zu den natürlichen Zahlen auch die negative Zahlen hinzu, so gelangen wir zu den *ganzen* Zahlen, die mit $\mathbb{Z}$ bezeichnet werden. Die Quotienten (Brüche) ganzer Zahlen mit von Null verschiedenem Nenner heißen die *rationalen Zahlen*; diese sind bereits ausreichend, um die meisten praktisch auftretenden Rechnungen zu bewältigen und werden mit $\mathbb{Q}$ bezeichnet. Allerdings wurden schon früh in der Geschichte der Mathematik Zahlen „entdeckt", die nicht rational sind, z.B. die Länge der Diagonale im Einheitsquadrat. Nimmt man diese Zahlen hinzu, so landet man schließlich bei den *reellen Zahlen*, die durch die Zahlengerade veranschaulicht werden können. In der Schulmathematik wird oft die folgende Vorstellung bemüht: Man fügt zu den rationalen Zahlen, die man sich als abbrechende oder periodische Dezimalzahlen vorstellen kann, alle — also auch die nicht abbrechenden — Dezimalzahlen hinzu.

Haben Sie in der Schule sogar die *komplexen Zahlen* kennengelernt, so werden Sie sich sicher freuen, diese am Ende dieses Skriptums wiederzufinden. Bis Sie dorthin gelangt sind werden Sie allerdings auch schon genau wissen, wie die natürlichen, ganzen, rationalen und sogar die reellen Zahlen *mathematisch exakt definiert* sind. Nun aber nocheinmal als Überblick und zum „naiven" Einstieg:

natürliche Zahlen	$\mathbb{N}$:	$0, 1, 2, 3, \ldots$
ganze Zahlen	$\mathbb{Z}$:	$0, \pm 1, \pm 2, \pm 3, \ldots$
rationale Zahlen	$\mathbb{Q}$:	Brüche ganzer Zahlen mit nicht verschwindendem Nenner.
reelle Zahlen	$\mathbb{R}$:	Zahlen auf der Zahlengeraden, *alle* Dezimalzahlen.

KAPITEL 2

Grundlagen

Bevor wir uns auf den Ozean der Mathematik hinauswagen, müssen wir als ersten Schritt einiges an Grundlagenwissen ansammeln, einfache Schreibweisen und Ideen, ohne die wir unser Ziel, das Wesen der „höheren“ Mathematik zu erforschen, nicht erreichen können.

2.1. Beweise

Wie wir schon in der Einleitung (Abschnitt 1.1.3) erwähnt haben, bilden *Beweise* die Grundlage des mathematischen Gebäudes. Während wir in den weiteren Abschnitten tiefer auf die Art und Weise eingehen werden, wie Beweise aufgebaut und geführt werden, wollen wir zunächst mit ein paar einfach verständlichen Beispielen beginnen.

Proposition 2.1.1. *Das Quadrat einer geraden Zahl ist gerade.*

Man kann sich die gesamte Mathematik denken als eine Ansammlung von Aussagen, die aus gewissen Grundaussagen (den **Axiomen**) durch logische Schlussfolgerungen abgeleitet werden. Dieser Vorgang heißt **beweisen**. Gilt eine Aussage A als bewiesen, und kann man eine weitere Aussage B logisch aus A ableiten, so gilt auch B als bewiesen.

Die solcherart bewiesenen Aussagen nennt man **Sätze** oder auch **Theoreme**. üblich in der Literatur ist, zuerst die Aussage des Satzes aufzuschreiben und danach den Beweis anzuschließen, in dem die Aussage des Satzes aus bekannten Resultaten hergeleitet wird. Mit diesem Prinzip steht und fällt die Mathematik, daran lässt sich nicht deuteln.

Anstelle von **Satz** bzw. **Theorem** werden auch zuweilen andere Ausdrücke verwendet, die den Stellenwert der Aussagen untereinander im Rahmen einer Theorie andeuten. Ob und wie man diese Begriffe verwendet ist auch Geschmackssache.

Satz, Theorem: Dies ist das typische Resultat einer Theorie.

Hauptsatz: So wird ein besonders wichtiger Satz in einem Teilgebiet der Mathematik genannt. Ein Beispiel ist etwa der Hauptsatz der Differential- und Integralrechnung, den Sie im Rahmen der Analysis Vorlesungen kennen lernen werden.

Lemma: Dieses Wort stammt aus dem Griechischen (die Mehrzahl ist daher **Lemmata**) und bedeutet „Stichwort“ oder „Hauptgedanke“. Es wird in zwei verschiedenen Zusammenhängen verwendet. Zum einen bezeichnet es ein kleines, meist technisches Resultat, einen **Hilfssatz**, der im Rahmen des Beweises eines wichtigen Satzes verwendet wird aber selbst meist uninteressant ist. Zum anderen handelt es sich dabei um besonders wichtige **Schlüsselgedanken**, die in vielen Situationen nützlich sind. Solche genialen Erkenntnisse tragen meist den Namen des Erfinders (Lemma von Zorn, Lemma von Urysohn,...).

Proposition: Dies ist die lateinische Bezeichnung für Satz und wird manchmal an dessen Stelle verwendet, meist aber um ein Resultat zu bezeichnen, dessen Wichtigkeit zwischen der eines Hilfssatzes und der eines Theorems liegt.

Korollar, Folgerung: Dies ist ein Satz, der aus einem anderen Satz durch triviale oder sehr einfache Schlussweise folgt. Manchmal ist es ein Spezialfall einer bereits bewiesenen allgemeineren Aussage. Das Wort Korollar stammt übrigens vom lateinischen Wort *corollarium* ab, welches ein Kränzchen bezeichnet, das der Gastgeber dem Gast „einfach so“ schenkt.

Beweis. Sei n eine beliebige gerade Zahl. Nachdem n durch 2 teilbar ist, existiert eine ganze Zahl m mit $n = 2m$.

Wir können also nun das Quadrat von n durch m ausdrücken und erhalten $n^2 = (2m)^2 = 4m^2$. Natürlich ist $4m^2$ durch 2 teilbar, und daher ist n^2 gerade. □

Falls Ihnen der Beweis (zu) einfach erscheint, dann beherzigen Sie bitte nochmals Punkt (1) auf Seite 3 und lesen aufmerksam weiter.

Im obigen Beweis haben wir die Voraussetzung (die ursprüngliche Zahl ist gerade) genommen, sie ein wenig umgeformt und daraus die Behauptung (ihr Quadrat ist gerade) hergeleitet. Beweise, die auf diese Art vorgehen, nennen wir **direkte Beweise**.

Definition 2.1.2. *Eine* Primzahl *ist eine natürliche Zahl $p > 1$, die nur die trivialen Teiler besitzt, d.h. deren einzige Teiler* 1 *und sie selbst sind.*

Definitionen dienen zur Vergabe von *Namen*. Sie sind weder richtig noch falsch (außer bei der Reproduktion schon vorhandener Definitionen im Rahmen einer Prüfung); sie können allerdings sinnvoll oder unsinnig sein.

Eine Definition verändert nicht das mathematische Gebäude, bloß die Sprache darüber wird um ein weiteres Vokabel ergänzt.

Theorem 2.1.3. *(Satz von Euklid) Es gibt unendlich viele Primzahlen.*

Beweis. Nehmen wir einmal an, es gäbe nur endlich viele Primzahlen. Wenn das so ist, können wir sie mit $p_1, \dots, p_n$ bezeichnen.

Nun bilden wir $m = p_1 p_2 \dots p_n + 1$. Die Zahl m ist verschieden von allen Primzahlen und muss daher durch eine der Zahlen p_i teilbar sein.

Nun ist aber das Produkt $p_1 \dots p_n$ durch jede der endlich vielen Primzahlen p_i teilbar, und daher muss auch 1 durch p_i teilbar sein, damit m durch p_i teilbar sein kann. Dies ist jedoch offensichtlich nicht möglich, und so endet unsere logische Beweiskette in einem Widerspruch.

Wir müssen also unsere oben getroffene Annahme verwerfen, und daher existieren tatsächlich unendlich viele Primzahlen. □

In diesem Beweis sind wir anders herum vorgegangen. Wir haben mit einer Annahme begonnen, deren Aussage gerade das Gegenteil unserer Behauptung war. Danach haben wir eine logische Schlusskette bis zu einem Widerspruch verfolgt. Die Annahme konnte also nicht richtig gewesen sein, und daher musste zwangsläufig ihr Gegenteil stimmen („tertium non datur“), also unsere Behauptung wahr sein.

Beweise dieser Struktur nennen wir **indirekte Beweise**.

2.2. Indizes

Im Beweis von Theorem 2.1.3 sind Ausdrücke der Form $p_1, \dots, p_n$ und p_i vorgekommen. Die unter das p tiefer gestellten Zahlen und Buchstaben nennt man **Indizes**.

Indizes dienen dem Mathematiker dazu, miteinander verwandte Objekte weitgehend einheitlich zu bezeichnen. Darum keine Angst vor Indizes. In vielen Fällen sind sie einfacher und klarer als alle anderen Darstellungsmöglichkeiten. Besonders im Zusammenhang mit Summen und Produkten (siehe Abschnitt 2.3) treten sie häufig auf.

Eine wichtige Eigenschaft eines Index ist, dass er verschiedene Werte annehmen kann, ganz wie eine Variable. So kann der Index i im Ausdruck p_i im Beweis zu Theorem 2.1.3 als Wert alle natürlichen Zahlen von 1 bis n annehmen.

Die Einzahl von Indizes ist übrigens *Index* und nicht Indiz, deren Mehrzahl lautet Indizien, und diese haben in Gerichtssälen nicht aber in Mathematiktexten Platz.

Es ist z.B. offensichtlich, dass die Argumente der Funktion h im folgenden Beispiel allesamt Variable sein sollen, und dass h genau n Argumente benötigt.

$$h(x_1, \dots, x_n)$$

Vergleichen Sie das mit der viel unklareren Schreibweise

$$h(x, y, \dots, z)$$

Besonders in der linearen Algebra werden Indizes von Anfang an auftreten. Auch Doppel- (A_{12}, a_{kl}, $b_{i,j+1}$) und sogar Mehrfachindizes (r_{12345}, p_{ijkm}, $Y_{i,i+1,\dots,i+n}$), ja selbst indizierte Indizes ($Y_{i_1,\dots,i_n}$) sind möglich und sinnvoll. Folgender Rat:

> Machen Sie sich immer klar, was welcher Index bedeutet. Falls Buchstaben als Index auftreten, behalten sie immer im Auge, welche Werte der Index annehmen kann.

Beispiel 2.2.1. *Wir ordnen die Zahlen* $1, 2, \dots, 20$ *in einer* Matrix*, also einem rechteckigen Schema von Zahlen, wie folgt an. Dabei bezeichnen wir die Matrix mit* A*.*

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \end{pmatrix}$$

Mit Hilfe eines Doppelindex können wir die einzelnen Einträge der Matrix bezeichnen. Wir haben z.B. $A_{23} = 8$ *und* $A_{31} = 11$*. Wir können sogar die gesamte Matrix über ihre Elemente mit Hilfe der Indizes definieren, indem wir schreiben*

$$A_{ij} = 5i + j - 5, \quad i = 1 \dots 4,\ j = 1 \dots 5.$$

Oft werden die Einträge von Matrizen auch mit kleinen Buchstaben bezeichnet, also die Einträge der Matrix A *mit* a_{ij}*.*

Bei Umformungen von Ausdrücken sind Indizes „in Schachteln verpackt“. Das bedeutet, dass man sie nicht „wegkürzen“ oder ähnliches kann. Zur Illustration seien einige richtige und einige falsche Beispiele angegeben.

$$\begin{aligned} A_{i+1+3\cdot 5,j} &= A_{i+16,j} \\ f_i - 1 &\neq f_{i-1} \\ B_s B_s &= B_s^2 \neq B_{s^2} \\ \frac{B_s}{s} &\neq B \end{aligned}$$

2.3. Summen, Produkte — Zeichen

In der Mathematik untersucht man häufig Summen, in denen die Anzahl der Terme nicht a priori fest steht. So hat etwa ein allgemeines **Polynom** n–ten Grades die Form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

mit $n+1$ Termen, die aufsummiert werden. Um die Schreibweise von den Punkten $(+\dots+)$ zu befreien, verwendet man eine allgemeinere Notation.

Zeichen wie das Summen- und das Produktzeichen, werden also dazu eingeführt, um eine vielfache Verknüpfung ähnlicher Ausdrücke vereinfacht darzustellen. So kann man mit Hilfe des Summenzeichens Σ das Polynom im oberen Beispiel schreiben als

$$p(x) = \sum_{i=0}^{n} a_i x^i. \tag{2.1}$$

Genauer betrachtet besteht der allgemeine Summenausdruck mit dem Summenzeichen aus vier verschiedenen Teilen.

- Es gibt es eine **Laufvariable**, den **Summationsindex**, in unserem Beispiel i.
- Diese Variable nimmt *alle ganzen* Zahlen beginnend mit der **unteren Grenze**, im Beispiel 0,
- bis zur **oberen Grenze**, in Gleichung (2.1) ist sie n, in Einserschritten an.
- Der Gesamtausdruck entspricht dann einer Summe von Termen, die aussehen wie der **allgemeine Summand**, hier $a_i x^i$, in dem der Summationsindex jeweils durch alle Werte ersetzt wird. **In der dadurch gebildeten Summe kommt der Summationsindex also nicht mehr vor!**

Betrachtet man eine Summe, so kann man sofort erkennen, aus wievielen Teilen die Summe besteht

$$\text{Anzahl der Summanden} = \text{obere Grenze} - \text{untere Grenze} + 1.$$

Dies ist auch der erste Schritt in der Analyse eines allgemeinen Summenausdrucks.

Man kann das Summenzeichen dazu verwenden, die Verknüpfung einer bestimmten Anzahl von Ausdrücken darzustellen. Ein einfaches Beispiel dazu ist

$$\sum_{i=1}^{4} \frac{1}{i+1} = \frac{1}{1+1} + \frac{1}{2+1} + \frac{1}{3+1} + \frac{1}{4+1}$$

Die wahre Stärke besteht allerdings, wie erwähnt, darin, dass man eine unbestimmte Anzahl von Termen summieren kann:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$$

In der Analysis wird gezeigt werden, dass selbst die Unendlichkeit hier **keine** Grenze bildet! Man kann zum Beispiel eine **unendliche Reihe** (hier an einem Beispiel) bilden, und schreiben:

$$\sum_{i=1}^{\infty} \frac{1}{i} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots$$

Den tieferen mathematischen Sinn dieses Ausdrucks wollen wir an dieser Stelle allerdings nicht untersuchen.

Die Laufvariable kann man den jeweiligen Bedürfnissen des Problems anpassen. Man kann sie beliebig umbenennen und sogar weitere Transformationen durchführen (ähnlich der Substitutionsregel für Integrale), wenn man dabei beachtet, dass sich das Ergebnis nicht ändert. So kann man etwa eine **Indexverschiebung** durchführen: Setze zum Beispiel $i = j + 2$ so gilt:

$$\sum_{i=3}^{9} a_i = \sum_{j=1}^{7} a_{j+2}$$

Wir haben dabei die neuen Grenzen für j durch Einsetzen berechnet

$$\begin{aligned} \text{untere Grenze:} \quad & 3 = j + 2 \Rightarrow j = 1 \\ \text{obere Grenze:} \quad & 9 = j + 2 \Rightarrow j = 7 \end{aligned}$$

und im allgemeinen Summanden i durch $j+2$ ersetzt.

Nach Definition ist übrigens das Ergebnis einer allgemeinen Summe gleich 0, falls die untere Grenze größer als die obere Grenze ist.

Es treten in der Mathematik natürlich nicht nur Summen variierender Länge auf, auch für andere Operationen, etwa Produkte, benötigt man ein ähnliches Prinzip, und daher hat man viele dem Summenzeichen entsprechende Zeichen eingeführt. So gibt es etwa das bereits in der Analysis wichtige Produktzeichen ($\prod$) und noch weitere, etwa $\bigcup$, $\bigcap$, $\bigodot$, $\bigoplus$, usw., die in anderen Bereichen der Mathematik eine große Rolle spielen.

Die Anwendung dieser Zeichen folgt demselben Schema wie die des Summenzeichens. So ist etwa

$$\prod_{i=1}^{5} b_i = b_1 b_2 b_3 b_4 b_5,$$

$$\prod_{i=1}^{0} x_i = \mathbf{1},$$

Das „leere Produkt“ (obere Grenze ist kleiner als untere Grenze) wird also als 1 festgelegt.

Oft lassen sich Teile der verknüpften Ausdrücke vor das Verknüpfungszeichen ziehen, wobei man stets darauf achten muss, dass dies nach den Rechenregeln für die jeweilige Operation geschieht. Beim Summenzeichen verwendet man das Herausheben:

$$\sum_{i=1}^{n} 7x_i = 7\sum_{i=1}^{n} x_i.$$

ACHTUNG: Man kann nur Konstante herausheben! Also nicht:

$$\sum_{i=1}^{n} ix_i \neq i\sum_{i=1}^{n} x_i.$$

Beim Produktzeichen muss man beachten, dass solche Konstanten ja multipliziert werten! Daher:

$$\prod_{i=1}^{n} 7x_i = \mathbf{7^n}\prod_{i=1}^{n} x_i.$$

Man kann das Produktzeichen auch verwenden um **Fakultäten** anzuschreiben:

$$n! = \prod_{i=1}^{n} i \quad \forall n \geq 0.$$

Definition 2.3.1. *Die* Fakultät *ist rekursiv definiert durch:*

$$0! := 1$$
$$(n+1)! := (n+1)n!$$

Dieser Ausdruck wird besonders für kombinatorische Probleme benötigt. So gibt $n!$ die Anzahl der Möglichkeiten an, n verschiedene Dinge hintereinander aufzureihen.

Eine wesentliche Vereinfachung ist bei Summanden spezieller Gestalt möglich, nämlich für sogenannte **Teleskopsummen**:

$$\sum_{i=1}^{n}(a_i - a_{i-1}) = \cancel{a_1} - a_0 + \cancel{a_2} - \cancel{a_1} + \cancel{a_3} - \cancel{a_2} + \cdots + \cancel{a_{n-1}} - \cancel{a_{n-2}} + a_n - \cancel{a_{n-1}} = a_n - a_0$$

Analog ergeben sich **Teleskopprodukte**:

$$\prod_{i=1}^{n} \frac{a_i}{a_{i-1}} = \frac{a_n}{a_0}$$

Zum Abschluss stellen wir noch eine weitere Verwendung des Summenzeichens vor (Analoges gilt natürlich auch für die verwandten Zeichen). Der Ausdruck

$$\sum_{i \in I} a_i$$

definiert eine Summe, die für jedes Element der Menge I einen Term enthält. ähnlich wie zuvor wird im allgemeinen Summanden die Laufvariable i jeweils durch das ausgewählte Element ersetzt. Diese Notation hat vor allem zwei Vorteile. Zum einen können auch „unregelmäßige" Indexmengen verwendet werden, und zum anderen bleibt die Anzahl der Indices nicht auf endlich (oder abzählbar; vgl. 3.3.4 unten) viele beschränkt.

Beispiel 2.3.2. *Es gilt*

$$\sum_{i \in \{1,4,7,21\}} a_i^2 = a_1^2 + a_4^2 + a_7^2 + a_{21}^2.$$

2.4. Gleichungsumformungen in Beweisen — Stil und Fallen

2.4.1. Elementare Umformungen. Zunächst zur Schreib- und Sprechweise:

Wenn man Ketten von Gleichungen untereinander schreibt, so bedeutet das, dass die *untere* Gleichung *aus der oberen* folgt. Das bedeutet: Wenn die obere Gleichung gilt, dann gilt auch die untere.

Beispiel 2.4.1. *Betrachten wir die Ableitung*

$$\begin{array}{rcll}
3r^2 + 4r + 5 &=& -r^3 + r + 4 & \quad | + r^3 - r - 4 \\
r^3 + 3r^2 + 3r + 1 &=& 0 & \\
(r+1)^3 &=& 0 & \quad | \sqrt[3]{\ } \\
r + 1 &=& 0 & \quad | - 1 \\
r &=& -1 &
\end{array}$$

Sie ist, wie in der Mathematik üblich, von oben nach unten gültig. Das bedeutet, wenn wir Folgerungspfeile einführen, können wir die Implikationen hervorheben

$$\begin{array}{rcllr}
3r^2 + 4r + 5 &=& -r^3 + r + 4 & \quad | + r^3 - r - 4 & \Rightarrow \\
r^3 + 3r^2 + 3r + 1 &=& 0 & & \Rightarrow \\
(r+1)^3 &=& 0 & \quad | \sqrt[3]{\ } & \Rightarrow \\
r + 1 &=& 0 & \quad | - 1 & \Rightarrow \\
r &=& -1 & &
\end{array}$$

und wenn wir alle Zwischenschritte weglassen, ergibt sich der logische Schluss

$$3r^2 + 4r + 5 = -r^3 + r + 4 \Rightarrow r = -1.$$

Wenn man Umformungen durchführt, bei denen man ausdrücken möchte, dass sie in beide Richtungen stimmen, so **muss** man das durch explizites Setzen von Äquivalenzpfeilen ($\Leftrightarrow$) anzeigen.

Beispiel 2.4.2. *In Beispiel 2.4.1 folgen in Wahrheit die oberen Gleichungen auch aus den unteren, d.h. sie sind wirklich alle äquivalent. Um das zu unterstreichen, wollen wir* *daher*

$$\begin{array}{rcll} 3r^2+4r+5 &=& -r^3+r+4 & \mid +r^3-r-4 \quad \Leftrightarrow \\ r^3+3r^2+3r+1 &=& 0 & \quad \Leftrightarrow \\ (r+1)^3 &=& 0 & \mid \sqrt[3]{} \quad \Leftrightarrow \\ r+1 &=& 0 & \mid -1 \quad \Leftrightarrow \\ r &=& -1 & \end{array}$$

schreiben.

Auch bei Schlüssen von unten nach oben in einer Umformung müsste man die Implikationsrichtung durch Setzen des entsprechenden Pfeils ($\Leftarrow$) angeben. **Schlüsse von unten nach oben gelten nicht als guter mathematischer Stil und sollten daher unbedingt vermieden werden.** Machen Sie sich daher immer klar, womit eine Umformung beginnt und was Sie abzuleiten gedenken. Wenn Sie die Rechnung vom Ergebnis zum Ausgangspunkt hin durchführen, so kehren sie die Schlussweise in der Reinschrift um!

Welche Umformungen sind eigentlich erlaubt? Man darf auf beiden Seiten dasselbe addieren (subtrahieren). Man darf auch beide Seiten mit demselben multiplizieren; Wie steht es mit der Division?

Theorem 2.4.3 (Sinnlosigkeit der Zahlen)**.** *Alle Zahlen sind gleich.*

Beweis. O.B.d.A. werden wir den Spezialfall $1 = 2$ beweisen. Wir werden nur elementare Umformungen benutzen. Wir beginnen mit reellen Zahlen a und b mit $a = b$.

Die Abkürzung **O.B.d.A.** steht für *ohne Beschränkung der Allgemeinheit*. Korrekt verwendet man sie zu Beginn eines Beweises oder Beweisteils. Damit wird der Leser auf zwei Dinge aufmerksam gemacht. Einerseits soll nur ein Teil der Aussage bewiesen werden, und andererseits ist der Autor des Beweises der Meinung, dass die Gesamtaussage einfach aus dem Bewiesenen folgt. Es steckt also hinter o.B.d.A. ein weiterer mathematischer Satz („aus dem tatsächlich Bewiesenen folgt die Aussage des Satzes"), und o.B.d.A. bedeutet dann, dass diese Implikation nach Meinung des Autors *trivial*, also besonders einfach herzuleiten ist.

Zusätzlich zur Beschränkung auf einen Sonderfall, aus dem schon die gesamte Aussage folgt, kann man O.B.d.A. auch noch zur Vereinfachung der Bezeichnung oder zum Ausschließen trivialer Sonderfälle verwenden. Beispiele zu diesen Verwendungen werden Sie in späteren Beweisen finden.

$$\begin{array}{rcll} a &=& b & \\ a^2 &=& ab & \text{nach Multiplikation mit } a \\ a^2+a^2 &=& a^2+ab & \text{nach Addition von } a^2 \\ 2a^2 &=& a^2+ab & \\ 2a^2-2ab &=& a^2+ab-2ab & \text{nach Subtraktion von } 2ab \\ 2a^2-2ab &=& a^2-ab & \\ 2(a^2-ab) &=& 1(a^2-ab) & \\ 2 &=& 1 & \text{nach Division durch } a^2-ab, \end{array}$$

woraus unsere Behauptung folgt. □

Natürlich haben wir in diesem Beweis einen Fehler gemacht. Können Sie ihn entdecken?

An diesem Beispiel sieht man schön die Falle, in die man tappen kann bei Verwendung der Division als Äquivalenzumformung. Man muss sich immer überzeugen, dass man nicht durch 0 dividiert wie im obigen Beweis, und 0 kann sich hinter komplizierten Ausdrücken verbergen.

2.4.2. Anwendung von Funktionen. Man kann nicht nur auf beiden Seiten der Gleichung elementare arithmetische Operationen ausführen, sondern man kann auch versuchen, geeignete Funktionen anzuwenden um zu vereinfachen. Besonders beliebt sind Umkehrfunktionen von Funktionen, die auf beiden Seiten der Gleichung auftauchen.

Ein einfaches Beispiel bietet die nächste Umformungskette, in der wir im ersten Schritt die Umkehrfunktion log der Exponentialfunktion angewendet haben.

$$\begin{aligned} e^{3x+4} &= e^{x-2} \quad \mid \log\_ \\ 3x+4 &= x-2 \\ 2x &= -6 \\ x &= -3 \end{aligned}$$

In der Mathematik wird der natürliche Logarithmus oft mit log und nicht mit ln bezeichnet.

Theorem 2.4.4 (Sinnlosigkeit der Zahlen — 2. Versuch)**.** *Alle Zahlen sind gleich.*

Beweis. O.B.d.A werden wir den Spezialfall $4 = 5$ beweisen:

$$\begin{aligned} -20 &= -20 \\ 16-36 &= 25-45 \\ 16-36+\tfrac{81}{4} &= 25-45+\tfrac{81}{4} \\ 4^2-2\cdot 4\cdot \tfrac{9}{2}+\left(\tfrac{9}{2}\right)^2 &= 5^2-2\cdot 5\cdot \tfrac{9}{2}+\left(\tfrac{9}{2}\right)^2 \\ \left(4-\tfrac{9}{2}\right)^2 &= \left(5-\tfrac{9}{2}\right)^2 \qquad \text{weil } (a-b)^2 = a^2-2ab+b^2 \\ 4-\tfrac{9}{2} &= 5-\tfrac{9}{2} \\ 4 &= 5, \end{aligned}$$

womit die Sinnlosigkeit des Zahlenbegriffs erwiesen ist. □

Offensichtlich steckt in diesem Beweis ein Fehler, denn die Ungültigkeit des Satzes steht wohl außer Zweifel. Können Sie den Fehler entdecken?

Die falsche Umformung steht in der vorletzten Zeile: Das Ziehen der Quadratwurzel ist keine Äquivalenzumformung! Möchte man eine Gleichung durch Wurzel Ziehen umformen, so muss man sich zuvor überzeugen, dass die Vorzeichen auf beiden Seiten überein stimmen. Dies ist im obigen Beispiel nicht der Fall, und daher hätten wir schreiben müssen

$$\begin{aligned} \left(4-\tfrac{9}{2}\right)^2 &= \left(5-\tfrac{9}{2}\right)^2 \qquad \Leftarrow \\ 4-\tfrac{9}{2} &= 5-\tfrac{9}{2}. \end{aligned}$$

Allgemein muss man bei der Anwendung von Umkehrfunktionen f^{-1} darauf achten, dass die Funktion f, die man „entfernen" möchte, *injektiv* (siehe Abschnitt 3.3.3) ist, auf den Definitionsbereichen beider Seiten der Gleichung.

Beispiel 2.4.5. *Normalerweise ist das Quadratwurzel Ziehen nicht erlaubt, weil die Funktion $f(x) = x^2$ sowohl x als auch $-x$ auf x^2 abbildet; also das Ziehen der Wurzel nicht eindeutig ist! Schränken wir aber f auf positive reelle Zahlen ein, so vermeiden wir dieses Problem und können gefahrlos Wurzel ziehen.*

Sei $x \geq 0$, und seien $a, b \in \mathbb{R}$. Dann gilt

$$\begin{aligned} 4x^2 &= (a^2+b^2)^2 \\ 2x &= a^2+b^2 \\ x &= \tfrac{1}{2}(a^2+b^2), \end{aligned}$$

und diese Umformung ist richtig, da wir schon wissen, dass $x \geq 0$ und $a^2 + b^2 \geq 0$ (warum?) gelten.

Ist die Anwendung der Umkehrfunktion zwingend nötig, um eine Rechnung fortsetzen zu können, so muss man bei Mehrdeutigkeit Fallunterscheidungen durchführen.

Um wieder zum Beispiel „Quadratwurzel“ zurückzukehren, sehen wir uns an, wie der vorletzte Umformungsschritt im falschen Beweis von Theorem 2.4.4 richtigerweise geführt hätte werden müssen.

$$\left(4 - \tfrac{9}{2}\right)^2 = \left(5 - \tfrac{9}{2}\right)^2$$
$$4 - \tfrac{9}{2} = \pm(5 - \tfrac{9}{2})$$

1. Fall: Vorzeichen $+$:

$$4 - \tfrac{9}{2} = 5 - \tfrac{9}{2}$$
$$-\tfrac{1}{2} = \tfrac{1}{2} \quad \text{ist offensichtlich falsch}$$

2. Fall: Vorzeichen $-$:

$$4 - \tfrac{9}{2} = -\left(5 - \tfrac{9}{2}\right)$$
$$-\tfrac{1}{2} = -\tfrac{1}{2} \quad \text{was stimmt.}$$

Der 1. Fall führt offensichtlich zu einem unsinnigen Ergebnis und muss daher verworfen werden. Der 2. Fall hingegen liefert das richtige Resultat. Nur dieser darf im Beweis des Theorems verwendet werden und wir sind daher erwartungsgemäß nicht in der Lage, die Behauptung $4 = 5$ zu beweisen.

2.5. Vollständige Induktion

Wir haben im Abschnitt 2.1 bereits die beiden grundlegenden Beweisprinzipien, den direkten und den indirekten Beweis kennengelernt.

Die erste *Beweisidee*, die wir kennenlernen wollen, benötigt man oftmals, wenn man eine Behauptung *für alle* natürlichen Zahlen beweisen möchte.

Beispiel 2.5.1. *Betrachten wir die folgende Reihe von Ausdrücken.*

$$1 = 1 = 1^2$$
$$1 + 3 = 4 = 2^2$$
$$1 + 3 + 5 = 9 = 3^2$$
$$1 + 3 + 5 + 7 = 16 = 4^2$$
$$1 + 3 + 5 + 7 + 9 = 25 = 5^2$$

Nach einem „Intelligenztest“ finden wir also heraus, dass die Summe der ersten n ungeraden Zahlen genau das Quadrat von n ergibt.

Nun, besser gesagt hätten wir behaupten sollen, dass wir *vermuten*, dass dem so ist. Die ersten fünf Testbeispiele zu überprüfen ist natürlich nicht genug, um daraus schon auf die allgemeine Aussage schließen zu können, ja nicht einmal das überprüfen der ersten 10 Millionen Fälle würde genügen.

> Was wir benötigen, ist eine Technik, um mit einem Schlag das Resultat *für alle unendlich vielen natürlichen Zahlen auf einmal* zu beweisen.

Machen wir einen Zwischenausflug ins tägliche Leben: Welche Hilfsmittel würden Sie verwenden, um ein Dach zu erklimmen? Wahrscheinlich eine Leiter. Ist es zum Erklimmen einer Leiter wichtig, deren Höhe zu kennen? Nein. Das Wissen um die Technik des Leiterkletterns genügt (abgesehen von Höhenangst und eingeschränkter Kondition — das wollen wir wegabstrahieren).

Was müssen wir wissen, um die Technik des Leiterkletterns zu erlernen. Erstaunlicherweise nur zwei Dinge:

(1) Wie komme ich auf die unterste Leitersprosse? (Leiteranfang)
(2) Wie komme ich von einer Leitersprosse auf die nächst höhere Sprosse? (Leiterschritt)

Finden Sie eine Antwort auf diese beiden Fragen, und kein Dach wird vor Ihnen sicher sein (sofern Sie eine Leiter auftreiben können, die lang genug ist).

Wenn wir nun den Gipfel der Erkenntnis über natürliche Zahlen erklimmen wollen, so gehen wir ganz ähnlich vor. Die mathematische Version des Leiterkletterns heißt **vollständige Induktion**.

Um sie korrekt durchzuführen müssen wir ganz analog zum Leiteranfang erst eine Grundlage, einen Anfang für unsere Behauptung finden. Meist werden wir also unsere für alle natürlichen Zahlen zu beweisende Behauptung erst einmal in einem einfachen Fall überprüfen. üblicherweise ist das der Fall für $n = 0$ oder $n = 1$ aber jede andere natürliche Zahl kann ebenfalls als **Induktionsanfang** dienen.

Danach müssen wir eine Methode finden, den Leiterschritt zu imitieren. Für so einen Schritt gehen wir davon aus, dass wir uns bereits auf einer Leitersprosse befinden, wir also die Aussage schon bewiesen haben für eine bestimmte natürliche Zahl n. Das nennt man die **Induktionsannahme** oder **Induktionsbehauptung**. Von dieser Sprosse ausgehend müssen wir nun eine Methode finden, die nächst höhere Sprosse zu erklimmen. Im Falle der Leiter ist das ein einfacher Schritt, in der Mathematik ist dazu ein Beweis von Nöten. In diesem **Induktionsschritt** leitet man logisch aus der Behauptung für n die Aussage für die Zahl $n + 1$ (die nächste Sprosse) her.

Hat man das geschafft, ist der **Induktionsbeweis** beendet, und man hat tatsächlich die Behauptung für alle natürlichen Zahlen bewiesen (resp. für alle natürlichen Zahlen größer als der Induktionsanfang).

Warum ist das so? Für jede natürliche Zahl können wir die „Induktionsleiter“ so lange hinaufklettern bis die Behauptung auch für diese Zahl bewiesen ist — die Höhe des Daches ist nicht wichtig, so lange wir nur die Technik des Kletterns beherrschen.

Verwenden wir also nun unsere neue Technik, um die Behauptung über die Summe ungerader Zahlen aus Beispiel 2.5.1 zu beweisen.

Proposition 2.5.2. *Es gilt*

$$\sum_{k=1}^{n} 2k - 1 = n^2$$

Beweis. Wir beweisen die Aussage mit vollständiger Induktion.

Induktionsanfang: Es gilt $1 = 1^2$. (Wie gesagt, der Induktionsanfang ist meist leicht.)

Induktionsannahme: Es sei die Behauptung für n bereits bewiesen, also

$$\sum_{k=1}^{n} 2k - 1 = n^2.$$

Induktionsschritt: Wir müssen nun die Behauptung für $n + 1$ zeigen, also

$$\sum_{k=1}^{n+1} 2k - 1 = (n + 1)^2$$

beweisen. Beginnen wir den Beweis mit der linken Seite

$$\sum_{k=1}^{n+1} 2k-1 = \sum_{k=1}^{n}(2k-1) + 2n+1.$$

Für diese Umformung haben wir einfach die Definition des Summensymbols Σ verwendet und den letzten Term explizit aufgeschrieben. Durch diesen Trick (ein Standardtrick in Induktionsbeweisen) haben wir auf der rechten Seite einen Term (den Summenausdruck) erzeugt, der in der Induktionsannahme vorkommt. Wir können also die Induktionsannahme einsetzen und erhalten

$$\sum_{k=1}^{n}(2k-1) + 2n+1 = n^2+2n+1.$$

Die rechte Seite ist ein vollständiges Quadrat, und daher können wir fertig umformen

$$n^2+2n+1 = (n+1)^2,$$

und wir haben den Induktionsschritt beendet.

Damit ist alles bewiesen — in einem Schritt für unendlich viele, ja für alle, natürlichen Zahlen. □

Als ein komplexeres Beispiel für die Anwendung der vollständigen Induktion zum Beweis einer wichtigen mathematischen Tatsache behandeln wir im folgenden Abschnitt den *binomischen Lehrsatz*.

2.5.1. Der binomische Lehrsatz. Der binomische Lehrsatz dient der Auflösung von Potenzen der Form $(a+b)^n$ in eine Summe von Produkten. Er lautet:

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

Er begründet sich durch folgende Überlegung: Beim Ausmultiplizieren von n gleichen Binomen $(a+b)$ wird für jedes Produkt aus jedem Binom entweder ein a oder ein b verwendet. Somit entstehen Produkte der Formen $a^n b^0, a^{n-1}b^1, \ldots, a^1 b^{n-1}, a^0 b^n$. Die entstehenden Produkte werden additiv verknüpft, bleibt also nur noch die Frage, welche Produkte wie oft entstehen. Diese Frage nach dem *Koeffizienten* wird im binomischen Lehrsatz mit $\binom{n}{k}$ beantwortet. Weil er der Koeffizient in der Entwicklung der Potenz eines Binoms $(a+b)$ ist, nennt man ihn **Binomialkoeffizienten**.

Die mathematische Disziplin, die sich unter anderem mit dem Abzählen von Objekten beschäftigt, ist die **Kombinatorik**. Dort besteht eine übliche Lösungsmethode darin, ein Problem durch ein äquivalentes Problem zu ersetzen (die Äquivalenz ist oft schwierig zu zeigen), welches leichter zu lösen ist. Ein im Zusammenhang mit Binomialkoeffizienten stets zitiertes äquivalentes Problem ist das *Pascalsche Dreieck*. Es folgt nachstehenden Regeln:

- Die oberste Ebene enthält eine Position.
- Jede Ebene enthält eine Position mehr als die darüberliegende.
- Jeder Position werden in der darunterliegenden Ebene zwei benachbarte Positionen als Linksuntere und Rechtsuntere zugeordnet.
- Die Linksuntere einer Position ist stets gleich der Rechtsunteren ihrer links benachbarten Position und umgekehrt.
- Um einen Weg zu einer Zielposition zu erhalten, startet man von der einzigen Position der obersten Ebene. Dann geht man immer zur Links- oder Rechtsunteren der aktuellen Position, bis man bei der Zielposition angekommen ist.

- An jeder Position notieren wir dann die Anzahl der Wege, die zu ihr führen. Dabei gilt die Position in der obersten Ebene als Weg zu sich selbst, bekommt also eine 1 zugeordnet.

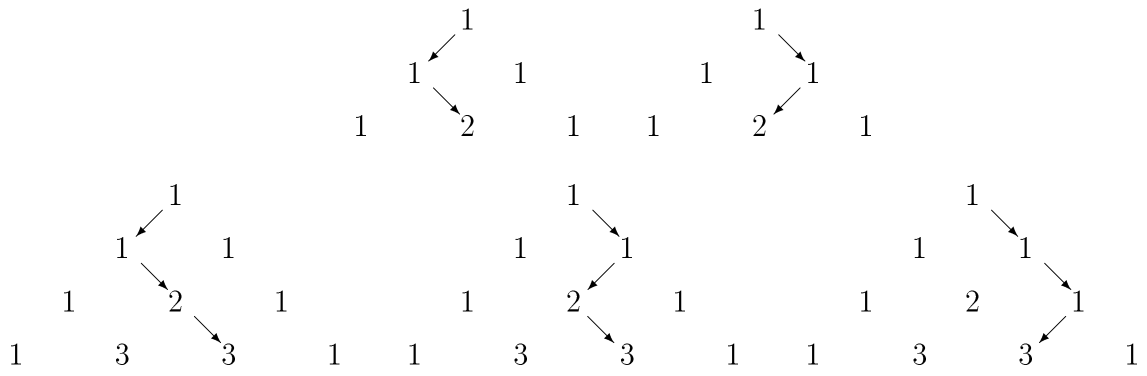


Abbildung 2.1. Pascalsches Dreieck

Der Zusammenhang zwischen dem Pascalschen Dreieck und der Frage, wie oft die einzelnen Produkte beim Ausmultiplizieren auftreten, ist folgender:

- Auf der einen Seite steht beim Finden eines Weges auf jeder Ebene die Entscheidung an, ob man entweder zum Links- oder Rechtsunteren weitergeht.
- Auf der anderen Seite muss man beim Ausmultiplizieren aus jedem Binom entweder ein a oder ein b entnehmen.
- Der an einer Position notierte Wert wird also zum Binomialkoeffizienten des entsprechenden Produktes gleich sein (Dies hier noch unbewiesen wird im Weiteren gezeigt werden.), wobei die Ebene der Potenz entsprechend gewählt werden muss; die Koeffizienten $\binom{n}{k}$ von $(a+b)^n$ findet man also in der $(n+1)$–ten Ebene.

$\binom{n}{k}$ beansprucht also, als Ergebnis den Wert der *k–ten Position der n–ten Ebene* des Pascalschen Dreiecks zu haben, wobei die Nummerierung sowohl für n als auch für k mit 0 beginnt. überlegen wir uns, dass eine Position im Pascalschen Dreieck nur über ihre maximal zwei Oberen zu erreichen ist und alle Wege, zu den beiden Oberen verschieden sind, so ist klarer Weise der Wert einer Position gleich der Summe der Werte ihrer (höchstens zwei) Oberen. Aus dieser Überlegung definieren wir rekursiv.

Definition 2.5.3. *Der* Binomialkoeffizient $\binom{n}{k}$ *für n, $k \in \mathbb{N}$ ist (rekursiv) definiert durch*

(i) $\displaystyle\binom{0}{0} := 1$

(ii) $\displaystyle\binom{n}{k} := 0 \qquad \forall n \in \mathbb{N}$ *und* $k < 0$ *oder* $k > n$,

(iii) $\displaystyle\binom{n}{k} := \binom{n-1}{k-1} + \binom{n-1}{k}$.

In vielen Situationen (auch im Falle des Binomischen Lehrsatzes) ist die rekursive Definition des Binomialkoeffizienten etwas unhandlich. Wir beweisen daher zunächst eine andere (sog. geschlossene) Darstellung desselben.

Proposition 2.5.4. *Es gilt:*

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Beweis. Zu beweisen ist:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Dafür müssen wir zeigen, dass die Formel

$$\frac{n!}{(n-k)!k!}$$

der rekursiven Definition von $\binom{n}{k}$ genügt.

Dabei haben wir zu beachten, dass die Formel nur für $n \geq 0, 0 \leq k \leq n$ gilt. Außerhalb dieser Grenzen ist $\binom{n}{k}$ als 0 definiert.

Zuerst untersuchen wir die Ränder des Pascalschen Dreiecks und zeigen, dass sie ausschließlich aus Einsen bestehen.

Beginnen wir mit dem linken Rand also dem Fall $k = 0$, d.h. den Binomialkoeffizienten der Form $\binom{n}{0}$, $n \in \mathbb{N}$. Aus der rechten Seite der Behauptung ergibt sich tatsächlich

$$\frac{n!}{(n-0)!0!} = \frac{n!}{n!} = 1.$$

Wir müssen nun auch *beweisen*, dass dasselbe aus der rekursiven Definition für $\binom{n}{0}$ folgt. Dazu verwenden wir das Prinzip der vollständigen Induktion:

Behauptung:

$$\forall n \in \mathbb{N} : \binom{n}{0} = 1$$

Induktionsanfang: $n = 0$

$$\binom{0}{0} = 1 \quad \text{nach Definition.}$$

Induktionsannahme: Es gelte

$$\binom{n}{0} = 1.$$

Induktionsschritt:

$$\begin{array}{rclclll} \binom{n+1}{0} & = & \binom{n}{-1} & + & \binom{n}{0} & & \text{rekursive Definition von } \binom{n}{k} \\ & = & 0 & + & 1 & & \text{nach Definition bzw. Induktionsannahme} \\ & = & 1 & & & & \end{array}$$

Das beweist die Behauptung über den linken Rand des Pascalschen Dreiecks.

Ganz analog behandeln wir den rechten Rand, also die Binomialkoeffizienten der Form $\binom{n}{n}$. Aus der rechten Seite der Aussage des Satzes berechnen wir

$$\frac{n!}{(n-n)!n!} = \frac{n!}{n!} = 1.$$

Behauptung:

$$\forall n \in \mathbb{N} : \binom{n}{n} = 1$$

Induktionsanfang: $n = 0$

$$\binom{0}{0} = 1 \quad \text{nach Definition.}$$

Induktionsannahme: Es gelte

$$\binom{n}{n} = 1.$$

Induktionsschritt:

$$\begin{aligned}\binom{n+1}{n+1} &= \binom{n}{n} + \binom{n}{n+1} && \text{rekursive Definition von } \tbinom{n}{k}\\ &= 1 + 0 && \text{nach Induktionsannahme bzw. Definition}\\ &= 1\end{aligned}$$

Das zeigt die Behauptung über den rechten Rand.

Nun beweisen wir die Formel für alle (restlichen) n und k. Dafür müssen wir nachweisen, dass für alle $n \in \mathbb{N}$, $2 \leq n$ und $1 \leq k \leq n-1$

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

gilt. Wir verwenden ein weiteres Mal vollständige Induktion.
Induktionsanfang: $n = 2$, daher $k = 1$

$$\begin{aligned}\binom{2}{1} &= \binom{1}{0} + \binom{1}{1} && \text{nach der rekursiven Definition von } \tbinom{n}{k}\\ &= 1 + 1 && \text{nach dem bereits bewiesenen}\\ &= 2\end{aligned}$$

Andererseits gilt

$$\frac{2!}{(2-1)!\,1!} = \frac{2}{1 \cdot 1} = 2$$

Induktionsannahme: Es gelte

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} \quad \text{für } 1 \leq k \leq n-1.$$

Induktionsschritt:

$$\begin{aligned}\binom{n+1}{k} &= \binom{n}{k} + \binom{n}{k-1} && \text{rekursive Definition von } \tbinom{n}{k}\\ &= \frac{n!}{(n-k)!k!} + \frac{n!}{(n-k+1)!(k-1)!} && \text{Induktionsannahme}\\ &= \frac{n!(n-k+1)}{(n-k+1)(n-k)!k!}\\ &\quad + \frac{n!k}{(n-k+1)!(k-1)!k} && \text{Erweitern}\\ &= \frac{n!(n-k+1)}{(n+1-k)!k!} + \frac{n!k}{(n+1-k)!k!} && \text{Definition der Fakultät}\\ &= \frac{n!(n-k+1) + n!k}{(n+1-k)!k!} && \text{Zusammenfassen der Brüche}\\ &= \frac{n!(n-k+k+1)}{(n+1-k)!k!} && \text{Herausheben}\\ &= \frac{n!(n+1)}{(n+1-k)!k!} && \text{Addieren}\\ &= \frac{(n+1)!}{(n+1-k)!k!} && \text{Definition der Fakultät}\end{aligned}$$

Das beweist, dass die Formel der rekursiven Darstellung von $\binom{n}{k}$ genügt. □

Zum Rechnen mit der Formel aus Proposition 2.5.4 empfiehlt es sich, zu kürzen:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}.$$

Mit Hilfe der in Proposition 2.5.4 nachgewiesenen Formel lässt sich die Definition des Binomialkoeffizienten wie folgt erweitern:

Definition 2.5.5. *Der* Binomialkoeffizient *ist für* $\alpha \in \mathbb{R}$ *und* $k \in \mathbb{N}$ *definiert durch:*

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!} = \frac{\prod_{i=0}^{k-1}(\alpha-i)}{k!}.$$

Kehren wir nun nach diesem Ausflug in die Kombinatorik zum Binomischen Lehrsatz zurück, den wir zum Abschluss diese Kapitels beweisen:

Proposition 2.5.6. *Es gilt für* $a, b \in \mathbb{R}, n \in \mathbb{N}$*:*

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

Beweis. Zu zeigen:

$$\forall n \in \mathbb{N} : \forall a, b \in \mathbb{R} : (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Wir beweisen mittels vollständiger Induktion:
Induktionsanfang: $n = 0$
Klarerweise gilt $(a+b)^0 = 1$. Andererseits

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

Induktionsannahme: Es gelte

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

Induktionsschritt:

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n && \\
&= (a+b)\sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j} && \text{Induktionsannahme}\\
&= \sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j}(a+b) && \text{Ausmultiplizieren}\\
&= \sum_{j=0}^{n}\binom{n}{j}(a^{j+1}b^{n-j}+a^j b^{n-j+1}) && \text{Ausmultiplizieren}\\
&= \sum_{j=0}^{n}\left(\binom{n}{j}a^{j+1}b^{n-j}+\binom{n}{j}a^j b^{n-j+1}\right) && \text{Ausmultiplizieren}\\
&= \sum_{j=0}^{n}\binom{n}{j}a^{j+1}b^{n-j}+\sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j+1} && \text{Aufspalten der Summe}\\
&= \sum_{i=1}^{n+1}\binom{n}{i-1}a^{i}b^{n-i+1}+\sum_{j=0}^{n+1}\binom{n}{j}a^j b^{n-j+1} && \begin{array}{l}\text{Indexverschiebung}\\ j+1=i \text{ und } \binom{n}{n+1}=0\end{array}\\
&= \sum_{k=0}^{n+1}\binom{n}{k-1}a^{k}b^{n-k+1}+\sum_{k=0}^{n+1}\binom{n}{k}a^k b^{n-k+1} && \begin{array}{l}\binom{n}{-1}=0 \text{ und}\\ \text{Laufvariablen umbenannt}\end{array}\\
&= \sum_{k=0}^{n+1}\left(\binom{n}{k-1}a^{k}b^{n-k+1}+\binom{n}{k}a^k b^{n-k+1}\right) && \text{Vereinigen der Summen}\\
&= \sum_{k=0}^{n+1}a^{k}b^{n-k+1}\left(\binom{n}{k-1}+\binom{n}{k}\right) && \text{Herausheben}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{k}b^{n-k+1} && \text{rekursive Definition von } \binom{n}{k}
\end{aligned}
$$

Das beweist den binomischen Lehrsatz. □

KAPITEL 3

Logik, Mengenlehre

Dieses Kapitel handelt von *den* Grundlagen der Mathematik. Der Abschnitt über Boolesche Algebren sollte schon aus der Schule bekannt sein. Versteht man erst das Prinzip von Booleschen Algebren, so hat man damit schon den ersten Schritt zum Verständnis der Aussagenlogik getan. Die Bedeutung der *Quantoren* wird im darauf folgenden Abschnitt erklärt, und schließlich wird auf naive Weise die erste mathematische Struktur eingeführt, die *Mengen*.

3.1. Boolesche Algebren

In diesem Abschnitt wollen wir das Kapitel über Boolesche Algebren aus der Schule aufarbeiten. Es soll uns nicht dazu dienen, daraus die Grundlagen der Mathematik zu bauen, sondern lediglich die Grundoperation der Aussagenlogik motivieren. Wir beschränken uns dabei auf die Schaltalgebra, ein Konzept, das für das Verständnis der Informatik von großer Bedeutung ist.

Elektronische (auch elektrische) Schaltungen bestehen aus elektrischen Leitungen und aus Schaltern. Jede Leitung kann sich in zwei Zuständen befinden (Strom führend bzw. nicht Strom führend), so wie jeder Schalter zwei Zustände (Stellungen) hat: „Ein" und „Aus".

Mathematisch kann man sowohl den Zustand einer Leitung als auch die Stellung eines Schalters mit Hilfe einer Variable beschreiben, die zwei Werte annehmen kann: 0 oder 1. Eine solche Variable nennt man *binäre Variable*.

Mit Schaltern kann man steuern, ob Strom durch eine bestimmte Leitung fließt oder nicht. Das heißt, die Schalterzustände steuern die Zustände von Leitungen. Schaltet man den Schalter ein, so lässt er den Strom passieren, und ergibt sich ein geschlossener Stromkreis, so fließt Strom durch die Leitung. In der Computertechnik wurden mit Hilfe von Transitoren Schaltungen entwickelt, die wie elektronische Schalter funktionieren. Führt dort eine bestimmte Leitung A Strom, so verhält sie sich wie ein Schalter im Zustand „Ein" für eine andere Leitung B. Fließt kein Strom durch Leitung A, so verhält sie sich wie ein Schalter im „Aus"-Zustand für Leitung B.

Baut man eine komplizierte Schaltung aus mehreren Schaltern, die durch Leitungen verbunden sind, so ist meist auf den ersten Blick nicht zu erkennen, welche Leitungen bei welchen Schalterstellungen Strom führen und welche nicht. Man kann sich dann einen Überblick verschaffen, indem man so genannte Schaltwerttabellen aufstellt. An einigen einfachen Schaltungen sei das Prinzip demonstriert.

(1) Setzt man in einem Stromkreis wie in Abbildung 3.1 zwei Schalter hintereinander, bildet man also eine *Serienschaltung*, und untersucht, wann die Leitung Strom führt, erhält man folgende Schaltwerttabelle. Die Bedeutung der Tabelle ist rechts daneben noch einmal explizit erläutert.

a	b	$a \wedge b$	
0	0	0	$0 \wedge 0 = 0$
0	1	0	$0 \wedge 1 = 0$
1	0	0	$1 \wedge 0 = 0$
1	1	1	$1 \wedge 1 = 1$

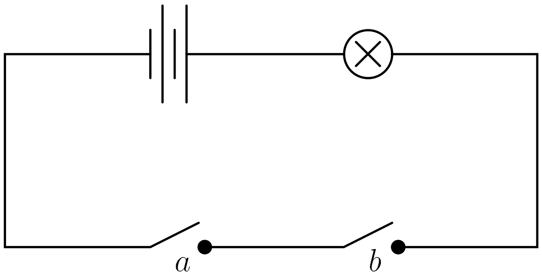


ABBILDUNG 3.1. Serienschaltung — Und-Verknüpfung

Der Strom fließt also, wenn Schalter a **und** Schalter b eingeschaltet sind. Mathematisch schreibt man kurz $a \wedge b$ und spricht a **und** b bzw. von der **Und-Verknüpfung** oder AND-Verknüpfung.

(2) Setzt man in einem Stromkreis wie in Abbildung 3.2 zwei Schalter nebeneinander, so wird man folgendes feststellen: Damit die Leitung Strom führt, reicht es

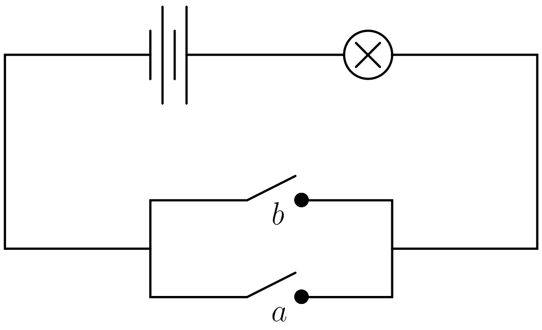


ABBILDUNG 3.2. Parallelschaltung — Oder-Verknüpfung

Schalter a **oder** Schalter b einzuschalten. Eine Schaltung dieser Art nennt man Parallelschaltung und die entsprechende mathematische Verknüpfung heißt **Oder-Verknüpfung** bzw. OR-Verknüpfung. Man schreibt $a \vee b$ und sprich a **oder** b. Die Schaltwerttabelle ist

a	b	$a \vee b$
0	0	0
0	1	1
1	0	1
1	1	1

ACHTUNG: Beachten Sie, dass „oder“ im Gegensatz zum umgangssprachlichen Gebrauch bedeutet, dass a oder b **oder beide** eingeschaltet sein müssen (vgl. Beispiel 3.1.2 und Abschnitt 3.2.1).

(3) Beschriftet man einen Schalter „verkehrt“, so erhält man die einfachste Schaltung, die **Negation** $\neg a$ mit der Schaltwerttabelle

a	$\neg a$
0	1
1	0

Bemerkung 3.1.1. *Mit* elektrischen *Leitungen und echten Schaltern kann man nicht so leicht komplizierte Schaltungen bauen. Mit* elektronischen *Schaltern hingegen kann man auch Schaltungen bauen, in denen eine Leitung den Strom in mehreren anderen Leitungen schaltet. Mit dieser Technik kann man aus den drei Grundschaltungen Serienschaltung ($\wedge$), Parallelschaltung ($\vee$) und Negation ($\neg$) jede beliebige Schaltung bauen.*

Zum besseren Verständnis der Grundschaltungen bringen wir noch einen Vergleich aus dem „wirklichen Leben“. Wenn Sie als Abenteurer in einem Fantasy-Spiel in ein Haus eindringen müssen, dann werden Sie zuerst die Türen untersuchen. Besitzt eine Tür zwei Schlösser A und B, so müssen Sie A **und** B öffnen, um die Tür zu überwinden. Hat das Haus aber zwei Türen a und b, so müssen Sie a **oder** b öffnen, um einzudringen. Dies ist ein **einschließendes Oder**, denn wenn sie beide Türen aufbekommen, ist das bestimmt kein Hindernis für das Durchsuchen des Hauses — und falls Sie an der logischen Aufgabe mit den Türen und Schlössern scheitern, können Sie immer noch mit Hilfe der vollständigen Induktion ein Fenster im zweiten Stock einschlagen.

Es existieren vier einstellige Operatoren (wie $\neg$) und 16 mögliche binäre Operatoren (wie $\wedge$ oder $\vee$). über zwei dieser binären Operatoren wollen wir im Folgenden sprechen.

Beispiel 3.1.2. XOR. *Betrachten wir zunächst die Schaltwerttabelle*

a	b	$a \veebar b$
0	0	0
0	1	1
1	0	1
1	1	0

Diese zweistellige Operation heißt XOR (exklusives Oder, **ausschließendes Oder***). Sie entspricht der Bedeutung von „oder“ in der Umgangssprache:* Entweder a oder b *sind eingeschaltet — keinesfalls beide.*

WICHTIG: In der Mathematik ist es unbedingt notwendig, das Ausschließende der XOR-Operation zu betonen, wie etwa durch Einführen des Wortes „entweder“, um Verwechslungen mit der OR-Operation zu vermeiden, die ja als einschließende Oder einen Einser in der letzten Zeile der Schaltwerttabelle aufweist (vgl. auch Abschnitt 3.2.1).

Beispiel 3.1.3. NAND. *Interessanterweise gibt es eine Operation — übrigens sehr billig mittels Transistoren herstellbar — die allein ausreicht, um alle anderen Operationen und damit alle möglichen Schaltungen zu erzeugen. Diese binäre Operation hat die Schaltwerttabelle*

a	b	$a \bar{\wedge} b$
0	0	1
0	1	1
1	0	1
1	1	0

und trägt den Namen NAND *(negated AND, also negiertes Und). Der Zusammenhang mit den bereits definierten Operationen ist $a \bar{\wedge} b = \neg(a \wedge b)$.*

Bemerkung 3.1.4. *Wie kann man die bereits bekannten Grundoperationen mit Hilfe der NAND Operation zusammensetzen?*

(1) *Es gilt $\neg a = a \bar{\wedge} a$, wie wir an Hand der Schaltwerttabelle leicht überprüfen können:*

a	$a \bar{\wedge} a$	$\neg a$
0	1	1
1	0	0

(2) *Für die Oder-Verknüpfung erhalten wir* $a \vee b = (a \barwedge a) \barwedge (b \barwedge b)$*:*

a	b	$a \barwedge a$	$b \barwedge b$	$(a \barwedge a) \barwedge (b \barwedge b)$	$a \vee b$
0	0	1	1	0	0
0	1	1	0	1	1
1	0	0	1	1	1
1	1	0	0	1	1

(3) *Zuletzt stellen wir die Und-Verknüpfung ebenfalls durch drei NAND Operationen dar als* $a \wedge b = (a \barwedge b) \barwedge (a \barwedge b)$*. überprüfen wir die Richtigkeit wieder mit Hilfe der Schaltwerttabelle:*

a	b	$a \barwedge b$	$(a \barwedge b) \barwedge (a \barwedge b)$	$a \wedge b$
0	0	1	0	0
0	1	1	0	0
1	0	1	0	0
1	1	0	1	1

Eine wichtige Frage bei der technischen Herstellung von Schaltungen ist die folgende: Es sei festgelegt, bei welchen Schalterstellungen welche Leitungen Strom führen sollen und welche nicht; es sei also die Schalttafel gegeben. Was ist die einfachste Schaltung, die genau diese Schalttafel besitzt?

Diese Frage zu beantworten ist nicht ganz einfach. Es ist sicher, dass es eine Schaltung gibt, die der Schalttafel entspricht. Man kann sie auch immer konstruieren mit Hilfe der sogenannten **disjunktiven Normalform**. Es sei also eine Funktion f gegeben, deren Wert 0 oder 1 ist und von den binären Variablen $a_1, \dots, a_n$ abhängt. Möchte man eine Schaltung konstruieren mit n Schaltern, die den Variablen entsprechen, die immer den Wert $f(a_1, \dots, a_n)$ ergibt, so folgt man dem folgenden *Algorithmus*:

(1) Stelle die Schaltwerttabelle mit den Variablen links und dem gewünschten Funktionswert rechts auf.
(2) Streiche alle Zeilen, in denen $f(a_1, \dots, a_n)$ den Wert 0 hat.
(3) Ordne jeder der verbliebenen Zeilen eine Und-Verknüpfung von allen Variablen a_i zu, die in dieser Zeile den Wert 1 haben und von den Negationen $\neg a_j$ aller Variablen, die in dieser Zeile den Wert 0 haben.
(4) Verknüpfe alle gerade konstruierten Und-Glieder durch Oder-Verknüpfungen.

Beispiel 3.1.5. *Konstruieren wir die disjunktive Normalform zur Schaltwerttabelle*

a	b	c	$f(a,b,c)$	*Und-Verknüpfung*
0	0	0	1	$\neg a \wedge \neg b \wedge \neg c$
0	0	1	0	
0	1	0	1	$\neg a \wedge b \wedge \neg c$
0	1	1	1	$\neg a \wedge b \wedge c$
1	0	0	1	$a \wedge \neg b \wedge \neg c$
1	0	1	0	
1	1	0	0	
1	1	1	1	$a \wedge b \wedge c$

Die disjunktive Normalform ist dann

$$f(a,b,c) = (\neg a \wedge \neg b \wedge \neg c) \vee (\neg a \wedge b \wedge \neg c) \vee (\neg a \wedge b \wedge c) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c).$$

Die disjunktive Normalform ist übrigens nicht die einzige Möglichkeit, zu einer gegebenen Schaltwerttabelle eine Schaltung zu konstruieren. Es existiert zum Beispiel auch noch die **konjunktive Normalform**, die sich grob gesprochen dadurch auszeichnet, dass sie eine Und-Verknüpfung von Oder-Ausdrücken ist. Konstruiert wird sie mit einem analogen (inversen) Algorithmus:

(1) Stelle die Schaltwerttabelle mit den Variablen links und dem gewünschten Funktionswert rechts auf.
(2) Streiche alle Zeilen, in denen $f(a_1, \ldots, a_n)$ den Wert 1 hat.
(3) Ordne jeder der verbliebenen Zeilen eine Oder-Verknüpfung von allen Variablen a_i zu, die in dieser Zeile den Wert 0 haben und von den Negationen $\neg a_j$ aller Variablen, die in dieser Zeile den Wert 1 haben.
(4) Verknüpfe alle gerade konstruierten Oder-Glieder durch Und-Verknüpfungen.

Die Normalformen zu einem Ausdruck sind üblicherweise sehr kompliziert, und die Frage ist, ob man eine einfachere Schaltung konstruieren kann, die dieselbe Schaltwerttabelle ergibt. Tatsächlich können komplizierte Verknüpfungen mit Hilfe der folgenden Rechenregeln vereinfacht werden (vgl. Beispiel 3.1.8), die man leicht mit Hilfe der jeweiligen Schaltwerttabellen überprüfen kann.

Theorem 3.1.6. *Für die Operationen $\wedge$, $\vee$ und $\neg$ gelten die folgenden Rechenregeln.*

Kommutativgesetze:	$a \vee b = b \vee a$	$a \wedge b = b \wedge a$
Assoziativgesetze:	$a \vee (b \vee c) = (a \vee b) \vee c$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$
Distributivgesetze:	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
Verschmelzungsgesetze:	$a \vee (b \wedge a) = a$	$a \wedge (b \vee a) = a$
Idempotenzgesetze:	$a \vee a = a$	$a \wedge a = a$
Neutralitätsgesetze:	$a \vee 0 = a$	$a \wedge 1 = a$
Absorptionsgesetze:	$a \vee 1 = 1$	$a \wedge 0 = 0$
Komplementaritätsgesetze:	$a \vee \neg a = 1$	$a \wedge \neg a = 0$
	$\neg 0 = 1$	
	$\neg 1 = 0$	
Gesetz der doppelten Verneinung:	$\neg(\neg a) = a$	
Gesetze von De Morgan:	$\neg(a \vee b) = \neg a \wedge \neg b$	$\neg(a \wedge b) = \neg a \vee \neg b$

Beweis. Aufstellen der Schaltwerttabellen. □

Bemerkung 3.1.7. *Eine mathematische Struktur mit* 0, 1 *und drei Operationen $\wedge$, $\vee$ und $\neg$, die die Rechengesetze*

(1) *Kommutativgesetze*
(2) *Distributivgesetze*
(3) *Neutralitätsgesetze*
(4) *Komplementaritätsgesetze*

*erfüllt, heißt **Boolesche Algebra**. Alle anderen Rechengesetze aus Theorem 3.1.6 lassen sich aus diesen acht herleiten.*

Beispiel 3.1.8. *Mit Hilfe der Rechengesetze aus Theorem 3.1.6 können wir versuchen, die disjunktive Normalform aus Beispiel 3.1.5 zu vereinfachen.*

$$\begin{aligned}
f(a,b,c) &= (\neg a \wedge \neg b \wedge \neg c) \vee (\neg a \wedge b \wedge \neg c) \vee (\neg a \wedge b \wedge c) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c) = \\
&= \Big(\neg a \wedge \big((\neg b \wedge \neg c) \vee (b \wedge \neg c) \vee (b \wedge c)\big)\Big) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c) = \\
&= \Big(\neg a \wedge \big(((\neg b \vee b) \wedge \neg c) \vee (b \wedge c)\big)\Big) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c) = \\
&= \Big(\neg a \wedge \big((1 \wedge \neg c) \vee (b \wedge c)\big)\Big) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c) = \\
&= \Big(\neg a \wedge \big(\neg c \vee (b \wedge c)\big)\Big) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c) = \\
&= (\neg a \wedge \neg c) \vee (\neg a \wedge b \wedge c) \vee (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c) = \\
&= (\neg a \wedge \neg c) \vee (a \wedge \neg b \wedge \neg c) \vee (\neg a \wedge b \wedge c) \vee (a \wedge b \wedge c) = \\
&= (\neg a \wedge \neg c) \vee (a \wedge \neg b \wedge \neg c) \vee \big((\neg a \vee a) \wedge (b \wedge c)\big) = \\
&= (\neg a \wedge \neg c) \vee (a \wedge \neg b \wedge \neg c) \vee \big(1 \wedge (b \wedge c)\big) = \\
&= \big((\neg a \vee (a \wedge \neg b)) \wedge \neg c\big) \vee (b \wedge c) = \\
&= \big((\neg a \vee a) \wedge (\neg a \vee \neg b) \wedge \neg c\big) \vee (b \wedge c) = \\
&= \big(1 \wedge (\neg a \vee \neg b) \wedge \neg c\big) \vee (b \wedge c) = \\
&= \big((\neg a \vee \neg b) \wedge \neg c\big) \vee (b \wedge c) = \\
&= \big(\neg(a \wedge b) \wedge \neg c\big) \vee (b \wedge c) = \\
&= \neg\big((a \wedge b) \vee c\big) \vee (b \wedge c)
\end{aligned}$$

dies ist schon eine wesentlich kompaktere Formel, und an Hand der Schaltwerttabelle kann man leicht überprüfen, dass diese Formel eine äquivalente Schaltung beschreibt.

Beispiel 3.1.9. *Zwei weitere Beispiele binärer Operationen, die im folgenden noch wichtig sein werden sind die* Implikation *und die* Äquivalenz

a	b	$a \Rightarrow b$
0	0	1
0	1	1
1	0	0
1	1	1

und

a	b	$a \Leftrightarrow b$
0	0	1
0	1	0
1	0	0
1	1	1

In elementaren Operationen ausgedrückt finden wir die disjunktive Normalform

$$a \Leftrightarrow b = (\neg a \wedge \neg b) \vee (a \wedge b),$$

und für $a \Rightarrow b$ vereinfachen wir die disjunktive Normalform zu

$$\begin{aligned}
\underline{a \Rightarrow b} &= (\neg a \wedge \neg b) \vee (\neg a \wedge b) \vee (a \wedge b) = \big(\neg a \wedge (\neg b \vee b)\big) \vee (a \wedge b) = \\
&= (\neg a \wedge 1) \vee (a \wedge b) = \neg a \vee (a \wedge b) = (\neg a \vee a) \wedge (\neg a \vee b) = 1 \wedge (\neg a \vee b) = \underline{\neg a \vee b}.
\end{aligned}$$

3.2. Aussagen, Logik

In der Mathematik werden Begriffe und Regeln der Logik verwendet, um das Theoriegebäude zu erbauen.

Die Mathematik arbeitet dabei mit Aussagen. Das hervorstechende Merkmal einer Aussage ist dabei:

Eine **Aussage** ist entweder **wahr** oder **falsch**.

Beispiel 3.2.1. *Beispiele für Aussagen sind etwa:*

- 7 *ist größer als* 5, *oder in Zeichen* $7 > 5$.
- *Es gibt unendlich viele Primzahlen.*
- *Wale sind Säugetiere.*

Die folgenden Sätze sind keine *Aussagen:*

- *Wer geht heute ins Clubbing?*
- $5 + 8$

Eine Besonderheit der Mathematik besteht darin, dass zu Beginn als Fundament der gesamten Wissenschaft eine Reihe von Aussagen, die **Axiome** als *wahr angenommen* werden. Danach werden ausgehend von diesen Aussagen weitere **wahre** Aussagen abgeleitet. Gewissermaßen könnte man also sagen, dass sich die Mathematiker eine eigene streng logisch aufgebaute „Welt“ erschaffen, in der sie niemals lügen (d.h. sie machen nur wahre Aussagen). Die Gültigkeit dieser Aussagen wird dadurch sicher gestellt, dass sie durch definierte logische Umformungsschritte aus bereits als wahr erkannten Aussagen abgeleitet werden (auch was ableiten bedeutet, kann man exakt definieren — das ist aber Gegenstand der Vorlesungen aus dem Gebiet „Logik“). Diesen Vorgang nennt man **beweisen**.

3.2.1. Und oder oder, oder nicht? Nachdem Aussagen *zwei* mögliche „Werte“ haben können, kann man sie mit den gleichen Augen betrachten wie Schalter oder Stromleitungen, und man kann genau dieselben Verknüpfungen von Aussagen machen wie man aus Schaltern und Leitungen Schaltungen bauen kann. Man beachte, dass bei der Untersuchung von Aussagen an Stelle von Schaltungen die Schaltwerttabellen als **Wahrheitstafeln** bezeichnen werden.

Setzen wir in den Tabellen für **wahr** den Wert **1** und für **falsch** den Wert **0** und werfen wir noch einmal einen Blick auf die drei Grundoperationen, und versuchen wir zu klären, was sie im Zusammenhang mit Aussagen bedeuten.

3.2.1.1. Oder ($\vee$). Bei der Definition der Oder-Verknüpfung muss man aufmerksam sein, und daher wollen wir sie zu Beginn behandeln.

Die Aussage

Peter ist Professor **oder** Student.

bedeutet, dass Peter Professor oder Student *oder beides* ist. Das Oder in der Mathematik ist ein *einschließendes Oder* — im Gegensatz zum umgangssprachlichen Gebrauch. Das entspricht auch der Tabelle zur Verknüpfung $\vee$.

Ein Oder in einer mathematische Aussage ist immer als einschließenden Oder zu verstehen. Möchte man in einer mathematischen Aussage ein Oder so verstanden wissen, dass es, ähnlich zur Umgangssprache, das „oder beides“ ausschließt, möchte man also statt einem einschließenden Oder ein ausschließendes Oder verwenden, so muss man das explizit machen, indem man beispielsweise formuliert:

Peter ist **entweder** Professor **oder** Student.

und eventuell sogar hinzufügt:

Aber nicht beides.

Merke: Hat man zwei Aussagen p und q, dann ist $p \vee q$ (in Sprache p *oder* q) wahr, wenn p *oder* q *oder beide* wahr sind.

So ist den meisten SchülernInnen und Studierenden die Aussage, „Um eine Prüfung zu bestehen, muss man viel lernen *oder* gut schummeln“ allzu gut bekannt.

3.2.1.2. Und ($\wedge$). Während die Oder-Verknüpfung einigen Erklärungsbedarf nach sich gezogen hat, ist die **Und-Verknüpfung** aus der Umgangssprache intuitiv klar.

Was bedeutet die folgende Aussage?

Die Zahl 6 ist durch 3 teilbar **und** die Zahl 6 ist durch 2 teilbar.

Klarerweise ist diese Aussage eine Und-Verknüpfung ($\wedge$) der beiden Aussagen „6 ist durch 3 teilbar“ und „6 ist durch 2 teilbar“. Beide diese Aussagen sind wahr, also ist auch die Und-Verknüpfung der beiden Aussagen wahr, und damit ist auch die Aussage von oben.

Merke: Hat man zwei Aussagen p und q, dann ist $p \wedge q$ (in Sprache p *und* q) wahr, wenn p und q *beide* wahr sind.

Im Gegensatz zu beliebigen Prüfungen seien die StudentInnen aber gewarnt, dass für die Prüfung zu dieser Vorlesung die Aussage gilt: „Zum Bestehen der Einführungsprüfung müssen die Studierenden viel lernen *und* gut schummeln.“

3.2.1.3. Negation ($\neg$). Die Negation einer Aussage ist klarerweise deren Verneinung. Wenn wir etwa die Negation der Aussage

Der Fußboden ist blau.

bilden, so erhalten wir natürlich

Der Fußboden ist **nicht** blau.

ACHTUNG: „Der Fußboden ist gelb“ ist **keine** Verneinung der obigen Aussage!

Interessant wird es, wenn wir Aussagen verneinen, in denen bereits Verknüpfungen $\vee$ oder $\wedge$ vorkommen. Dann müssen wir achtgeben. Hier helfen uns die Untersuchungen aus Abschnitt 3.1 weiter, denn in Theorem 3.1.6 haben wir die Regeln von De Morgan kennen gelernt, die uns Aufschluss darüber geben, was passiert, wenn man Und- und Oder-Verknüpfungen negiert. Betrachten wir einige Beispiele:

- Verneint man
  Der Fußboden ist blau und die Decke ist grün.
  so erhält man
  Der Fußboden ist nicht blau **oder** die Decke ist nicht grün.
- Will man dagegen die Aussage
  Die Zahl 3 ist eine Primzahl oder die Zahl 4 ist eine Primzahl.
  negieren, so muss man folgendermaßen formulieren.
  Die Zahl 3 ist keine Primzahl **und** die Zahl 4 ist keine Primzahl.

Merke: Will man $\wedge$- oder $\vee$-Verknüpfungen von Aussagen verneinen, so verneint man die Einzelaussagen und tauscht dann $\wedge$ gegen $\vee$ aus. Es gelten also die Regeln von De Morgan

$$\neg(p \wedge q) = \neg p \vee \neg q \qquad \neg(p \vee q) = \neg p \wedge \neg q.$$

Die letzte wichtige Regel für Negationen ist schließlich, dass doppelte Verneinungen wegfallen:

Wale sind nicht keine Säugetiere.

bedeutet dasselbe wie

Wale sind Säugetiere.

Merke: Doppelte Verneinungen fallen weg. Es gilt $\neg(\neg p) = p$.

Beispiel 3.2.2. *Trifft ein Informatiker seinen Freund, der mit rauchendem Kopf verzweifelt vor dem Computer sitzt. Weil er aus ihm kein vernünftiges Wort herausbringt, blickt er kurz auf den Monitor und liest:* `Nicht alle Dateien nicht löschen? (J/N)`.

3.2.2. Implikation und Äquivalenz. Wie versprochen tauchen die in Beispiel 3.1.9 eingeführten binäre Operationen hier an wichtiger Stelle wieder auf.

3.2.2.1. Die Impliaktion (⇒). Wir haben schon diskutiert, dass in der Mathematik neue Aussagen aus bereits bekannten Resultaten *abgeleitet* werden. Werfen wir einen genaueren Blick auf diesen Vorgang. **Alle** mathematischen Sätze haben bei genauer Betrachtung das folgende Aussehen:

Theorem 3.2.3. *Aus* den Voraussetzungen *folgt* das Resultat.

Genauer: Ein Theorem ist **eine Aussage** der Form: Voraussetzungen ⇒ Resultat. Der Beweis stellt sicher dass diese Aussage **wahr** ist.

Was das bedeutet, können wir erst erkennen, wenn wir die Wahrheitstafel der ⇒-Operation noch einmal betrachten.

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Wir erkennen, dass es nur *einen Fall* gibt, in dem die Aussage einer Implikation *falsch* ist, nämlich wenn die Voraussetzung wahr aber die Folgerung falsch ist. Das entspricht durchaus unserer Intuition. Ebenso steht wohl die letzte Zeile der Wahrheitstabelle außer Diskussion: Wenn die Voraussetzung und Resultat wahr ist, dann ist auch die Implikation wahr.

Eine spezielle Betrachtung verdienen die beiden Fälle, in denen p, also die Voraussetzung, falsch ist. In diesen Fällen ist die Aussage der Implikation nämlich wahr unabhängig vom Wahrheitswert des Resultats („ex falso quodlibet“ — lat. aus falschem wie es beliebt). Diese mathematische Definition widerspricht ein wenig der sprachlichen Intuition und es hat sich gezeigt, dass diese Tatsache zu Beginn meist (philosophische) Probleme bereitet.

Überlegen wir: Der Ergebniswert kann in beiden Fällen nur 0 oder 1 sein, denn eine dritte Möglichkeit kennt die formale (zweiwertige) Logik nicht („tertium non datur!“). Ein pragmatischer Standpunkt wäre nun zu sagen: „Wir wollen möglichst viele wahre Aussagen in unseren Theorien haben, und daher setzen wir an beide Stellen 1.“ Das macht Sinn, denn wir wollen mit dem Theorem nur Aussagen machen über Fälle, in denen die Voraussetzungen erfüllt sind, und alle anderen Fälle wollen wir nicht betrachten. Dann soll das Theorem immer noch wahr sein, auch wenn die Voraussetzungen einmal nicht erfüllt sein sollten.

Schließlich wollen wir ein Beispiel betrachten, das aufzeigt, dass die Wahrheitstabelle der Implikation im täglichen Leben durchaus eine Entsprechung findet. Wir betrachten die folgende Aussage.

(∗) Es wird ein Stein durch die Glasscheibe geworfen,
und daher zerbricht sie.

Diese Aussage steht, denke ich, außer Zweifel. Sie ist also wahr. Analysieren wir die Sache genauer. Wir haben die folgenden Aussagen:

p: Ein Stein wird durch die Glasscheibe geworfen.
q: Die Glasscheibe zerbricht.
$p \Rightarrow q$: Ein Stein wird durch die Glasscheibe geworfen, und daraus folgt, dass die Glasscheibe zerbricht.

Die Aussage $p \Rightarrow q$ ist eine etwas deutlichere Formulierung unserer Beispielaussage $(*)$ von oben, deren Wahrheit wir akzeptiert haben. Nun gehen wir alle Fälle unserer Wahrheitstabelle durch:

$p = 0, q = 0$: *Kein Stein wird durch die Glasscheibe geworfen. Die Glasscheibe zerbricht nicht.* Dies ist mit der Wirklichkeit durchaus verträglich, und widerspricht nicht im Mindesten unserer Beispielbehauptung $(*)$.

$p = 1, q = 1$: *Ein Stein wird durch die Glasscheibe geworfen. Die Glasscheibe zerbricht.* Auch das ist ein üblicher Vorgang (nicht das Werfen aber das darauf folgende Zerbrechen). Auch in diesem Fall entsteht kein Zweifel an $(*)$.

$p = 0, q = 1$: *Kein Stein wird durch die Glasscheibe geworfen. Die Glasscheibe zerbricht.* Dieser Fall bereitet üblicherweise Schwierigkeiten. Doch bei genauerer Betrachtung verblasst das Problem schnell. Vielleicht haben wir die Glasscheibe etwa mit einem Eisenträger durchstoßen. Die Scheibe ist kaputt ohne dass ein Stein geflogen wäre. Was der Scheibe auch immer passiert ist, genau können wir das aus dem Wahrheitsgehalt der Aussagen p und q nicht ableiten, die Tatsache, dass $(*)$ wahr ist, wird davon nicht berührt.

$p = 1, q = 0$: *Ein Stein wird durch die Glasscheibe geworfen. Die Glasscheibe zerbricht nicht.* Für einen solchen Fall fände ich keine Erklärung — Magie vielleicht? In der wirklichen Welt tendieren Scheiben zu zerbrechen, wenn man Steine durchwirft. Sollte aber tatsächlich der Fall eintreten, dass ein Stein geworfen wird, er durch die Scheibe fliegt und dann die Scheibe noch ganz ist, dann haben wir ein Problem. In diesem einen Fall müssten wir unsere Überzeugung aufgeben, dass $(*)$ gilt. Die Aussage $(*)$ wäre also tatsächlich *falsch.*

Wir haben also die Wahrheitswerte der Tabelle für $\Rightarrow$ in unserem Beispiel auf natürliche Weise wiedergefunden.

Alternativ dazu könnten wir versuchen herauszufinden, was es bedeutet, wenn wir die Ergebniswerte in den ersten beiden Zeilen anders setzen. Betrachten wir die anderen möglichen Fälle:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

p	q	q
0	0	0
0	1	1
1	0	0
1	1	1

Der erste Fall ist die Und-Verknüpfung der Aussagen p und q. Wir hätten also nur dann eine gültige Folgerung, wenn p und q beide wahr sind. Der Satz: „Das Quadrat einer geraden Zahl ist gerade.“ wäre also nicht wahr sondern hätte keinen zuordenbaren Wahrheitswert — das ist zumindest unpraktisch.

Der zweite Fall ist die Äquivalenz. Auch das ist ein wenig zu restriktiv. In diesem Fall wäre der Satz „Sind zwei Zahlen gleich, dann sind auch ihre Quadrate gleich.“ nicht wahr, denn $2 \neq -2$ aber $2^2 = (-2)^2$.

Im letzten Fall stimmen die Wahrheitswerte des Theorems mit denen von q, also denen des Resultates überein, und der Wahrheitsgehalt der Voraussetzung wird gar nicht betrachtet. Das ist ebenfalls unpraktisch; auch in diesem Fall wäre der Satz über die Quadrate gerader Zahlen nicht wahr.

Wir sehen also, dass vieles dafür spricht, die Implikation so und nicht anders zu definieren. Alle die jetzt noch nicht überzeugt sind, seien dazu angehalten, die Tatsache einfach zu akzeptieren und sich daran zu gewöhnen.

Nachdem Schlussfolgerungen *das* Instrument der Mathematik sind, kommen sie in mathematischen Texten ausgesprochen oft vor. Deshalb haben sich auch eine Reihe von Standardformulierungen ausgebildet, die an Stelle der Formulierung „daraus folgt“ angewendet werden können.

- **also**; **auf Grund** von; das **bedeutet**, dass; unter **Berücksichtigung** von; **daher**; **damit**; es **ergibt** sich; daraus **erhalten** wir; dies hat zur **Folge**; man kann **folgern**; wir **folgern**; **folglich**; genauer **gesagt**; dies **impliziert**; **insbesondere**; dies hat zur **Konsequenz**; **mithin**; dies lässt sich **schreiben** als; wir **sehen**; **somit**; ein Spezialfall hiervon ist; nach **Umformung** ergibt sich; mit anderen **Worten**; es **zeigt** sich, dass,...

Es haben zwar nicht alle diese Formulierungen dieselbe Bedeutung, doch wenn Sie ein bisschen überlegen, wird es Ihnen nicht schwer fallen, vielleicht mit ein wenig Erfahrung, die feinen Unterschiede herauszuarbeiten.

Gut ist auch, wenn Sie Ihre Leserin oder Ihren Hörer darauf hinweisen, warum eine Folgerung richtig ist.

- nach **Annahme**; **auf Grund** von Satz 4.29; unter **Berücksichtigung** der Theorie der...; **da** V endlich dimensional ist; aus der **Definition** ergibt sich; **per definitionem** ist; nach **Voraussetzung**; **wegen** Lemma 12.2; **weil** f stetig ist...

Zuletzt können Sie noch den Aufwand verdeutlichen, der benötigt wird, um ein Resultat nachzuvollziehen.

- durch **einfaches Ausrechnen**; durch **genaues Hinsehen**; wie man **leicht sieht**; **offenbar**; **offensichtlich**; durch **technische und uninteressante Abschätzungen**; durch **triviale und langweilige Rechnung**; **trivialerweise**; durch **mühsame Umformungen**; durch **überprüfen der Wahrheitstabellen**;...

Verjuxen Sie nicht den Vertrauensvorschuss Ihrer LeserIn durch falsche Angaben über den Aufwand. Behaupten Sie grundsätzlich nicht, dass etwas *leicht* einzusehen ist, wenn Sie mehr als 15 Minuten gebraucht haben, um es selbst einzusehen.

Zum Gebrauch des Wortes **trivial** ist noch zu sagen, dass die wenigsten Schritte in der Mathematik tatsächlich trivial sind. Trivial ist ein Beweisschritt *nur* dann, wenn er unmittelbar folgt (etwa direkt durch Anwendung einer Definition). Steckt ein, wenn auch noch so leicht einzusehender Beweis hinter dem Schritt, so ist er schon nicht mehr trivial.

Übrigens existiert noch eine zweite, technische Bedeutung des Wortes trivial in der Mathematik, nämlich als Adjektiv wie in

> Die **trivialen** Teiler einer natürlichen Zahl n sind 1 und n.

oder

> Ein homogenes lineares Gleichungssystem hat immer zumindest eine Lösung, nämlich die **triviale**.

Hier bedeutet trivial ein oder mehrere ausgezeichnete Objekte, die nach Definition immer existieren aber meist uninteressant sind.

Wollen wir einen Satz beweisen, so müssen wir sicher stellen, dass seine Aussage wahr ist. Die Wahrheitstabelle gibt uns dazu zwei Möglichkeiten (vgl. auch Abschnitt 2.1).

(1) Wir können annehmen, dass die Voraussetzungen (dies sind selbst Aussagen) gelten, dass also p wahr ist, und zeigen, dass dann das Resultat (die Aussage q) ebenfalls wahr ist. Beweise dieser Art nennt man **direkte Beweise**.
(2) Alternativ können wir annehmen, dass das Resultat (q) *falsch* ist und dann daraus folgern, dass die Voraussetzungen (die Aussage p) ebenfalls falsch sind. Beweise dieser Art nennt man **indirekte Beweise**. Dieses Beweisprinzip funktioniert, da

die Aussage des Satzes bei falschem q nur dann wahr ist, wenn auch p falsch ist. Ist jedoch q wahr, so kann p beliebig sein.

Nachdem schon einige direkte Beweise (z.B. die Induktionsbeweise) vorgekommen sind, betrachten wir hier nur ein weiteres Beispiel für einen indirekten Beweis.

Theorem 3.2.4. *Die Zahl $\sqrt{2}$ ist irrational.*

Beweis. Die Aussage des Satzes als Implikation aufgeschrieben lautet:

Ist q eine rationale Zahl, so gilt $q \neq \sqrt{2}$.

Wir führen einen indirekten Beweis. Davor schreiben wir noch einmal alle Voraussetzungen an, die wir verwenden wollen.

Für jede rationale Zahl q gibt es teilerfremde ganze Zahlen m und n mit $q = \frac{m}{n}$, und jede Bruchzahl ist rational. Daher ist $q \in \mathbb{Q}$ gleichbedeutend damit, dass q als Bruch zweier teilerfremder ganzer Zahlen darstellbar ist.

Wir können die Aussage des Satzes also auch folgendermaßen formulieren: Sind m und n zwei teilerfremde ganze Zahlen, so gilt $\frac{m}{n} \neq \sqrt{2}$.

Für den indirekten Beweis müssen wir das Resultat verneinen, also nehmen wir an, dass $\frac{m}{n} = \sqrt{2}$. Daraus reicht es zu folgern, dass m und n nicht teilerfremde ganze Zahlen sind.

Beweisen wir dies. Sei

$$\begin{aligned}\frac{m}{n} &= \sqrt{2}\\ \frac{m^2}{n^2} &= 2\\ m^2 &= 2n^2.\end{aligned}$$

Dies bedeutet aber, dass m^2 gerade ist, und da das Quadrat einer ungeraden Zahl ungerade ist, muss folglich m selbst gerade sein. Damit können wir m aber schreiben als $m = 2k$ und einsetzen,

$$\begin{aligned}(2k)^2 &= 2n^2\\ 4k^2 &= 2n^2\\ 2k^2 &= n^2.\end{aligned}$$

Wir sehen, dass auch n^2 und damit n gerade sind. Nachdem wir jetzt bewiesen haben, dass n und m beide gerade sind, können sie nicht länger teilerfremd sein (sie sind als gerade Zahlen beide durch 2 teilbar). Dies widerlegt unsere Voraussetzung, und der indirekte Beweis ist geglückt. □

Im Zusammenhang mit Implikationen tauchen in mathematischen Texten oft die die Wörter **notwendig** und **hinreichend** auf. Wenn A und B Aussagen sind und $A \Rightarrow B$ gilt, so heißt A *hinreichend* für B, und B heißt *notwendig* für A. Lernen Sie das auswendig und versuchen Sie nicht die Bedeutung zu hinterfragen. Beispiele sind:

- Notwendig dafür, dass eine Zahl $n > 2$ eine Primzahl ist, ist, dass sie ungerade ist.
- Hinreichend für die Stetigkeit einer Funktion ist ihre Differenzierbarkeit.

Nun zu **dann, wenn** und **nur dann, wenn**:

- „A gilt dann, wenn B gilt“ bedeutet: $A \Leftarrow B$.
- „A gilt nur dann, wenn B gilt“ heißt hingegen $A \Rightarrow B$.

Um ein Beispiel für letztere Formulierung zu geben, betrachten wir die Aussagen: A sei „Ein neuer Papst wird gewählt.“, B sei „Der alte Papst ist gestorben.“. Die Formulierung

„Ein neuer Papst wird **nur dann** gewählt, **wenn** der alte gestorben ist“ entspricht dann der Folgerung $A \Rightarrow B$. Wenn wir den Satz umdrehen, so ergibt das die Aussage „Wenn ein neuer Papst gewählt wird, dann ist der alte jedenfalls gestorben.“ Seien Sie in jedem Fall vorsichtig, wenn Sie die Formulierungen mit dann und wenn benutzen.

3.2.2.2. Die Äquivalenz ($\Leftrightarrow$). Eine zweite Klasse von Sätzen der Mathematik hat die logische Äquivalenz (die Operation $\Leftrightarrow$) als Grundlage. Eine leichte Rechnung mit den Wahrheitstabellen ergibt $a \Leftrightarrow b = (a \Rightarrow b) \wedge (b \Rightarrow a)$.

Die typische Aussage eines Äquivalenzsatzes sieht so aus

Theorem 3.2.5. *Resultat 1 gilt* ***genau dann, wenn*** *Resultat 2 gilt.*

Auch an Stelle der Standardaussage „das gilt genau dann, wenn“ haben sich einige andere Formulierungen eingebürgert.

- das ist **äquivalent** zu; dies ist **gleichbedeutend** mit; dies ist **gleichwertig** mit; die beiden Aussagen **gehen auseinander hervor**; dies ist **notwendig und hinreichend** für; **dann und nur dann**...

Die übrigen Hinweise, wie Aufwandsangabe und Erwähnung der Begründung, die wir bei den Implikationen schon besprochen haben, gelten natürlich auch für Äquivalenzen.

Äquivalenzen kommen in der Mathematik sehr häufig vor. Die Äquivalenz zweier Aussagen A und B beweist man dabei so wie es von der obigen Formel suggeriert wird. Man weist die Gültigkeit von $A \Rightarrow B$ nach *und* auch die der *umgekehrten Richtung* $B \Rightarrow A$.
WICHTIG: Der Beweis einer Äquivalenz ist erst dann vollendet, wenn *beide* Implikationsrichtungen gezeigt sind. Um dies zu verdeutlichen betrachten wir die folgende Aussage.

Proposition 3.2.6. *Eine Zahl ist genau dann gerade, wenn ihr Quadrat gerade ist.*

Beweis. Umformuliert bedeutet die Aussage für eine beliebige natürliche Zahl n

$$n \text{ gerade } \Leftrightarrow n^2 \text{ gerade }.$$

Wir müssen also beide Implikationen beweisen und beginnen mit der „Hinrichtung“.
$\Rightarrow$: Diese Implikation ist aber genau die Aussage von Proposition 2.1.1, sodass wir nichts mehr zu beweisen haben.

Es bleibt uns die „Rückrichtung“ zu zeigen.
$\Leftarrow$: Genauer ist zu zeigen n^2 gerade $\Rightarrow n$ gerade.
Das beweisen wir indirekt. Sei also n ungerade, d.h. $n = 2k + 1$ für eine ganze Zahl k. Dann ist $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ und n^2 somit ungerade.

Nachdem wir beide Implikationen bewiesen haben, gilt die im Satz behauptete Äquivalenz. □

Ganz nebenbei schließt die „Rückrichtung“ der Proposition mittels der Äquivalenz $(\neg p \Rightarrow \neg q) \Leftrightarrow (q \Rightarrow p)$ (Diese ist ganz einfach mittels Wahrheitstabellen nachzuweisen.) auch die (kleine) Lücke im Beweis von Theorem 3.2.4 (Ganz ehrlich: Haben Sie diese bemerkt?).

Hat man mehr als zwei Aussagen, von denen man die Äquivalenz zeigen möchte, etwa A, B und C, so kann man einen sogenannten **Zirkelschluss** $A \Rightarrow B$, $B \Rightarrow C$, $C \Rightarrow A$ durchführen, um die Äquivalenz der Aussagen sicher zu stellen. Vorsicht: Solche Zirkelschlüsse beweisen nur die Äquivalenz von Aussagen. über deren Wahrheitswert wird durch solch einen Beweis nichts bekannt.

Interessant ist noch die Verneinung einer Äquivalenzen. Mit Hilfe der Wahrheitstabelle sehen wir nämlich $\neg(p \Leftrightarrow q) = p \veebar q$, also „$p$ ist nicht äquivalent zu q“ ist gleichbedeutend mit „entweder p oder q“. Umgekehrt ist natürlich die Verneinung einer Entweder-Oder-Aussage eine Äquivalenz.

3.2.3. Quantoren. Viele mathematische Aussagen gelten für bestimmte oder auch alle Objekte einer Gattung; diesen Formulierung wollen wir uns nun zuwenden.

3.2.3.1. Der Allquantor (∀). Ein Großteil der mathematischen Theorien handelt von Strukturen und Regeln. Ein Beispiel für Regeln sind Rechengesetze, die etwa **für alle** Objekte eine bestimmten Menge gelten. In diesem Fall verwenden wir das Zeichen ∀, den **Allquantor**.

Die Formulierung „$\forall x \in M :$" bedeutet „Für alle x in M gilt…".

Andere Formulierung für dieselbe Zeichenfolge sind etwa

- Für jedes x in M gilt…
- Sei $m \in M$ beliebig. Dann gilt…
- Für eine beliebiges Element von M gilt…
- Ist $m \in M$, dann gilt…
- Jedes Element aus M erfüllt…
- Die Elemente von M erfüllen…
- $\bigwedge m \in M$.

Bezieht sich ein ∀ auf mehrere Variable auf einmal, so verwendet man auch oft „je zwei", „je drei", …

- Durch je zwei (verschiedene) Punkte P und Q geht genau eine Gerade.

bedeutet nur „Für jeden Punkt P und jeden Punkt $Q \neq P$ gibt es genau eine…

Der Unterschied zwischen „alle" und „jedes" besteht meist darin, dass „für alle" auf die Gesamtheit aller Objekte abzielt, während „jedes" ein beliebige herausgegriffenes Objekt meint:

- Alle bijektiven Funktionen sind invertierbar.
- Für jede bijektive Funktion f existiert die Umkehrfunktion, welche wir mit f^{-1} bezeichnen.

Merke: Um eine Allaussage zu widerlegen genügt die Angabe *einer* Gegenbeispieles.
Behauptung: Alle ungeraden Zahlen sind Primzahlen. Dies ist natürlich falsch, denn die Zahl $9 = 3 \cdot 3$ ist eine ungerade Zahl, die keine Primzahl ist.

3.2.3.2. Existenz (∃ und ∃!). Oftmals wird eine mathematische Aussage nicht über alle Elemente einer Menge getroffen, sondern es wird nur die **Existenz** eines bestimmten Objektes behauptet.

Für ein homogenes lineares Gleichungssystem existiert eine Lösung.

Die Formulierung in Zeichen mit Hilfe des **Existenzquantors** ist „$\exists x \in M :$" und in Worten: „Es existiert ein x in M mit…". Diese Aussage bedeutet, dass es **mindestens ein** Element in M gibt mit…

Möchte man in Zeichen ausdrücken dass es **genau ein** Element in M gibt mit…, so schreibt man „$\exists! x \in M :$".

Auch für die Existenzaussage gibt es viele Formulierungen.

- Es gibt ein $x \in M$ mit…
- Jede monotone beschränkte Folge reeller Zahlen hat einen Häufungspunkt (d.h. es existiert ein Häufungspunkt)
- Für ein geeignetes x ist $\log x \leq x$. Das bedeutet nichts anderes als, dass solch ein x existiert.

- Im allgemeinen gilt nicht, dass $x^2 + x + 41$ eine Primzahl ist. (Das wiederum heißt, dass ein x existiert, sodass $x^2 + x + 41$ keine Primzahl ist.)
- $\bigvee x \in M$:

Merke: Die Verneinung einer Existenzaussage ist eine Allaussage und umgekehrt.

- Die Verneinung von „Alle Kinder hassen die Schule" ist „Es gibt ein Kind, das die Schule nicht hasst".
- Die Verneinung von „Es gibt einen klugen Assistenten" ist „Alle Assistenten sind dumm."

In Zeichen ausgedrückt, gilt für die Verneinungen:

$$\neg(\forall x \in M : A(x)) \quad \text{entspricht} \quad \exists x \in M : \neg A(x),$$

wenn A eine Aussage über Elemente von M ist, etwa $A(x) = (x < 7)$. Für den Existenzquantor gilt analoges:

$$\neg(\exists x \in M : A(x)) \quad \text{entspricht} \quad \forall x \in M : \neg A(x).$$

ACHTUNG: Die Verneinung einer Existiert-Genau-Ein-Aussage ist *keine* Allaussage! Man muss komplizierter formulieren. Die Verneinung von „Ich habe genau einen Bruder." ist am kürzesten formuliert „Ich habe nicht genau einen Bruder." Möchte man das „*nicht*" zur Aussage befördern, dann muss man mit einer Fallunterscheidung operieren: „Ich habe keinen Bruder oder mehr als einen Bruder."

3.2.3.3. Reihenfolge von Quantoren ($\forall\exists$ oder $\exists\forall$?). Seien Sie vorsichtig, wenn mehr als ein Quantor $\forall$ oder $\exists$ in einem Satz vorkommt. Dabei kommt es nämlich wesentlich auf die Reihenfolge an.

Beispiel 3.2.7. *Sei M die Menge aller Männer und F die Menge aller Frauen. Die Aussage $h(m, f)$ sei „m ist verliebt in f". Unter diesen Voraussetzungen machen Sie sich die Bedeutung der beiden Aussagen klar. Danach werden Sie immer auf die Reihenfolge der Quantoren achten.*

(1) $\forall m \in M : \exists f \in F : h(m, f)$.
(2) $\exists f \in F : \forall m \in M : h(m, f)$.

Mitunter ist es aus der Formulierung nur schwer zu erkennen, dass ein $\exists\forall$ oder ein $\forall\exists$ versteckt ist. Dann ist es besonders wichtig, die Formulierung sehr lange zu prüfen und eventuell auch formalisiert noch einmal aufzuschreiben.

- „Der Wert von $y = f(x)$ ist unabhängig von der Wahl von x" ist gleichbedeutend mit $\exists y : \forall x : f(x) = y$.

3.3. Mengen

Mengen sind die erste mathematische Struktur, die wir einführen wollen. An diesem Punkt stoßen wir also zum ersten Mal auf das in der Einleitung erwähnte Grundprinzip der Mathematik: Definition und Untersuchung von *Strukturen*.

Ein Großteil der mathematischen Theorien ist darauf aufgebaut, Objekte mit bestimmten Eigenschaften und deren Beziehungen untereinander zu untersuchen. Strukturen können neben einander existieren oder aber auf einander aufbauen, d.h. sie sind Spezialisierungen oder Kombinationen von bereits bestehenden Strukturen.

Die Basisstruktur für die meisten Gebiete der Mathematik ist diejenige der *Mengen und Abbildungen*, hinzu kommen noch *Relationen*.

3.3.1. Naive Mengenlehre. Bevor wir in Abschnitt 3.4.1 kurz einen logisch exakten Zugang zur Mengenlehre skizzieren, wollen wir uns hier, aus Gründen der Motivation und des besseren Verständnisses, auf den Zugang von Georg Cantor (1845–1918) zurückziehen, den dieser gegen Ende des 19. Jahrhunderts erstmals formuliert hat:

> Unter einer **Menge** verstehen wir jede Zusammenfassung S von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die **Elemente** von S genannt werden) zu einem Ganzen.

Vorstellen kann man sich eine Menge gewissermaßen als einen Sack. Die Elemente sind die Gegenstände, die sich in dem Sack befinden. Natürlich können Mengen andere Mengen enthalten so, wie sich auch weitere Säcke innerhalb eines Sackes befinden können.

Beispiel 3.3.1. *Bilden kann man etwa die folgenden Mengen.*

- *Die Menge aller Studierenden im Hörsaal.*
- *Die Menge der natürlichen Zahlen.*
- *Die Menge der Lösungen einer Ungleichung.*
- *Die **leere Menge** („ein leerer Sack“).*

Der Gebrauch des bestimmten Artikels ist in der Mathematik äußerst eingeschränkt. Es gibt eine feste Regel, die nie gebrochen werden darf.

> **Ein bestimmter Artikel darf nur dann verwendet werden, wenn es klar ist, dass das fragliche Objekt eindeutig bestimmt ist.**

So ist es unzulässig zu formulieren

- … ~~der~~ Teiler von 6 (denn es gibt 1, 2, 3 und 6).
- … ~~die~~ Matrix, die einer lineare Abbildung f entspricht… (denn sie ist nicht eindeutig).
- … ~~die~~ Basis des $\mathbb{R}^3$.

Richtig wäre es dagegen zu sagen:

- Sei n **die** kleinste natürliche Zahl, die …
- … **die** leere Menge.
- … **die** Menge der natürlichen/ganzen/rationalen/reellen Zahlen.

Bevor wir den Begriff „Menge“ weiter studieren, machen wir einen kurzen historischen Exkurs, denn die Geschichte der Mengenlehre unterscheidet sich grundlegend von der fast aller anderen Gebiete der Mathematik, wie etwa in [**O’Connor, Robertson 1996**] dargestellt.

üblicherweise geht die mathematische Entwicklung verschlungene Wege. Theorien werden über Jahrhunderte hinweg von mitunter konkurrierenden Schulen von Mathematikern gepflegt und weiterentwickelt. Plötzlich ist die Theorie an einem Punkt angelangt, an dem oftmals mehrere Mathematiker gleichzeitig einen Geistesblitz haben und ein bedeutendes Resultat entdeckt wird. Die Mengenlehre steht dem vollständig entgegen. Bis auf wenige zusätzliche Arbeiten ist sie die Entwicklung eines einzigen Mannes, Georg Cantor.

Die „Unendlichkeit“ hat die Philosophie (und damit die Mathematik) jedenfalls seit Zeno von Elea (ca. 490-425 v.Chr), also seit etwa 450 v.Chr. beschäftigt. Später haben sich bedeutende Philosophen, unter anderen Aristoteles (384–322 v.Chr.), René Descartes (1596–1650), Georeg Berkeley (1685–1753), Gottfried W. Leibniz (1646–1716), aber auch Albert von Sachsen (1316-1390), der die Volumina unendlicher Mengen (Strahlen, Raum,…) verglichen hat, mit diesem Problem auseinandergesetzt.


ABBILDUNG 3.3. Georg Cantor (1845–1918)

Anders die Idee der Menge. Diese begann erst Mitte des 19. Jahrhunderts langsam in die Köpfe der Mathematiker Einzug zu halten. So hat etwa der tschechische Mathematiker Bernard Bolzano (1781–1848) ein Jahr vor seinem Tod folgendermaßen formuliert:

> ...eine Verkörperung der Idee oder des Konzeptes, das wir erhalten, wenn wir die Anordnung seiner Teile für gleichgültig erachten.

Der wirkliche Durchbruch der Mengenlehre kam aber erst mit Georg Cantor, der nach einem Besuch bei Richard Dedekind (1831–1916) und darauf folgender Korrespondenz im Jahr 1874 eine wissenschaftliche Arbeit im Crelle-Journal publizierte, in der er Mengen und das Konzept verschiedener Klassen von Unendlichkeit einführte.

Im Jahr 1878 versuchte er eine weitere Publikation im Crelle-Journal, doch stieß er auf heftigen Widerstand der damals Ton angebenden mathematischen Schule der *Konstruktivisten* mit ihrem führenden Kopf Leopold Kronecker (1823–1891), die keine mathematischen Sachverhalte akzeptieren wollten, die sich nicht in endlich vielen Schritten aus den natürlichen Zahlen konstruieren ließen. Erst nach massiver Intervention von Karl Weierstrass (1815–1897) wurde die Arbeit schließlich akzeptiert. Das war der Beginn eines langen Kampfes innerhalb der Mathematik um ihre philosophischen und später auch logischen Grundlagen, der z.B. durch folgende Zitate schön belegt werden kann:

> „Aus dem Paradies [die Mengenlehre], das Cantor uns geschaffen hat, soll uns niemand mehr vertreiben können.“ David Hilbert (1862–1943)

> „Spätere Generationen werden die Mengenlehre als Krankheit ansehen, die man überwunden hat.“ Jules Henri Poincare (1854–1912)

Dieser Kampf wurde nicht nur auf mathematischer sondern auch auf menschlicher Ebene ausgetragen, so blockierten etwa Kronecker und Hermann Schwarz (1843–1921) Cantors Stellenbewerbungen.

Von 1879 bis 1884 veröffentlichte Cantor in den *Mathematischen Annalen* eine sechsteilige Abhandlung über die Mengenlehre, die zu großen Kontroversen in der mathematischen Welt führte. Einige Mathematiker hielten sich an Kronecker, doch andere folgten Cantors Weg. So führte etwa Giuseppe Peano (1858–1932), nach seinem berühmten Satz über Differentialgleichungen (1886) und der ersten Definition eines Vektorraumes (1888) und vor seinen berühmten Peano-Kurven (1890), neben der Axiomatisierung der natürlichen Zahlen 1889 auch das Zeichen $\in$ in die Mengenlehre ein.

Im Jahr 1897 fand Cesare Burali-Forti (1861-1931) das erste Paradoxon in der Mengenlehre, obwohl es durch eine fehlerhaft verstandene Definition des Begriffes „wohlgeordnete Menge" entwertet, wenn auch nicht ausgelöscht wurde. Interessanter Weise ereignete sich der erste persönliche Erfolg für Cantor im selben Jahr auf einem Mathematiker-Kongress in Zürich, wo sein Werk zum ersten Mal positiv aufgenommen, ja von manchen in höchsten Tönen gepriesen wurde.

Nachdem Cantor selbst 1899 ein weiteres Paradoxon gefunden hatte, entdeckte schließlich Bertrand Russell (1872-1970) im Jahre 1902 das ultimative Paradoxon (heute Russellsche Antinomie), das insbesondere wegen seiner Einfachheit die neuen Grundlagen der Mathematik in ihren Grundfesten erschütterte. Russel betrachtetet die Menge R aller Mengen, die sich nicht selbst enthalten; nennen wir solche Mengen „vernünftig". Die Frage ob R sich selbst enthält, führt nun zu einem Widerspruch: Nehmen wir nämlich an, dass R ein Element von R ist, so ist R keine „vernünftige" Menge und kann daher nicht Element von R sein. Ist andererseits R nicht Element von R, so ist R eine „vernünftige" Menge und es muss gelten, dass R Element von R ist.

Zu diesem Zeitpunkt hatte sich die Mengenlehre allerdings schon durchgesetzt. Sowohl die Analysis baute darauf auf als auch Teile der Algebra. Die Maßtheorie und das mengentheoretische Integral waren 1901 bzw. 1902 von Henri Lebesgue (1875–1941) erfunden worden. Daher wurde die Mengenlehre nicht gleich wieder verworfen sondern eine fieberhafte Suche startete nach einer „Rettung" der Mengenlehre ohne ihre wichtigsten Eigenschaften aufgeben zu müssen.

Russell selbst versuchte, sein Paradoxon aus der Mathematik „wegzudefinieren". In seinem sehr einflussreichen Werk *Principia Mathematica*, das er gemeinsam mit Alfred Whitehead (1861–1947) in den Jahren 1910–1913 veröffentlichte, stellte er eine Lösung mit Hilfe der *Theory of types* vor, doch diese wurde von den meisten nicht als befriedigend erachtet.

Der erste, der eine Lösung für das Paradoxien-Problem fand war Ernst Zermelo (1871–1953), der im Jahr 1908 das erste befriedigende Axiomensystem für die Mengenlehre publizierte, das im Jahr 1922 von Adolf Fraenkel (1891–1965) nochmals verbessert wurde, und das heute aus zehn Axiomen bestehend für viele die Grundlage der Mathematik darstellt (siehe Abschnitt 3.4.1). Auch andere berühmte Mathematiker wie Kurt Gödel (1906–1978), Paul Bernays (1888–1977) und John von Neumann (1903–1957) axiomatisierten die Mengenlehre auf unterschiedliche Weisen, und welches der Axiomensysteme die Grundlage bilden soll, wird in der heutigen Zeit von den meisten Mathematikern als „reine Geschmackssache" angesehen.

Um die Jahrhundertwende strebten noch viele Mathematiker allen voran David Hilbert und Gottlob Frege (1848–1925) danach die Mathematik (und auch die Physik) vollständig auf die formale Logik zu reduzieren. Hilbert — wahrscheinlich der einflußreichste Mathematiker seiner Zeit — erwähnte dies noch 1900 in seiner berühmten Rede auf dem Internationalen Mathematiker-Kongresses in Paris. Für dieses Ziel war eine möglichst umfassende und widerspruchsfreie Axiomatisierung der Mengenlehre wesentlich. Nach Gödels ω-Unvollständigkeitssatz im Jahr 1931, der die Grenzen jedes axiomatischen Systems aufzeigte, wurden alle diese Versuche zerschlagen und weitere Ansätze bereits im Keim erstickt.

Geblieben von dieser Entwicklung ist das heutige Bestreben der Mathematiker nach exaktem und logischem Vorgehen beim Entwickeln und Beweisen von mathematischen Theorien, beim Aufbau des mathematischen Theoriegebäudes. Jetzt ist es wichtig, Grundlagen zu *haben*, die die mathematisch exakte Behandlung der Theorie erlauben. Nachdem alle heute gängigen Axiomensysteme das bieten, ist die genaue Auswahl eines bestimmten Systems den meisten Mathematikern nicht mehr so wichtig.

Nach diesem historischen Überblick wollen wir die Mengenlehre genauer kennenlernen und zunächst wie Cantor naiv beginnen.

Wollen wir über Mengen sprechen, so müssen wir zuerst erklären, wie wir sie beschreiben können. Grundsätzlich stehen uns zwei Methoden zur Verfügung.

(1) **Aufzählen:** Wir können **alle** Elemente einer *endlichen* Menge angeben, um die Menge zu definieren. So könnten wir etwa durch

$$M := \{0, 2, 5, 9\}$$

die Menge M einführen. Sie enthält als Elemente die vier Zahlen 0, 2, 5 und 9.

Diese in der Mengenlehre fundamentale Beziehung zwischen den Mengen und ihren Elementen wird durch das Symbol $\in$ ausgedrückt. Hier also: $0 \in M$, $2 \in M$, ...

Auf die Reihenfolge kommt es bei der Aufzählung übrigens nicht an: $\{0, 5, 2, 9\}$ ist ebenso wie $\{9, 0, 2, 5\}$ die gleiche Menge wie M.

Das Zeichen := bedeutet, dass wir gerade etwas **definieren**, in diesem Fall geben wir der Menge der Zahlen 0, 2, 5 und 9 den Namen M. Merke: Der Doppelpunkt im Zeichen := (oder =:) steht immer auf der Seite des Gleichheitszeichens, auf der der zu definierende Begriff steht.

Grundsätzlich dienen Definitionen dazu, neue *Abkürzungen* einzuführen. Man kann jederzeit den definierten Begriff durch die definierende Beschreibung ersetzen, und manchmal muss man das auch tun, speziell in Beweisen.

Den Sinn von Definitionen rein darauf zu reduzieren, dass sie Abkürzungen einführen, heißt aber, die Bedeutung von Definitionen stark unter zu bewerten. Eine Definition ist ein schöpferischer Akt! Es ist einer der bedeutendsten Schritte in der Entwicklung einer mathematischen Theorie, die wichtigen Objekte zu erkennen und ihnen Namen zu geben. Dadurch rücken sie ins Zentrum des Interesses, es werden neue Begriffe geschaffen, und man kann beginnen, sich mit diesen neuen Begriffen auseinander zu setzen.

In diesem Zusammenhang ist noch einmal wichtig heraus zu streichen, dass eine Definition niemals *falsch* sein kann (abgesehen von Prüfungen, wenn bereits bestehende Definitionen falsch rezitiert werden), sie kann allerdings *sinnlos* oder *wenig hilfreich* sein.

Scheuen Sie nicht davor zurück, bei der Lösung Ihrer Aufgaben, wichtigen Objekten eigene Namen zu geben z.B. „starke" Matrizen, „coole" Elemente,. . . .

(2) **Beschreiben:** Gemäß einer Idee von Cantor können wir eine Menge auch dadurch definieren, dass wir *Eigenschaften ihrer Elemente* angeben. Dies läßt sich auch auf *unendliche* Mengen anwenden. Die Menge P aller Primzahlen ließe sich etwa definieren durch

$$P := \{p \in \mathbb{N} \mid p > 1 \wedge \forall m \in \mathbb{N} : (m|p \Rightarrow (m = 1 \vee m = p))\}.$$

Genauer bedeutet das, dass man P als die Menge all jener Elemente p von $\mathbb{N}$ definiert, die größer 1 sind und folgende Eigenschaft besitzen: Jedes Element m von $\mathbb{N}$, das p teilt, ist entweder 1 oder p selbst. Das bedeutet aber wiederum, dass p größer 1 ist und nur die trivialen Teiler 1 und p hat — genau unsere Definition 2.1.2.

Oft wird statt des senkrechten Strichs (|) auch ein Doppelpunkt verwendet, also $P := \{p \in \mathbb{N} : \ \dots \}$.

Viele Definitionen verwenden nicht nur verbale Ausdrücke sondern auch mathematische Symbolik, wie obige Definition von P. Man muss aber nicht rein symbolisch formulieren. Eine ähnlich gute Definition von P wäre

$$P := \{p \in \mathbb{N} \mid p > 1 \text{ und } p \text{ besitzt nur die Teiler 1 und } p\}.$$

Symbole im Text erhöhen zwar oft dessen Präzision, doch im selben Maße verringern sie seine Lesbarkeit. Geht man zu sorglos mit ihnen um, so kann der Text sogar mehrdeutig werden. Beherzigt man allerdings einige Regeln, so verbessert das die Lage sofort.

- **Ein Satz sollte nicht mit einem Symbol beginnen**. Man formuliert den Satz

  $\cancel{\mathbb{R}}$ bezeichnet die Menge der reellen Zahlen.

  besser um

  Die Menge der reellen Zahlen bezeichnen wir mit $\mathbb{R}$.
- **Axiom von Siegel** (nach dem Mathematiker Carl Siegel (1896–1981)): **Zwei mathematische Symbole** (die sich nicht zu einem größeren Symbolkomplex ergänzen) **müssen stets durch mindestens ein Wort getrennt sein!**

  Eine 10-elementige Menge hat genau ~~45 2~~-elementige Teilmengen.

  könnte bei engerem Druck fehlinterpretiert werden. Besser wäre etwa die Formulierung

  Die Anzahl der 2-elementigen Teilmengen einer 10-elementigen Menge ist 45.
- **Verwenden Sie niemals mathematische Symbole als Abkürzungen für Worte im Text.**

  Sei V ein Vektorraum $\cancel{\mid}$ endlich dimensional.

Verwenden Sie die Symbole sorgfältig und behalten Sie ihre mathematische Bedeutung stets im Auge. Konzentrieren Sie die Symbolik nicht zu sehr. Eine gute Mischung aus Symbolik und Text garantiert einerseits die Präzision und erhöht andererseits die Lesbarkeit.

Unverzichtbar ist, dass Sie stets in der Lage sind, zwischen verbaler und formaler Beschreibung hin und her zu schalten. Es ist wichtig, schon zu Beginn die Fähigkeit zu trainieren, die eine Beschreibung in die andere zu verwandeln.

Beispiel 3.3.2.

- *Es gilt* $2 \in \{2, 4, 7, 9\}$,
- *weiters haben wir* $42 \in \mathbb{N}$.
- *Steht die Menge links vom Element, so dreht man das Zeichen* $\in$ *einfach um:* $\mathbb{R} \ni \pi$.
- *Wollen wir ausdrücken, dass ein Objekt* nicht *Element einer bestimmten Menge ist, so streichen wir das Zeichen* $\in$ *einfach durch, wie in* $\frac{1}{2} \notin \mathbb{N}$.

Definition 3.3.3. *Zwei Mengen gelten genau dann als* gleich, *wenn sie dieselben Elemente haben. In Symbolen notiert:*

$$A = B \quad \text{genau dann wenn} \quad \forall x : (x \in A \Leftrightarrow x \in B).$$

Definition 3.3.4. *Die* leere Menge $\emptyset$ *ist definiert als die Menge, die kein Element enthält. Formal kann das z.B. so ausgedrückt werden*

$$\emptyset := \{x \mid x \neq x\}.$$

In der Mathematik ist das Symbol $\emptyset$ *üblich, auch wenn mitunter* $\{\}$ *als Bezeichnung für die leere Menge verwendet wird.*

WICHTIG: Beachten Sie, dass ein Element in einer Menge enthalten ist, oder eben nicht. Es steht immer eindeutig fest welche Elemente zu einer Menge gehören.

Ein und dasselbe Element kann nicht mehrfach in einer Menge auftreten. Eine Menge ist eine Ansammlung *verschiedener* Objekte! Allerdings ist es nicht verboten, einige Elemente mehrfach anzuführen. $\{1, 2\}$ ist die gleiche Menge wie $\{1, 1, 2\}$. Zugegeben, dieses Beispiel ist gekünstelt — der Sinn dieser Vereinbarung wird erst dann deutlich wenn man z.B. eine Menge $\{a, b, c\}$ untersucht, wobei a, b und c erst später festgesetzt oder näher bestimmt werden. Dann ist es sehr praktisch, $\{a, b, c\}$ schreiben zu können, selbst wenn sich später herausstellen sollte, dass $a = b$ gilt.

3.3.1.1. Teilmengen. Bevor wir untersuchen, wie wir Mengen mit einander verknüpfen können, betrachten wir das einfachste Konzept, das von *Teilmengen.*

Definition 3.3.5. *Eine Menge B heißt* Teilmenge *der Menge A, wenn B nur Elemente von A enthält. In der Sprache der Logik formuliert, bedeutet das*

$$\forall x : x \in B \Rightarrow x \in A,$$

oder kürzer und etwas salopper

$$\forall x \in B : x \in A.$$

Ist B Teilmenge von A, so schreiben wir

$$B \subseteq A \quad \text{oder} \quad A \supseteq B.$$

A heißt dann Obermenge *von B.*

Beispiel 3.3.6. *Wir finden etwa:*

- *Die leere Menge ist Teilmenge* jeder *Menge.*
- *Jede Menge M ist ihre eigene Teilmenge. Die Menge M und $\emptyset$ heißen die* ***trivialen Teilmengen*** *von M.*
- *Alle Teilmengen, die ungleich der Menge selbst sind, nennt man auch* ***echte Teilmengen****. Möchte man betonen, dass B echte Teilmenge von A ist, so schreibt man meist*

$$B \subset A \quad \text{oder expliziter} \quad B \subsetneqq A.$$

- *Alle Teilmengen von $\{1, 2, 3\}$ sind $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$ und $\{1, 2, 3\}$.*

Die Teilmengenrelation entspricht, wie schon in der Definition explizit gemacht wurde, der logischen Implikation $\Rightarrow$. Daraus läßt sich auch sofort ableiten, wie man Gleichheit von Mengen überprüfen kann.

Proposition 3.3.7. *Zwei Mengen A und B sind genau dann gleich, wenn $A \subseteq B$ und $B \subseteq A$; formal*

$$A \subseteq B \;\wedge\; B \subseteq A \;\Leftrightarrow\; A = B.$$

Beweis. Dieser Satz behauptet eine Äquivalenz und wir müssen wiederum beide Implikationsrichtungen beweisen.
$\Leftarrow$: Zu zeigen ist, dass wenn $A = B$ gilt, auch die beiden Enthalten-Relationen $A \subseteq B$ und $B \subseteq A$ gelten. Dies ist aber trivial, da $A \subseteq A$ für jede Menge stimmt.
$\Rightarrow$: Wir müssen zeigen, dass aus beiden Enthalten-Relationen schon die Gleichheit folgt. Es gelte also $A \subseteq B$ und $B \subseteq A$. Wegen $A \subseteq B$ gilt $x \in A \Rightarrow x \in B$. Andererseits folgt aus $B \subseteq A$, dass $x \in B \Rightarrow x \in A$ gilt. Fassen wir die beiden Implikationen zusammen, erhalten wir für beliebiges x den Zusammenhang $x \in A \Leftrightarrow x \in B$. Das wiederum bedeutet laut Definition 3.3.3, dass $A = B$ gilt. □

3.3.1.2. Mengenoperationen. Wenn man mehr als eine Menge betrachtet, so kann man aus diesen Mengen weitere Mengen erzeugen. Die folgenden Mengenoperationen werden dabei standardmäßig verwendet.

Definition 3.3.8 (Vereinigung).

(i) *Seien zwei Mengen A und B gegeben. Wir konstruieren eine neue Menge aus allen Elementen von A und B. Diese Menge heißt* Vereinigungsmenge *$A \cup B$ von A und B, und in formalerer Schreibweise ist sie definiert als*

$$A \cup B := \{x \mid x \in A \vee x \in B\}.$$

Hier wurde also eine Operation $\cup$ *für Paare von Mengen definiert, die* Vereinigung.

(ii) *Man kann auch mehr als zwei Mengen vereinigen, sogar beliebig viele. Sei* A_i, $i \in I$ *eine Familie von Mengen. Dann ist*

$$\bigcup_{i\in I} A_i := \{x \mid \exists i \in I : x \in A_i\}$$

die Vereinigung aller A_i. *Das bedeutet, wir nehmen alle* x *auf, die in* ***wenigstens einer*** *der Mengen* A_i *liegen. Die* ***Indexmenge*** I *kann dabei beliebig (groß) sein.*

Beispiel 3.3.9. *Es gelten:*

- $\{1, 3, 6\} \cup \{2, 6\} = \{1, 2, 3, 6\}$,
- $M \cup \emptyset = M$,
- $\bigcup_{n\in\mathbb{N}} \{-n, n\} = \mathbb{Z}$.

Definition 3.3.10 (Durchschnitt)**.**

(i) *Seien wieder zwei Mengen* A *und* B *gegeben. Wir bezeichnen die Menge, die alle Elemente von* A *enthält, die auch in* B *enthalten sind, mit* $A \cap B$ *und nennt sie* Durchschnittsmenge *von* A *und* B*. Formal ist sie definiert durch*

$$A \cap B := \{x \mid x \in A \wedge x \in B\}.$$

(ii) *Genau wie die Vereinigung kann man auch den Durchschnitt beliebig vieler Mengen definieren. Sei wieder* A_i, $i \in I$ *eine Familie von Mengen. Dann ist*

$$\bigcap_{i\in I} A_i := \{x \mid \forall i : x \in A_i\}$$

der Durchschnitt aller A_i. *Wir nehmen also alle jene Elemente auf, die in* ***allen*** *Mengen* A_i *liegen.*

(iii) *Haben zwei Mengen* A *und* B *leeren Durchschnitt (*$A \cap B = \emptyset$*), so sagen wir* A *und* B *sind* disjunkt.

Sind alle von uns betrachteten Mengen Teilmengen eines (sog.) Universums U, so können wir eine weitere Definition hinzufügen.

Definition 3.3.11. *Sei* A *eine Teilmenge der Menge* U*. Dann definieren wir das* Komplement $\complement A$ *von* A *(in* U*) durch die Beziehung*

$$\complement A := \{x \in U \mid x \notin A\}.$$

Oft werden auch die Bezeichnungen A' *und* A^c *für das Komplement von* A *verwendet.*

Hinweis: Beachten Sie, dass wir die Universalmenge *nur* zur Bildung des Komplements einführen und verwenden. Alle Rechenoperationen und Rechenregeln, in denen kein Komplement vorkommt, gelten unabhängig von der Existenz solch einer Universalmenge. Ohne Universalmenge muss man auf die Bildung des Komplements verzichten. Man kann es in den meisten Fällen durch die Mengendifferenz (siehe Definition 3.3.13) ersetzen. In diesem Fall muss man aber die Rechenregeln geeignet anpassen.

Vergleichen wir die Definitionen mit den logischen Operatoren, die wir in Abschnitt 3.1 eingeführt haben, so erkennen wir rasch die Zusammenhänge. Die Vereinigung $\cup$ wird gewonnen durch logische Oder-Verknüpfung ($\vee$) der Elementbeziehung zu den zu vereinigenden Mengen. Der Durchschnitt entspricht der Und-Verknüpfung ($\wedge$), und die Bildung des Komplements der Negation ($\neg$). Diese enge Verwandtschaft zwischen den logischen Verknüpfungen und den Mengenoperationen hat als Konsequenz, dass die Mengenoperationen dieselben Rechengesetze erfüllen.

Theorem 3.3.12. *Die mengentheoretischen Operationen $\cup$, $\cap$ und $\complement$ erfüllen die folgenden Operationen, wobei U das für die Komplementbildung notwendige Universum bezeichne.*

Kommutativgesetze:	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Assoziativgesetze:	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Distributivgesetze:	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Verschmelzungsgesetze:	$A \cup (B \cap A) = A$	$A \cap (B \cup A) = A$
Idempotenzgesetze:	$A \cup A = A$	$A \cap A = A$
Neutralitätsgesetze:	$A \cup \emptyset = A$	$A \cap U = A$
Absorptionsgesetze:	$A \cup U = U$	$A \cap \emptyset = \emptyset$
Komplementaritätsgesetze:	$A \cup \complement A = U$	$A \cap \complement A = \emptyset$
	$\complement \emptyset = U$	
	$\complement U = \emptyset$	
Gesetz des doppelten Komplements:	$\complement(\complement A) = A$	
Gesetze von De Morgan:	$\complement(A \cup B) = \complement A \cap \complement B$	$\complement(A \cap B) = \complement A \cup \complement B$

Beweis. Alle Aussagen des Theorems können entweder durch Aufstellen von Mengentafeln oder aber durch zurückführen auf Theorem 3.1.6 bewiesen werden. Wir beweisen ein Verschmelzungsgesetz nach der 1. und eine Distributivgesetz nach der 2. Methode. Alle anderen Behauptungen folgen analog.

Zu zeigen ist $A \cup (B \cap A) = A$.

A	B	$B \cap A$	$A \cup (B \cap A)$
$\in$	$\in$	$\in$	$\in$
$\in$	$\notin$	$\notin$	$\in$
$\notin$	$\in$	$\notin$	$\notin$
$\notin$	$\notin$	$\notin$	$\notin$

Da die erste und die letzte Spalte übereinstimmen, ist der Beweis des Verschmelzungsgesetz geglückt.

Zu zeigen ist: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Wir wissen,

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow x \in A \wedge x \in B \cup C \\ &\Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \\ &\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \quad \text{wegen Theorem 3.1.6} \\ &\Leftrightarrow x \in A \cap B \vee x \in A \cap C \Leftrightarrow x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Außer der explizit angegebenen Äquivalenz gelten alle anderen Zeilen wegen der Definitionen von $\cup$ und $\cap$. Die behauptete Aussage folgt schließlich aus Definition 3.3.3. $\square$

Eine weitere Mengenoperation, die mit der Komplementbildung „verwandt" ist, ist die *Differenz von Mengen.*

Definition 3.3.13 (Mengendifferenz). *Seien A und B zwei Mengen. Die Menge $A \setminus B$ ist die Menge aller Elemente von A, die nicht in B sind. Es gilt also*

$$A \setminus B := \{x \in A \mid x \notin B\}.$$

Bemerkung 3.3.14. *Die Komplementbildung* $\complement A$ *kann mit Hilfe der Mengendifferenz und dem Universum* U *kurz beschreiben als*

$$\complement A = U \setminus A.$$

Beispiel 3.3.15. *Seien* $A = \{2, 3, 6\}$ *und* $B = \{2, 5, 7\}$*. Dann ist* $A \setminus B = \{3, 6\}$*.*

Die *symmetrische Mengendifferenz* ist die letzte Grundoperation, die wir für Mengen einführen wollen.

Definition 3.3.16 (Symmetrische Differenz)**.** *Es seien wieder zwei Mengen* A *und* B *gegeben. Definieren wir die Menge* $A \triangle B$ *als diejenigen Elemente von* A *und* B*, die nicht in beiden Mengen liegen*

$$A \triangle B := (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Beispiel 3.3.17. *Seien* $A = \{2, 3, 6\}$ *und* $B = \{2, 5, 7\}$*. Dann ist* $A \triangle B = \{3, 6, 5, 7\}$*.*

3.3.1.3. Potenzmenge, Produktmenge. Kommen wir nun, nachdem wir Operationen definiert haben, um aus bestehenden Mengen neue Mengen zu definieren, zum nächsten Schritt. Zunächst verwenden wir die Tatsache, dass Mengen wieder Mengen enthalten dürfen, um die Potenzmenge einer Menge zu definieren.

Definition 3.3.18. *Sei* M *eine Menge. Die* Potenzmenge $\mathbb{P}M$ *von* M *ist definiert als die Menge aller Teilmengen von* M*.*

Beispiel 3.3.19.

- *Die Potenzmenge von* $\{1, 2, 3\}$ *ist*

  $$\mathbb{P}\{1, 2, 3\} = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}.$$

- *Die Potenzmenge der leeren Menge ist* nicht *die leere Menge sondern eine einelementige Menge, die nur die leere Menge* enthält. *(Also ein Sack, der nur einen leeren Sack enthält!)*

  $$\mathbb{P}\emptyset = \{\emptyset\}.$$

Allgemein bezeichnet man eine Menge, die wieder Mengen enthält als **Mengensystem**.

Sind schließlich zwei Mengen A und B gegeben, so kann man die Produktmenge $A \times B$ bilden. Zu diesem Zweck formen wir aus den Elementen a von A und b von B **geordnete Paare** (a, b). In diesen Paaren schreiben wir die Elemente von A an erster und die Elemente von B an zweiter Stelle. Zwei dieser geordneten Paare wollen wir nur dann als gleich betrachten, wenn *beide* Komponenten übereinstimmen.

Definition 3.3.20 (Produkt)**.**

(i) *Seien* A *und* B *Mengen. Die* Produktmenge $A \times B$*, auch genannt das* Cartesische Produkt*, von* A *und* B *ist die Menge aller geordneten Paare* (a, b) *aus Elementen von* A *und* B*, formal*

$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}.$$

(ii) *Sind* k*-stück Mengen* $M_1, \ldots, M_k$ *gegeben, so können wir analog die geordneten* k*-tupel bilden* $(m_1, \ldots, m_k)$ *mit* $m_i \in M_i$ *für* $i = 1, \ldots, k$*. Das* Cartesische Produkt $\bigtimes_{i=1}^k M_i = M_1 \times \ldots \times M_k$ *der* M_i *ist dann die Menge aller geordneten* k*-tupel dieser Form, d.h.*

$$\bigtimes_{i=1}^{k} M_i := \{(m_1, \ldots, m_k) \mid \forall i : m_i \in M_i\}.$$

(iii) *Ist* $A = B$ *bzw.* $M_i = A$ *für alle* i*, so schreiben wir statt* $A \times A$ *und* $\underbrace{A \times \ldots \times A}_{k\ mal}$ *kurz* A^2 *bzw.* A^k*.*

Beispiel 3.3.21. *Seien $A = \{1, 2, 3\}$ und $B = \{a, b\}$, dann ist*

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

und

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

Man kann auch das Cartesische Produkt beliebig vieler Mengen M_i, $i \in I$ bilden; die Definition ist allerdings ein wenig kompliziert und benötigt Funktionen. Daher wird sie erst in Abschnitt 3.3.3 nachgeholt werden.

3.3.2. Relationen. In diesem Abschnitt geht es darum, Elemente von Mengen miteinander in Beziehung zu setzen.

Beispiel 3.3.22. *Sei etwa M die Menge aller Hörer in diesem Hörsaal. Betrachten wir die Beziehung „ist verwandt mit“. Wir können dann zu je zwei Personen A und B im Hörsaal eine Aussage darüber machen, ob A mit B verwandt ist.*

Eine andere Beziehung, die wir auf M betrachten könnten ist „ist Bruder von“. Natürlich ist jeder Bruder auch ein Verwandter. Umgekehrt muss das nicht der Fall sein.

Schließlich ist eine dritte mögliche Beziehung „wohnt im selben Bezirk wie“.

Beziehungen in der Art von Beispiel 3.3.22 zwischen Elementen von Mengen nennt man Relationen. Im folgenden wollen wir eine mathematische Definition dafür geben.

Definition 3.3.23. *Seien M und N Mengen. Eine* Relation auf $M \times N$ *ist eine Teilmenge R des Cartesischen Produkts, d.h. $R \subseteq A \times B$.*

Für zwei Elemente $a \in M$ und $b \in N$ sagen wir: a steht in Relation mit *b, falls $(a, b) \in R$ gilt. Wir schreiben dann in Symbolen*

$$a\,R\,b.$$

Stehen a und b nicht miteinander in Relation, so schreiben wir $a \not R\, b$.

Meist werden Relationen nicht mit R sondern mit Symbolen bezeichnet. Typische Relationssymbole sind $<$, $\subset$, $\sim$, $\cong$, $\ll$, $\equiv$, $\simeq$, $\sqsubset$, $\frown$, $\preccurlyeq$ und viele andere mehr. Gerichtete Symbole wie $<$ werden üblicherweise für Ordnungsrelationen (siehe Abschnitt 3.3.2.2) verwendet, während symmetrische Symbole wie $\simeq$ meist für Äquivalenzrelationen (siehe Abschnitt 3.3.2.1) stehen.

Ist R eine Relation auf $M \times N$ und gilt $M = N$, so sprechen wir von einer *Relation auf M*. Im Folgenden befassen wir uns (fast) ausschließlich mit diesem Fall.

Beispiel 3.3.24. *Die Beziehungen aus Beispiel 3.3.22 sind natürlich Relationen auf M. Haben wir etwa ein Geschwisterpaar S und B im Hörsaal, so müssen wir in unsere Relation V für „verwandt“ die beiden Paare (S, B) und (B, S) aufnehmen. Ist S weiblich und B männlich, so darf in der „Bruder“-Relation R nur das Paar (B, S) vorkommen (es gilt ja „B ist Bruder von S“ aber nicht „S ist Bruder von B“).*

Zwei wichtige Hauptgruppen von Relationen wollen wir in den folgenden Abschnitten untersuchen. Zuvor definieren wir jedoch noch zwei Eigenschaft für Relationen, die in beiden Abschnitten wichtig sein werden.

Definition 3.3.25 (Transitivität, Reflexivität)**.** *Sei R eine Relation auf einer Menge M.*

(i) *R heißt* transitiv, *wenn für alle $a, b, c \in M$ gilt, dass*

$$a\,R\,b \wedge b\,R\,c \Rightarrow a\,R\,c.$$

(ii) *R heißt* reflexiv, *wenn für alle $a \in M$ gilt, dass $a\,R\,a$.*

Beispiel 3.3.26. *Kehren wir noch einmal — aber nicht zum letzten Mal — zu den Relationen aus Beispiel 3.3.22 zurück. Nicht alle sind transitiv, denn wenn A mit B und B mit C verwandt sind, so ist noch lange nicht A mit C verwandt. Anderes gilt für Brüder. Ist A Bruder von B und B Bruder von C, so ist auch A Bruder von C. Auch das Wohnen im gleichen Bezirk ist eine transitive Relation.*

Man könnte sagen, die Verwandtschaftsrelation ist reflexiv, wenn man festlegt, dass jeder Mensch mit sich selbst verwandt ist. Die Bruderbeziehung ist jedoch nicht reflexiv.

Auch ohne weitere Definition ist „wohnt im selben Bezirk wie“ eine reflexive Relation.

3.3.2.1. Äquivalenzrelationen.

Definition 3.3.27. *Eine reflexive und transitive Relation $\sim$ auf einer Menge M heißt* Äquivalenzrelation*, falls sie folgende weitere Eigenschaft erfüllt:*

Symmetrie: $\forall x, y \in M : (x \sim y \Rightarrow y \sim x)$.

Gilt $x \sim y$, so nennen wir x und y äquivalent.

Beispiel 3.3.28. *Wenn wir ein weiteres Mal die Relationen aus Beispiel 3.3.22 bemühen, so erkennen wir schnell, dass „wohnt im selben Bezirk wie“ eine Äquivalenzrelation ist. Die Symmetrie ist erfüllt, denn wenn A und B im selben Bezirk wohnen, wohnen auch B und A im selben Bezirk.*

Die zweite Relation „ist Bruder von“ ist keine *Äquivalenzrelation, da weder Reflexivität noch Symmetrie gelten.*

„Ist verwandt mit“ ist zwar symmetrisch, aber da die Transitivität falsch ist, ist es keine Äquivalenzrelation.

Ist eine Äquivalenzrelation $\sim$ auf einer Menge definiert, so können wir die Relation dafür verwenden, miteinander äquivalente Elemente von M in Gruppen zusammenzufassen. Dieses Prinzip ist wohlbekannt, denn in Telefonbüchern werden etwa jene Ärzte in eine Gruppe zusammengefasst, die im selben Bezirk praktizieren.

Definition 3.3.29. *Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Wir definieren die* Äquivalenzklasse von $a \in M$ *durch*

$$C_a := \{b \in M \mid b \sim a\}.$$

Alternative Bezeichnungen für C_a sind auch $[a]$ und $\bar{a}$.

Aus der Definition sehen wir unmittelbar, dass für jedes $a \in M$ die Äquivalenzklasse $C_a \subseteq M$ erfüllt. Wegen der Reflexivität von $\sim$ gilt $a \in C_a$ (Äquivalenzklassen sind also niemals leer!) und somit $\bigcup_{a \in M} C_a = M$.

Eine zweite wichtige Eigenschaft der Äquivalenzklassen wollen wir in der nachfolgenden Proposition fest halten.

Proposition 3.3.30. *Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Dann sind zwei Äquivalenzklassen C_a und C_b entweder disjunkt oder gleich. In Symbolen*

$$C_a \cap C_b \neq \emptyset \Leftrightarrow C_a = C_b.$$

Beweis. Da es sich um eine Äquivalenz handelt …
$\Leftarrow$: Ist $C_a = C_b$, so ist auch $C_a \cap C_b = C_a \neq \emptyset$, weil Äquivalenzklassen nie leer sind.
$\Rightarrow$: Ist umgekehrt $C_a \cap C_b \neq \emptyset$. Dann existiert ein $y \in C_a \cap C_b$, und somit gelten $y \sim a$ und $y \sim b$. Aus Symmetrie und Transitivität folgt $a \sim b$. Sei nun $x \in C_a$. Dann wissen wir $x \sim a$ und wegen der Transitivität auch $x \sim b$ und damit $x \in C_b$. Also gilt $C_a \subseteq C_b$. Nachdem wir analog durch Vertauschen von a und b in obiger Argumentation $C_b \subseteq C_a$ beweisen können, folgt $C_a = C_b$, was wir behauptet hatten. $\square$

Wir finden also für jede Äquivalenzrelation $\sim$ auf einer Menge M eine Familie von Teilmengen von M, die Äquivalenzklassen C_a, die

(i) $\bigcup_{a\in M} C_a = M$ (Man sagt: Die C_a **überdecken** M) und
(ii) $C_a \cap C_b \neq \emptyset \Leftrightarrow C_a = C_b$

erfüllen.

Definition 3.3.31. *Eine Familie disjunkter Teilmengen einer Menge, die die gesamte Menge überdecken, nennt man* Partition.

Anders ausgedrückt ist ein System von Teilmengen einer Menge M genau dann eine Partition, wenn jedes Element von M in genau einer der Teilmengen liegt.

Theorem 3.3.32. *Jede Äquivalenzrelation $\sim$ auf einer Menge M definiert eine Partition von M, und umgekehrt kann man aus jeder Partition U_i, $i \in I$ einer Menge M eine Äquivalenzrelation $\sim$ gewinnen durch*

$$a \sim b :\Leftrightarrow \exists i \in I : a, b \in U_i.$$

Beweis. Wir wissen bereits, dass eine Äquivalenzrelation auf M eine Partition definiert (Proposition 3.3.30), nämlich die Partition in Äquivalenzklassen.

Sei umgekehrt eine Partition U_i, $i \in I$ gegeben, und sei die Relation $\sim$ wie in der Aussage des Theorems definiert. Es bleibt zu zeigen, dass $\sim$ eine Äquivalenzrelation ist.

Reflexivität: Für alle $a \in M$ gilt $a \sim a$, da wegen $\bigcup_{i\in I} U_i = M$ ein $j \in I$ existieren muss mit $a \in U_j$.

Symmetrie: Das folgt ganz offensichtlich aus der Definition von $\sim$.

Transitivität: Gelten $a \sim b$ und $b \sim c$, so wissen wir, dass ein $j \in I$ mit $a, b \in U_j$ und ein $k \in I$ mit $b, c \in U_k$ existieren. Es ist somit $b \in U_j \cap U_k$, und daher ist $U_i = U_k$. Daraus wiederum folgt, dass $a, b, c \in U_i$ und daher $a \sim c$ gilt.

Also ist $\sim$ tatsächlich eine Äquivalenzrelation. □

Partitionen von Mengen zu Äquivalenzrelationen sind in der Mathematik äußerst wichtig. Aus diesem Grund hat man der Menge aller Äquivalenzklassen einen eigenen Namen gegeben.

Definition 3.3.33. *Sei M eine Menge, $\sim$ eine Äquivalenzrelation. Wir definieren die* Faktormenge *(oder auch* Quotientenmenge*) $M/_\sim$ (sprich: M modulo Tilde) als die Menge aller Äquivalenzklassen bezüglich $\sim$.*

Beispiel 3.3.34. *Sei auf $\mathbb{Z}$ die Relation*

$$n \sim_p m :\Leftrightarrow \exists k \in \mathbb{Z} \text{ mit } n = m + kp$$

gegeben. Dies ist eine Äquivalenzrelation:

Reflexivität: *$m \sim_p m$, weil $m = m + 0p$,*

Symmetrie: *Ist $n \sim_p m$, so finden wir ein $k \in \mathbb{Z}$ mit $n = m + kp$, und durch Umformen finden wir $m = n + (-k)p$. Damit gilt aber $m \sim_p n$.*

Transitivität: *Gelten $n_1 \sim_p n_2$ und $n_2 \sim_p n_3$, so finden wir k_1 und k_2 mit $n_1 = n_2 + k_1 p$ und $n_2 = n_3 + k_2 p$. Setzen wir die Gleichungen zusammen, finden wir $n_1 = n_3 + (k_1 + k_2)p$, und $k_1 + k_2$ ist als Summe ganzer Zahlen eine ganze Zahl. Deshalb folgt $n_1 \sim_p n_3$.*

Diese Äquivalenzrelation erzeugt genau p Äquivalenzklassen

$$\begin{aligned}
\overline{0} &= \{0, \pm p, \pm 2p, \pm 3p, \dots\} \\
\overline{1} &= \{1, 1 \pm p, 1 \pm 2p, 1 \pm 3p, \dots\} \\
\vdots \quad &\quad \vdots \\
\overline{p-1} &= \{-1, -1 \pm p, -1 \pm 2p, -1 \pm 3p, \dots\}.
\end{aligned}$$

Die p-elementige Faktormenge $\mathbb{Z}/_{\sim_p}$ wird in der Mathematik üblicherweise mit $\mathbb{Z}_p$ bezeichnet, und man nennt sie die ***Restklassen modulo*** *p.*

3.3.2.2. Ordnungsrelationen. Die zweite große Klasse von Relationen dient dazu, Mengen zu ordnen.

Definition 3.3.35 (Ordnung)**.**

(i) *Eine reflexive und transitive Relation* $\preceq$ *auf* M *heißt* Ordnungsrelation *oder* Halbordnung, *falls sie die folgende zusätzliche Eigenschaft erfüllt:*

Antisymmetrie: *Die Beziehungen* $a \preceq b$ *und* $b \preceq a$ *implizieren schon Gleichheit* $a = b$. *In Symbolen*

$$a \preceq b \wedge b \preceq a \Rightarrow a = b.$$

(ii) *Gilt für zwei Elemente von* M *weder* $x \preceq y$ *noch* $y \preceq x$, *so sagt man* x *und* y *sind* nicht vergleichbar *(bezüglich* $\preceq$*). Andernfalls nennt man die beiden Elemente* vergleichbar.

(iii) *Sind je zwei Elemente von* M *vergleichbar, gilt also für je zwei Elemente* $x, y \in M$ *wenigstens eine der Relationen* $x \preceq y$ *oder* $y \preceq x$, *so nennt man die Relation eine* Totalordnung *oder* lineare Ordnung *auf* M.

Betrachten wir eine Menge M zusammen mit einer Ordnungsrelation $\preceq$, so nennen wir das Paar $(M, \preceq)$ auch *geordnete Menge*.

Um mit Ordnungsrelationen leichter hantieren zu können, müssen wir einige Schreibweisen vereinbaren. Gilt $x \preceq y$, so schreiben wir auch manchmal $y \succeq x$. Haben wir $x \preceq y$ und gilt $x \neq y$, so kürzen wir ab zu $x \prec y$. Analog definieren wir $y \succ x$. Gilt andererseits $x = y$ oder $x \prec y$, so schreiben wir $x \preceq y$.

Beispiel 3.3.36.

- *Das bekannteste Beispiel für eine Ordnungsrelation (eine Totalordnung) ist die Beziehung* $\leq$ *auf den reellen Zahlen* $\mathbb{R}$.
- *Sei* M *die Menge aller Menschen. Wir definieren die Relation* $\prec$ *durch* $A \prec B$, *wenn* A *ein Vorfahre von* B *ist. Die entstehende Relation* $\preceq$ *ist klarerweise reflexiv und transitiv. Die Antisymmetrie folgt aus der Tatsache, dass kein Mensch Vorfahre von sich selbst sein kann. Es gibt aber Paare von Menschen, die nicht miteinander vergleichbar sind, für die also weder* $A \preceq B$ *noch* $A \succeq B$ *gelten. Die Relation „Ist Vorfahre von“ ist also eine Halbordnung auf* M.

So wie eine Äquivalenzrelation auf einer Menge M eine Struktur definiert, die wichtige Folgestrukturen entstehen lässt, erzeugt auch eine Ordnungsrelation auf M Folgebegriffe.

Definition 3.3.37 (Schranken)**.** *Sei* $(M, \preceq)$ *eine geordnete Menge, und sei* $E \subseteq M$ *eine Teilmenge.*

(i) *Gibt es ein* $\beta \in M$ *mit der Eigenschaft*

$$x \preceq \beta \text{ für jedes Element } x \in E,$$

so nennen wir β *eine* obere Schranke von E.

(ii) Untere Schranken *definiert man analog durch Ersetzen von* $\preceq$ *durch* $\succeq$.

(iii) *Die Teilmenge* E *heißt* nach oben (unten) beschränkt, *falls sie eine obere (untere) Schranke besitzt. Sie heißt* beschränkt, *falls sie nach oben und unten beschränkt ist.*

Beispiel 3.3.38.

- *Betrachten wir die geordnete Menge* $(\mathbb{R}, \leq)$. *Das Intervall* $E = [0, 1]$ *ist eine Teilmenge von* $\mathbb{R}$. *Jede Zahl im Intervall* $[1, \infty[$ *ist obere Schranke von* E, *und jede Zahl im Intervall* $]-\infty, 0]$ *ist untere Schranke von* E. E *ist also beschränkt.*
- *Die Menge* $M := \{1/n \mid n \in \mathbb{N} \setminus \{0\}\}$ *ist nach oben und unten beschränkt.* M *hat dieselben unteren und oberen Schranken wie* E.
- *Die Menge aller Primzahlen ist als Teilmenge von* $\mathbb{R}$ *nach unten beschränkt, sie besitzt aber keine obere Schranke.*

- *Die Menge $\mathbb{Z} \subset \mathbb{R}$ ist weder nach oben noch nach unten beschränkt.*

Wir sehen aus dem vorigen Beispiel, dass obere und untere Schranke bei weitem nicht eindeutig sind. Die interessante Frage ist, ob es eine ausgezeichnete obere bzw. untere Schranke gibt. Die Beantwortung dieser Frage für die geordnete Menge $(\mathbb{Q}, \leq)$ wird uns in Kapitel **??** zu den reellen Zahlen führen. Hier wollen wir uns mit einer Definition begnügen.

Definition 3.3.39 (Kleinste und größte Schranken). *Sei $(M, \preceq)$ eine geordnete Menge.*

(i) *Sei E eine nach oben beschränkte Teilmenge vom M. Existiert ein $\alpha \in M$ mit den Eigenschaften*
   (1) *α ist eine obere Schranke von E,*
   (2) *Ist $\gamma \prec \alpha$, so ist γ keine obere Schranke von E,*
   so nennen wir α die kleinste obere Schranke oder das Supremum *von E, und wir schreiben*
$$\alpha = \sup E$$
(ii) *Analog definieren wir die größte untere Schranke, das* Infimum
$$\alpha = \inf E$$
   einer nach unten beschränkten Teilmenge.
(iii) *Besitzt eine Teilmenge E ein Supremum (Infimum) α, und gilt $\alpha \in E$, dann nennen wir α auch das* Maximum *(*Minimum*) von E, in Zeichen* $\max E$ *(*$\min E$*).*

Beispiel 3.3.40. *Seien E und M wie in Beispiel 3.3.38. Es gilt $0 = \inf E = \inf M$ und $1 = \sup E = \sup M$. Für E sind 1 und 0 sogar Maximum bzw. Minimum. Für M ist 1 ein Maximum, aber 0 ist kein Minimum, da $0 \notin M$.*

3.3.3. Abbildungen. Wie bereits früher erwähnt, besteht ein großer Teil der modernen Mathematik in der Analyse von Strukturen. Diese Strukturen bestehen aus Objekten und den Beziehungen zwischen diesen Objekten. Wir haben schon erwähnt, dass *Mengen* für die meisten Strukturen die Basis bilden. Die in diesem Abschnitt behandelten Abbildungen sind die Basis für die Beziehungen zwischen den Objekten.

Wegen der zentralen Bedeutung des Begriffs Abbildung bzw. Funktion (diese beiden Bezeichnungen werden synonym verwendet; siehe auch unten) werden wir zwei Definitionen geben. Wir beginnen mit der weniger abstrakten, die Ihnen sicherlich bekannt vorkommen wird.

Definition 3.3.41 (Funktion). *Seien A und B Mengen.*

(i) *Unter einer* Funktion *oder* Abbildung f von A nach B *versteht man eine Vorschrift, die jedem $a \in A$* ***genau ein*** *$b \in B$ zuordnet.*
(ii) *Das dem Element a zugeordnete Element b bezeichnen wir mit $f(a)$ und nennen es* den Wert der Funktion f an der Stelle a *oder das* das Bild von a unter f*; a wird als* Urbild von b unter f *bezeichnet.*
(iii) *Weiters wird A als* Definitionsmenge *oder* -bereich *von f bezeichnet und B als* Zielmenge *oder* -bereich *von f.*

WICHTIG: Zur Festlegung einer Funktion **muß** man ausdrücklich Definitions- und Zielmenge angeben. Meist werden die Schreibweisen
$$f : A \to B \text{ oder } A \xrightarrow{f} B$$
verwendet. Die Angabe der Zuordnungsvorschrift alleine ist keinesfalls ausreichend (siehe auch Beispiel 3.3.50 unten)!

Das Symbol
$$a \mapsto f(a)$$

drückt aus, dass die Funktion f dem Element a des Definitionsbereichs das Bild $f(a)$ im Zielbereich zuordnet. Oft wird dieses Symbol auch zur Bezeichnung der Funktion selbst verwendet und man spricht von „der Funktion $a \mapsto f(a)$“ (lies: a geht über (in) $f(a)$). Dann muss allerdings Definitions- und Zielbereich gesondert angegeben werden.

Die ausführlichste und genaueste Darstellung einer Funktion erfolgt durch die Notation

$$\begin{array}{rcl} f : A & \to & B \\ a & \mapsto & f(a) \end{array} \qquad \text{bzw.} \qquad \begin{array}{rcl} f : A & \to & B \\ f(a) & = & \dots \end{array}$$

Beispiel 3.3.42. *Die Funktion, die jeder nichtnegativen reellen Zahl ihre Quadratwurzel zuordnet schreiben wir*

$$\begin{array}{rcl} f : [0,\infty[& \to & \mathbb{R} \\ x & \mapsto & \sqrt{x} \end{array} \qquad \textit{bzw.} \qquad \begin{array}{rcl} f : [0,\infty[& \to & \mathbb{R} \\ f(x) & = & \sqrt{x}. \end{array}$$

Einen Schönheitsfehler hat unserer Definition allerdings: sie beruht auf dem Wort „Zuordnung“, das wir strenggenommen gar nicht definiert haben — obwohl in diesem Fall die alltagssprachliche Bedeutung den mathematsichen Inhalt sehr genau trifft. Dieses Problem können wir umgehen indem wir eine rein mengentheoretische Definition des Funktionsbegriffs geben. Das ist unser nächstes Ziel.

Nach unserer obigen Definition setzt eine Funktion $f : A \to B$ die Elemente a von A mit gewissen Elementen $b = f(a)$ von B in Verbindung; fassen wir diese zu geordneten Paaren (a, b) zusammen, so folgt aus der Eindeutigkeit der Zuordnung, dass Paare mit gleichen ersten Komponenten gleiche zweite Komponenten besitzen, also bereits (als geordnetes Paar) gleich sind. Die durch f gegebene „Zuordnung“ kann deshalb als *spezielle* Teilmenge des Produkts $A \times B$ beschrieben werden. Genau das macht sich die folgende Definition zunutze.

Definition 3.3.43 (Mengentheoretische Definition des Funktionsbegriffs)**.** *Eine* Funktion *ist ein Tripel $f = (A, B, G)$ bestehend aus einer Menge A, genannt* Definitionsbereich*, einer Menge B, genannt* Zielbereich *und einer Teilmenge G des Produkts $A \times B$ mit den Eigenschaften*

(1) $\forall a \in A\ \exists b \in B : (a, b) \in G$
(D.h. jedes $a \in A$ tritt als erste Komponente eines Paares in G auf.)
(2) $\forall a \in A\ \forall b_1, b_2 \in B :\ (a, b_1) \in G \wedge (a, b_2) \in G\ \Rightarrow b_1 = b_2$
(D.h. stimmen die ersten Komponenten eines Paares in G überein, dann auch die zweiten.)

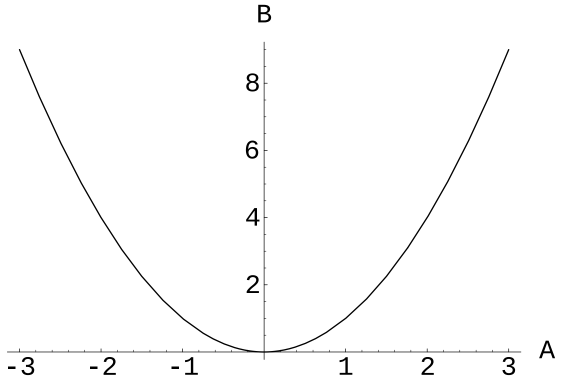
Die Menge G heißt Graph *der Funktion f und wird oft auch mit $G(f)$ bezeichnet. Gilt $(a, b) \in G$, so schreiben wir $f(a) = b$ und wir können den Graphen schreiben als*

$$G(f) = \{(a, f(a)|a \in A\}.$$

Die Paarungen $(a, f(a))$ sind gewissermaßen das abstrakte Analogon zur Zusammenstellung der a-Werte und der zugehörigen Funktionswerte $f(a)$ in einer Wertetabelle oder der graphischen Darstellung der Funktion als “Kurve“ in einem kartesischen Koordinatensystem (falls A und B Teilmengen von $\mathbb{R}$ sind); zwei Konzepte, die Ihnen sicherlich aus der Schule ein Begriff sind.

Vielleicht haben Sie bemerkt, dass wir noch immer nicht gesagt haben, *was* eine „Zuordnung“ denn eigentlich *ist*. Die moderne Mathematik zieht sich in dieser und ähnlichen Situationen aus der Affäre, indem Sie Ihnen die Objekte „aufzählt“, die einander „zugeordnet“ sind; in unserem Fall die geordneten Paare $(a, f(a))$. Nach dieser philosophischen Bemerkung kommen wir zu einem einfachen, konkreten Beispiel.

Beispiel 3.3.44. *Sei $A = \mathbb{R} = B$. Wir betrachten die Funktion $f : x \mapsto x^2$. Dann gilt $G = \{(x, x^2)|x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$, d.h. $(0, 0) \in G$, $(1, 1) \in G$, $(-1, 1) \in G$, $(2, 4) \in G$, …*



$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

Bemerkung 3.3.45. *Aus Definition 3.3.43 wird auch ersichtlich, dass jede Funktion $f : A \to B$ als spezielle Relation auf $A \times B$ aufgefasst werden kann: für jedes $a \in A$ existiert* genau ein *$b \in B$, mit dem es in Relation steht. Oft wird eine Funktion auch als derartige „eindeutige“ Relation* definiert.

Obwohl der Begriff der Abbildung zentral für die moderne Mathematik ist, wurde er erst sehr spät (im zwanzigsten Jahrhundert!) formalisiert. Daher existieren abhängig vom betrachteten Gebiet viele verschiedene Ausdrücke für Abbildung.

Der Terminus *Abbildung* ist der allgemeinste, doch der Begriff **Funktion** ist ein Synonym, auch wenn er meist dann verwendet wird, wenn B ein Körper (siehe Abschnitt **??**) ist.

Eine **Transformation** ist eine Abbildung einer Menge in sich (also für $A = B$). Eine bijektive (siehe Definition 3.3.49 (iii) unten) Transformation einer endlichen Menge heißt auch **Permutation**.

Ein **Operator** ist eine Abbildung zwischen Mengen von Abbildungen. So bildet etwa der *Ableitungsoperator* jede differenzierbare Funktion auf ihre Ableitungsfunktion ab.

Schließlich taucht besonders in der Linearen Algebra und der Funktionalanalysis der Begriff **Form** auf. Dieser beschreibt eine multilineare Abbildung in den Grundkörper eines Vektorraums (siehe Lineare Algebra!).

Es ist wichtig, in Texten zwischen der Funktion f und den Werten $f(x)$ einer Funktion zu unterscheiden.

Die Abbildung $f\cancel{(x)} \ldots$

Dafür hat man die $\mapsto$-Notation.

Die Abbildung $f : x \mapsto f(x) \ldots$

wäre in Ordnung.

Wir können mit Hilfe einer Abbildung ganze Teilmengen von A nach B abbilden.

Definition 3.3.46. *Sei $f : A \to B$ eine Abbildung, und sei $M \subseteq A$ eine Teilmenge. Wir nennen die Menge*

$$f(M) := \{b \in B \mid \exists a \in M : f(a) = b\}$$

das Bild der Menge M unter f.

Umgekehrt können wir für eine Teilmenge $N \subseteq B$ des Bildbereichs alle Elemente in A suchen, deren Bilder in N liegen.

Definition 3.3.47 (Urbild)**.** *Sei wieder $f : A \to B$ eine Abbildung.*

(i) *Sei $N \subseteq B$ eine Teilmenge des Bildbereichs. Wir definieren die Menge*

$$f^{-1}(N) := \{a \in A \mid f(a) \in N\}$$

und nennen sie das Urbild der Menge N unter f.

(ii) *Für ein Element $b \in B$ definieren wir das* Urbild von b *durch* $f^{-1}(b) := f^{-1}(\{b\})$. *Beachten Sie dabei, dass das Urbild von b* ***eine Menge*** *ist!*

Beispiel 3.3.48. *Betrachten wir nochmals die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$. Das Bild der Menge $M = [-1, 1]$ ist die Menge $f(M) = [0, 1]$. Das Urbild von $N = [-4, 4]$ ist die Menge $f^{-1}(N) = [-2, 2]$, und das Urbild des Punktes* 9 *ist* die Menge $f^{-1}(9) = \{-3, 3\}$.

Kommen wir jetzt zu *den* drei grundlegenden Eigenschaften von Abbildungen.

Definition 3.3.49 (Injektiv, surjektiv, bijektiv). *Sei $f : A \to B$ eine Abbildung.*

(i) *Wir sagen f ist* injektiv, *wenn jedes Element $b \in B$ von f* ***höchstens einmal*** *getroffen wird, d.h.* ***höchstens ein*** *Urbild hat. Anders ausgedrückt verlangen wir, dass verschiedene Urbilder auch verschiedene Bilder haben. In Symbolen können wir schreiben*

$$x \neq y \in A \Rightarrow f(x) \neq f(y) \quad \text{oder} \quad f(x) = f(y) \Rightarrow x = y.$$

(ii) *f heißt* surjektiv, *wenn* ***jedes*** *Element $b \in B$ von f* ***getroffen*** *wird, also* ***mindestens ein*** *Urbild besitzt. In Symbolen:*

$$\forall b \in B : \exists a \in A : f(a) = b.$$

(iii) *Wir nennen f* bijektiv, *wenn f injektiv und surjektiv ist. Das ist der Fall, wenn* ***jedes*** *Element in der Bildmenge B* ***genau ein*** *Urbild besitzt.*

Mitunter werden für die Begriffe *injektiv* und *bijektiv* auch die alten Begriffe *eindeutig* und *eineindeutig* verwendet. Das wäre ja leicht zu merken, doch unglücklicherweise verwenden manche Autoren den Begriff „eineindeutig“ statt für bijektiv für injektiv. Daher rate ich dringend zur Verwendung der lateinischen Bezeichnungen.

Ist $f : A \to B$ surjektiv, so sagt man auch f ist eine Abbildung von A **auf** B.

Wenn man Injektivität und Surjektivität von Abbildungen untersucht, ist es wichtig, nicht zu vergessen, Urbild- und Bildbereiche genau zu beachten. Wenn wir etwa die Zuordnungsvorschrift $x \mapsto x^2$ untersuchen, dann können wir abhängig von Definitions- und Bildbereich alle Varianten finden, wie uns das folgende Beispiel zeigt.

Beispiel 3.3.50. *Wir bezeichnen mit $\mathbb{R}_0^+$ die Menge der nichtnegativen reellen Zahlen, d.h. $\mathbb{R}_0^+ := \{x \in \mathbb{R} \mid x \geq 0\}$.*

- *$x \mapsto x^2 : \mathbb{R} \to \mathbb{R}$ ist weder injektiv noch surjektiv, weil $f(-1) = f(1)$, was der Injektivität widerspricht und -1 nicht von f getroffen wird, was die Surjektivität ausschließt.*
- *$x \mapsto x^2 : \mathbb{R}_0^+ \to \mathbb{R}$ ist injektiv aber nicht surjektiv.*
- *$x \mapsto x^2 : \mathbb{R} \to \mathbb{R}_0^+$ ist surjektiv aber nicht injektiv.*
- *$x \mapsto x^2 : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ ist bijektiv.*

Ein weiteres, wichtiges Beispiel für eine bijektive Abbildung ist für jede Menge M die **Identität**, die jedem $m \in M$ wieder m zuordnet, d.h.

$$\begin{aligned} \mathbb{1}_M : M &\to M \\ \mathbb{1}_X(m) &= m. \end{aligned}$$

In vielen Texten wird die Identität oder identische Abbildung auch mit id_M bezeichnet. Ist aus dem Zusammenhang klar, was die Menge M ist, so wird sie gerne notationell unterdrückt, d.h. man schreibt $\mathbb{1}$ oder id.

Sind $f : A \to B$ und $g : B \to C$ zwei Abbildungen, so können wir diese hinter einander ausführen, indem wir das Ergebnis von f in g einsetzen: $g(f(a))$. Dies ist ein wichtiges Konzept

Definition 3.3.51. *Seien $f : A \to B$ und $g : B \to C$ zwei Abbildungen. Wir definieren die* Verknüpfung von f mit g *(oder die* Hintereinanderausführung von f und g*) in Zeichen, $g \circ f : A \to C$ durch*

$$(g \circ f)(a) := g(f(a)).$$

Sind $f : A \to B$, $g : B \to C$ und $h : C \to D$ drei Abbildungen, so gilt das **Assoziativgesetz** $(f \circ g) \circ h = f \circ (g \circ h)$ (dies folgt leicht aus der Definition). Man darf also beim Zusammensetzen von Abbildungen die Klammern weglassen.

Ist $f : A \to B$ bijektiv, so gibt es zu jedem Bild $b \in B$ genau ein Urbild $a \in A$ mit $f(a) = b$. Diese Tatsache können wir benutzen, um eine neue Funktion, die Umkehrfunktion von f zu konstruieren, die jedem $b = f(a)$ *das* Urbild a zuordnet. Die Surjektivität von f garantiert dabei, dass *jedem* b ein a zugeordnet werden kann, die Injektivität von f hingegen, dass die Zuordnung eindeutig ist.

Definition 3.3.52. *Sei $f : A \to B$ bijektiv. Die* inverse Abbildung von f *oder die* Umkehrfunktion von f *ist definiert durch*

$$\begin{aligned} f^{-1} : B &\to A \\ f(a) &\mapsto a. \end{aligned}$$

Verwechseln Sie nicht die Umkehrfunktion f^{-1}, die wir nur für bijektive Abbildungen f definiert haben mit der "Mengenabbildung" aus 3.3.47, die für beliebiges f existiert! Um die latent vorhandene Verwechslungsgefahr zu entschärfen wird das alleinstehende Symbol f^{-1} nur für die inverse Abbildung verwendet; für die "Mengenabbildung", die einer Teilmenge C des Bildbereichs ihr Urbild zuordnet wird das Symbol f^{-1} ausschließlich zusammen mit der Menge verwendet, also $f^{-1}(C)$. Ist f bijektiv, so könnte $f^{-1}(C)$ allerdings auch das Bild von C unter f^{-1} bezeichnen; das ist aber kein Problem, da dieses mit dem Urbild von C unter f übereinstimmt! Bleibt alleine das Problem, dass $f^{-1}(b)$ für ein $b \in B$ einerseits das Bild von $b \in B$ unter der inversen Funktion f^{-1} und andererseits das Urbild von $\{b\} \subseteq B$ unter f (vgl. Definition 3.3.47(ii)) bezeichnet. Da f injektiv ist, ist letzteres die einelementige Menge $\{f^{-1}(b)\} \subseteq A$, sodass $f^{-1}(b)$ im ersten Fall ein Element von A bezeichnet im zweiten eine Teilmenge von A, die als einziges Element eben $f^{-1}(b)$ enthält; welche der beiden Möglichkeiten gemeint ist, wird aber immer aus dem Zusammenhang klar sein. Auch wenn Ihnen obige Bemerkung spitzfindig erscheint: wenn Sie sie verstehen, können Sie sicher sein, die Begriffe Bild, Urbild und Umkehrfunktion *gut* verstanden zu haben!

Bemerkung 3.3.53. *Die Zusammensetzung von f mit der Umkehrabbildung ergibt für alle $a \in A$ und alle $b \in B$, wie man leicht einsehen kann*

$$f(f^{-1}(b)) = b, \qquad f^{-1}(f(a)) = a$$

oder in Funktionsnotation

$$f \circ f^{-1} = \mathbb{1}_B, \qquad f^{-1} \circ f = \mathbb{1}_A.$$

Ein erstes Beispiel für eine mathematische Struktur war diejenige einer Menge. Die zugehörigen Beziehungen sind die Abbildungen. Wir haben aber im letzten Abschnitt eine weitere, etwas spezialisierte Struktur definiert, die *geordnete Menge*. Was sind die Beziehungen zwischen geordneten Mengen? Ganz einfach: Diejenigen Abbildungen, die die Ordnungsstruktur erhalten, also die monotonen Abbildungen.

Definition 3.3.54 (Monotonie). *Seien $(A, \preceq)$ und $(B, \trianglelefteq)$ zwei geordnete Mengen. Eine Abbildung $f : A \to B$ heißt* monoton wachsend, *falls aus $a \preceq b$ schon $f(a) \trianglelefteq f(b)$ folgt. Sie heißt* monoton fallend, *falls sich aus $a \preceq b$ die Relation $f(a) \trianglerighteq f(b)$ ergibt.*

Beispiel 3.3.55. *Die Funktion $f : \mathbb{R}_0^+ \to \mathbb{R}$ mit der Definition $f(x) = x^2$ ist monoton wachsend.*

Wir haben also bereits zwei Beispiele für typische mathematische Strukturen kennengelernt: *Mengen und Abbildungen* und *geordnete Mengen und monotone Abbildungen*.

Hat man zwei Mengen A und B, so können wir alle Abbildungen von A nach B wieder zu einer Menge zusammenfassen, der **Menge aller Abbildungen von A nach B**, die oft mit B^A bezeichnet wird. Warum das so ist, können wir gleich sehen.

Zuletzt, sei nämlich wie versprochen noch die Definition des Cartesischen Produktes von zwei Mengen auf beliebig viele Mengen verallgemeinert.

Definition 3.3.56. *Seien M_i, $i \in I$ Mengen. Wir definieren*

$$\prod_{i\in I} M_i := \bigtimes_{i\in I} M_i := \{f : I \to \bigcup_{i\in I} M_i \mid \forall i \in I : f(i) \in M_i\}$$

das Cartesische Produkt *der M_i.*

Sind alle Mengen $M_i = M$ gleich, dann schreiben wir statt $\prod_{i\in I} M$ auch M^I, und das stimmt mit der oberen Bezeichnung von M^I als Menge aller Abbildungen von I nach M überein!

Man beachte, dass diese Definition für endliche Indexmengen I äquivalent ist zur Definition mit k-tupeln. Haben wir etwa die Mengen M_0 und M_1, dann ist unsere Indexmenge $I = \{0, 1\}$. Setzen wir in die Definition 3.3.56 ein, so erhalten wir

$$M_0 \times M_1 = \{f : \{0, 1\} \to M_0 \cup M_1 \mid f(0) \in M_0 \wedge f(1) \in M_1\}. \tag{3.2}$$

Eine Abbildung f von $\{0, 1\}$ aus in irgendeine Menge ist schon eindeutig bestimmt durch die Werte bei 0 und 1. Die einzige Forderung an f ist, dass $f(0) \in M_0$ und $f(1) \in M_1$ liegen müssen. Verstehen wir nun die Indexmenge I als Positionsangaben und schreiben wir die Abbildung f ein wenig anders auf, dann sehen wir

$$\begin{array}{cccccc} I & & 0 & & 1 & \\ & (& f(0) & , & f(1) &), \\ & & \in M_0 & & \in M_1 & \end{array}$$

dass jede Funktion einem geordneten Paar entspricht, dessen erster Eintrag in M_0 liegt, und dessen zweiter Eintrag Element von M_1 sein muss. Alle möglichen Funktionen die die Form von (3.2) haben, findet man, indem man $f(0)$ alle möglichen Elemente von M_0 durchlaufen lässt und für $f(1)$ jedes Element von M_1 einsetzt. Man konstruiert also wirklich alle geordneten Paare von M_0 und M_1.

Zum weiteren Verständnis wollen wir die Konstruktion für $I = \{0, 1, 2\}$ und $M_0 = \{a, b\}$, $M_1 = \{1, 2, 3\}$ und $M_2 = \{\alpha, \beta\}$ genau vorrechnen:

$$\begin{aligned} M_0 \times M_1 \times M_2 = \{&(a, 1, \alpha), (a, 1, \beta), (a, 2, \alpha), (a, 2, \beta), (a, 3, \alpha), (a, 3, \beta),\\ &(b, 1, \alpha), (b, 1, \beta), (b, 2, \alpha), (b, 2, \beta), (b, 3, \alpha), (b, 3, \beta\} \end{aligned}$$

entspricht unserer ursprünglichen Definition durch Tripel (3-tupel).

Untersuchen wir die Menge aller Abbildungen

$$\begin{aligned} X := \{f : \{0, 1, 2\} \to M_0 \cup M_1 \cup M_2 = \{1, 2, 3, a, b, \alpha, \beta\} \mid \\ f(0) \in \{a, b\} \wedge f(1) \in \{1, 2, 3\} \wedge f(2) \in \{\alpha, \beta\}\}. \end{aligned} \tag{3.3}$$

Es gibt zwölf verschiedene Abbildungen in dieser Menge X:

$$\begin{array}{llll}
f_0 : 0 \mapsto a & f_1 : 0 \mapsto a & f_2 : 0 \mapsto a & f_3 : 0 \mapsto a \\
\quad 1 \mapsto 1 & \quad 1 \mapsto 1 & \quad 1 \mapsto 2 & \quad 1 \mapsto 2 \\
\quad 2 \mapsto \alpha & \quad 2 \mapsto \beta & \quad 2 \mapsto \alpha & \quad 2 \mapsto \beta \\
& & & \\
f_4 : 0 \mapsto a & f_5 : 0 \mapsto a & f_6 : 0 \mapsto b & f_7 : 0 \mapsto b \\
\quad 1 \mapsto 3 & \quad 1 \mapsto 3 & \quad 1 \mapsto 1 & \quad 1 \mapsto 1 \\
\quad 2 \mapsto \alpha & \quad 2 \mapsto \beta & \quad 2 \mapsto \alpha & \quad 2 \mapsto \beta \\
& & & \\
f_8 : 0 \mapsto b & f_9 : 0 \mapsto b & f_{10} : 0 \mapsto b & f_{11} : 0 \mapsto b \\
\quad 1 \mapsto 2 & \quad 1 \mapsto 2 & \quad 1 \mapsto 3 & \quad 1 \mapsto 3 \\
\quad 2 \mapsto \alpha & \quad 2 \mapsto \beta & \quad 2 \mapsto \alpha & \quad 2 \mapsto \beta
\end{array}$$

Sorgfältiger Vergleich zwischen den Mengen X und $M_0 \times M_1 \times M_2$ zeigt, dass in der Tat beide Mengen dasselbe beschreiben.

Beispiel 3.3.57. *Die Menge aller Abbildungen von $\mathbb{N}$ nach $\mathbb{R}$ (oder das Cartesische Produkt von „$\mathbb{N}$-vielen Kopien von $\mathbb{R}$“) ist die Menge aller reellen Zahlenfolgen*

$$(x_0, x_1, x_2, x_3, \dots), \qquad \textit{mit } x_i \in \mathbb{R} \textit{ für } i \in \mathbb{N}.$$

3.3.4. Mächtigkeit. Eine interessante Eigenschaft von Mengen, die diesen intrinsisch ist, ist ihre **Mächtigkeit**. Wie fast alles in der Mengenlehre geht auch dieses Konzept auf Georg Cantor zurück. Für unendliche Mengen hat er als erster definiert, wann es legitim ist zu sagen, dass zwei Mengen A und B *gleich mächtig* (gleich groß) sind.

Für endliche Mengen M ist die Mächtigkeit $|M|$ einfach die Anzahl ihrer Elemente. Für unendliche Mengen müssen wir aber etwas trickreicher vorgehen.

Definition 3.3.58. *Zwei Mengen A und B heißen* gleich mächtig, *wenn eine bijektive Abbildung (eine Bijektion) von A auf B existiert. In diesem Fall sagt man auch A und B haben gleiche* Kardinalität *oder die gleiche* Kardinalzahl *und schreibt* $\operatorname{card}(A) = \operatorname{card}(B)$.

Diese einfache Definition hat weit reichende Konsequenzen. Es wird unter anderem möglich, dass eine Menge zu einer ihrer echten Teilmengen gleich mächtig ist.

Beispiel 3.3.59. *Betrachten wir die Menge $\mathbb{N}$ und die Menge $\mathbb{N}_g$ aller geraden Zahlen. Es gilt $\mathbb{N}_g \subsetneqq \mathbb{N}$, doch die Abbildung $f : \mathbb{N} \to \mathbb{N}_g$ mit $f : x \mapsto 2x$ ist eine Bijektion. Die Mengen $\mathbb{N}$ und $\mathbb{N}_g$ sind also gleich mächtig.*

Es stellt sich heraus, dass nur die endlichen Mengen die Eigenschaft haben, eine größere Mächtigkeit zu besitzen als alle ihre echten Teilmengen.

Proposition 3.3.60. *Eine Menge ist unendlich genau dann, wenn sie eine gleich mächtige echte Teilmenge besitzt.*

Beweis. Ohne Beweis. □

Schon Cantor hat gezeigt, dass aus der Mächtigkeitsdefinition gefolgert werden kann, dass unendlich große Mengen nicht gleich groß zu sein brauchen. **Es gibt auch bei unendlichen Menge Größenunterschiede**. In der Mengentheorie ist also „unendlich nicht gleich unendlich“.

Das Wort *unendlich* ist in der Mathematik allgegenwärtig. Die meisten vom Mathematiker behandelten Gegenstände sind unendlich (z.B. $\mathbb{N}$, $\mathbb{R}^n$, $\dots$), die meisten Aussagen in mathematischen Theorien handeln von unendlich vielen Objekten.

Das Symbol für den Ausdruck *unendlich* ist ∞. Dass es ein (und nur ein) Symbol für „unendlich“ gibt, führt leider oft zu Missverständnissen, wird doch von vielen daraus geschlossen, dass man mit unendlich so umgehen kann wie mit den reellen oder komplexen Zahlen.

Eine Menge M hat unendlich viele Elemente

Diese Aussage bedeutet, dass es keine natürliche Zahl n gibt mit $|M| = n$. Man schreibt abkürzend manchmal $|M| = \infty$. Es bezeichnet $|M|$ die Mächtigkeit (**Kardinalität**) von M, doch ∞ ist keine Kardinalzahl. Daher ist obige Formulierung *keine* mathematisch exakte Aussage.

Man verwendet ∞ bei der Beschreibung von Grenzübergängen wie etwa in

$$\lim_{n\to\infty} a_n$$

oder in

Für $n \to \infty$ strebt die Folge $(x_n)_n$ gegen x.

Auch hier ist ∞ nur eine *Abkürzung* für die ε-δ-Definition, die Sie in der Analysis noch sehr genau studieren werden. Dasselbe gilt für die Notation in unendlichen Reihen, z.B.

$$\sum_{n=1}^{\infty} \frac{1}{n^2}.$$

Eine wirkliche mathematische Bedeutung hat das Symbol ∞ etwa in der Maßtheorie, in der die Menge $\bar{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$ eingeführt wird. In diesem Fall bezeichnet ∞ ein bestimmtes von allen reellen Zahlen wohlunterschiedenes Element von $\bar{\mathbb{R}}$ mit genau definierten Eigenschaften. Auch in der projektiven Geometrie kommt das Symbol ∞ vor, und auch dort hat es eine genau festgelegte Bedeutung. In diesen Fällen ist ∞ keine Abkürzung mehr; dort hat es aber auch eine fixe Bedeutung frei von Mythen.

Ihnen wird vielleicht aufgefallen sein, dass wir nur definiert haben, was es für zwei Mengen bedeutet, die gleiche Kardinalzahl zu haben, aber nicht, was eine Kardinalzahl ist; dies geht über den Rahmen dieser Vorlesung hinaus. Wir befinden uns hier in etwa in der Situation eines Cowboys, der die Größe zweier Rinderherden vergleichen soll, ohne weit genug zählen zu können. Um festzustellen, ob die beiden Herden gleich viele Tiere enthalten braucht man diese aber nur paarweise durch ein Tor laufen zu lassen!

Was ist eigentlich die „kleinste“ unendliche Menge? Diese Frage läßt sich beantworten. Es kann relativ leicht gezeigt werden, dass jede unendliche Menge mindestens so groß wie $\mathbb{N}$ sein muss.

Heuristisch lässt sich das so begründen: Wenn wir $\mathbb{N}$ genauer untersuchen, dann erkennen wir folgende Eigenheit: In der natürlichen Ordnung von $\mathbb{N}$ besitzt jede Teilmenge $T \subset \mathbb{N}$ ein kleinstes Element (ein Minimum). Man sagt, die Menge $\mathbb{N}$ ist **wohlgeordnet**. Nun finden wir, dass für Teilmengen T von $\mathbb{N}$ nur zwei Möglichkeiten in Betracht kommen.

(1) Die Menge T ist nach oben beschränkt. Dann ist T endlich. Ist nämlich α eine obere Schranke von T, so ist T Teilmenge der endlichen Menge $\{0, 1, \dots, \alpha\}$.
(2) Die Menge T ist nicht nach oben beschränkt. Dann kann man zu jedem Element t in T das nächst größere Element t' in T finden. Auf diese Weise kann man die Elemente von T durchnummerieren und eine Bijektion auf $\mathbb{N}$ konstruieren.

Also ist jede Teilmenge von $\mathbb{N}$ entweder endlich oder unendlich und genauso groß wie $\mathbb{N}$ selbst. „Zwischen“ den endlichen Mengen und $\mathbb{N}$ gibt es also keine Größenordnung mehr.

Um über die Mächtigkeit von $\mathbb{N}$ reden zu können, müssen wir ein neues Symbol einführen. Wir schreiben $|\mathbb{N}| =: \aleph_0$ (dieser Buchstabe stammt aus dem hebräischen Alphabet und heißt

Aleph; die Mächtigkeit von $\mathbb{N}$ ist also Aleph-Null) und nennen jede Menge, die gleich mächtig mit $\mathbb{N}$ ist, also Kardinalität $\aleph_0$ hat, **abzählbar**.

Cantor hat bereits knapp vor der Jahrhundertwende bewiesen, dass $\mathbb{N} \times \mathbb{N}$ abzählbar ist. Dazu hat er das nach ihm benannte Diagonalverfahren verwendet, das unten dargestellt ist. Alle geordneten Paare in $\mathbb{N} \times \mathbb{N}$ werden in einem Rechteckschema angeschrieben und entlang der Pfeile der Reihe nach durchlaufen; so wird eine Bijektion auf $\mathbb{N}$ hergestellt.

$$
\begin{tikzcd}
(0,0) \arrow[r] & (1,0) \arrow[dl] & (2,0) \arrow[dl] & (3,0) \arrow[dl] & \cdots \\
(0,1) \arrow[urr] & (1,1) \arrow[dl] & (2,1) \arrow[dl] & \cdots & \\
(0,2) \arrow[uurrr] & (1,2) \arrow[dl] & \cdots & & \\
(0,3) \arrow[uurrr, dotted, no head] & \cdots & & & \\
\vdots & \ddots & & &
\end{tikzcd}
$$

Eine Formel für die Zuordnung ist

$$f : (i, j) \mapsto \tfrac{1}{2}(i + j)(i + j + 1) + j.$$

Nachdem die positiven resp. die negativen rationalen Zahlen $\mathbb{Q}$ als Teilmenge von $\mathbb{N} \times \mathbb{N}$ aufgefasst werden können ($q = \pm\frac{m}{n}$ für zwei teilerfremde natürliche Zahlen m und $n \neq 0$), ist also auch $\mathbb{Q}$ abzählbar. Auch die Vereinigung von abzählbar vielen abzählbaren Mengen ist wieder abzählbar. Das kann man mit Hilfe des gleichen Prinzips beweisen (schreibe in Gedanken alle Mengen untereinander auf und konstruiere die Bijektion analog zur Diagonalabzählung).

Cantor hat aber auch bewiesen, dass es verschiedene Größenklassen von Mengen gibt. So ist etwa die Potenzmenge $\mathbb{P}M$ einer Menge M **immer** mächtiger als M selbst (die Mächtigkeit der Potenzmenge einer Menge erfüllt $|\mathbb{P}M| = 2^{|M|}$).

Interessant ist, dass die reellen Zahlen $\mathbb{R}$ mächtiger sind als $\mathbb{N}$. Man sagt, die reellen Zahlen sind **überabzählbar**. Das hat ebenfalls Cantor gezeigt.

Cantor hat bewiesen, dass $]\,0, 1\,[$ überabzählbar ist. Die Tatsache, dass $]\,0, 1\,[$ die gleiche Mächtigkeit wie $\mathbb{R}$ hat, ist einfach zu zeigen. So bildet etwa die Funktion $\frac{1}{\pi}(\arctan(x) + \frac{\pi}{2})$ ganz $\mathbb{R}$ bijektiv auf $]\,0, 1\,[$ ab. Zum Beweis der Überabzählbarkeit von $]\,0, 1\,[$ verwenden wir die Tatsache, dass sich jede reelle Zahl r als Dezimalentwicklung aufschreiben lässt, und dann gehen wir indirekt vor. Angenommen, es gäbe eine Bijektion b von $\mathbb{N}$ auf $]\,0, 1\,[$. Dann stellen wir uns vor, dass wir alle Zahlen in der Reihenfolge untereinander schreiben wie sie durch die Bijektion auf $\mathbb{N}$ gegeben ist. Im nachfolgenden Diagramm mögen die a_{ij} für Dezimalziffern stehen. Die oberste Reihe repräsentiere die Dezimalentwicklung der ersten Zahl, die nächste Zeile die der zweiten, usw. Wäre $\mathbb{R}$ abzählbar, so müsste in diesem Schema *jede* reelle Zahl aus $]\,0,1\,[$ irgendwo auftauchen.

$$\begin{array}{llllllll}
0: & 0, & \mathbf{a_{01}} & a_{02} & a_{03} & a_{04} & a_{05} & a_{06} & \cdots \\
1: & 0, & a_{11} & \mathbf{a_{12}} & a_{13} & a_{14} & a_{15} & a_{16} & \cdots \\
2: & 0, & a_{21} & a_{22} & \mathbf{a_{23}} & a_{24} & a_{25} & a_{26} & \cdots \\
3: & 0, & a_{31} & a_{32} & a_{33} & \mathbf{a_{34}} & a_{35} & a_{36} & \cdots \\
4: & 0, & a_{41} & a_{42} & a_{43} & a_{44} & \mathbf{a_{45}} & a_{46} & \cdots \\
5: & 0, & a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & \mathbf{a_{56}} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Betrachten wir jetzt die reelle Zahl r mit der Dezimalentwicklung

$$r = 0, \widehat{a_{01}}\ \widehat{a_{12}}\ \widehat{a_{23}}\ \widehat{a_{34}}\ \widehat{a_{45}}\ \widehat{a_{56}} \ldots \widehat{a_{n\,n+1}} \ldots,$$

wobei wir $\widehat{a_{ij}}$ definieren durch

$$\widehat{a_{ij}} := \begin{cases} a_{ij} + 2 & \text{falls } a_{ij} \leq 4 \\ a_{ij} - 2 & \text{falls } a_{ij} \geq 5 \end{cases}$$

Versuchen wir nun herauszufinden, an welcher Stelle r in der Liste eingetragen ist, so müssen wir feststellen, dass r gar nicht in der Aufzählung enthalten sein kann. Sei nämlich n diejenige natürliche Zahl mit $b(n) = r$. Dann gilt aber

$$\begin{aligned} b(n) &= 0,\ a_{n1}\ a_{n2}\ a_{n3}\ a_{n4}\ a_{n5}\ a_{n6} \ldots \\ r &= 0,\ \widehat{a_{01}}\ \widehat{a_{12}}\ \widehat{a_{23}}\ \widehat{a_{34}}\ \widehat{a_{45}}\ \widehat{a_{56}} \ldots \end{aligned}$$

Damit wirklich $b(n) = r$ gilt, müssen die Dezimalentwicklungen von $b(n)$ und r überein stimmen. Es gilt aber $\widehat{a_{n,n+1}} \neq a_{n,n+1}$. Daher sind $b(n)$ und r verschieden, und r war tatsächlich nicht in der Liste enthalten.

Genauer untersuchend sieht man, dass $\mathbb{R}$ gleich mächtig ist mit der Potenzmenge von $\mathbb{N}$. Man könnte nun vermuten, dass $\mathbb{R}$ die nächst höhere Mächtigkeit nach $\aleph_0$ besitzt, also $\aleph_1$.

Trotzdem bezeichnet man aus gutem Grund die Mächtigkeit von $\mathbb{R}$ mit $|\mathbb{R}| = c$, der Mächtigkeit des Kontinuums. Es lässt sich nämlich nicht $c = \aleph_1$ beweisen (**man kann beweisen, dass sich das nicht beweisen lässt** — das hat Kurt Gödel 1938 getan), es lässt sich übrigens auch nicht widerlegen (das hat Paul J. Cohen (geb. 1934) 1963 **bewiesen**). Die sogenannte **Kontinuumshypothese** von Georg Cantor, dass $c = \aleph_1$ ist, ist **unabhängig von den Axiomen der Mengenlehre**. Das heißt, es gibt *Modelle* der axiomatischen Mengenlehre, in denen $c = \aleph_1$ gilt und andere *Modelle*, in denen $c \neq \aleph_1$ zutrifft. Die Axiomatisierung des Mengenbegriffs bringt solche unangenehme Fakten mit sich, die zeigen, dass es noch nicht geschafft wurde, den naiven Mengenbegriff so gut zu axiomatisieren, dass die Axiome unsere Vorstellungswelt ganz einzufangen im Stande sind.

3.4. Axiomatische Mengenlehre

3.4.1. Die Axiome von Zermelo und Fraenkel. Eine Möglichkeit, die Mathematik auf ein festes Fundament zu stellen, ist die Axiomatisierung der Mengenlehre nach Zermelo und Fraenkel. Mit der Festlegung dieser *Axiome* gibt man ihr einen Satz von Grundaussagen. Aus diesen werden dann die mathematischen Theoreme abgeleitet, auf diesen Fundamenten wird das Gebäude der Mathematik entwickelt — theoretisch jedenfalls.

Der Ursprung der axiomatischen Mengenlehre liegt in den Paradoxien, die die naive Mengenlehre um die Jahrhundertwende geplagt haben, wie etwa die Russellsche Antinomie („die Menge aller Mengen, die sich nicht selbst enthalten"). Sie wurde 1908 von Zermelo erfunden, aber mittlerweile hat sie eine große Bedeutung gewonnen. Die Mengenlehre ist die

Basis für beinahe die gesamte Mathematik, und ihre Axiomatisierung erlaubt es, diese Basis einwandfrei zu legen.

Es gibt mehrere verschiedene Axiomensysteme, die alle die naive Mengenlehre präzisieren aber untereinander fundamentale Unterschiede aufweisen. Wir präsentieren hier die Axiome von Zermelo und Fraenkel (ZFC), etwa im Gegensatz zu den Systemen von Neumann-Bernays-Gödel oder Morse-Kelley, auch weil die Einführung von *Klassen* dadurch vermieden werden kann.

Grundlage für die Axiomatisierung der Mengenlehre ist die Logik, und obwohl man auch die Theorie der Aussagen (Aussagenlogik, Prädikatenlogik) formal exakt machen könnte, werden wir hier stoppen und die logischen Grundlagen naiv verwenden. Es sei nur festgehalten, dass *alle* auftretenden Zeichen Bedeutung in der Logik haben (auch $=$) mit der einzigen Ausnahme $\in$, und dass φ und ψ beliebige Formeln bezeichnen, deren Variable in Klammern angegeben werden.

Mit Hilfe der ersten sechs ZFC Axiome kann die gesamte *endliche* Mathematik konstruiert werden. Sie lauten wie folgt:

ZF1: $\exists x : (x = x)$ (Existenz)
ZF2: $\forall x : \forall y : \forall z : ((z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$ (Extensionalität)
ZF3: $\forall U : \forall p : \forall Z : \forall x : (x \in Z \Leftrightarrow (x \in U \wedge \varphi(x, p)))$ (Separation)
ZF4: $\forall x : \forall y : \exists Z : (x \in Z \wedge y \in Z)$ (Paare)
ZF5: $\forall \mathcal{F} : \exists Z : \forall F : \forall x : ((x \in F \wedge F \in \mathcal{F}) \Rightarrow x \in Z)$ (Vereinigung)
ZF6: $\forall U : \exists \mathcal{Z} : \forall Y : (\forall x : (x \in Y \Rightarrow x \in U) \Rightarrow Y \in \mathcal{Z})$ (Potenzmenge)

Für die Formulierung der folgenden Axiome ist ein wenig Erklärung von Nöten, und außerdem müssen wir einige Abkürzungen einführen. Das Axiom ZF1 stellt sicher, dass Mengen existieren, und ZF2 erklärt, dass zwei Mengen genau dann gleich sind, wenn sie dieselben Elemente haben. Mit Hilfe von ZF3 wird das erste Konstruktionsprizip für neue Mengen eingeführt, die Auswahl einer Teilmenge Z aus einer *gegebenen* Menge U mit Hilfe einer „Auswahlregel" φ. Für diese Menge Z führen wir die Abkürzung $\{x \in U \mid \varphi(x)\}$ ein. Weitere Abkürzungen seien die Formulierungen $\forall x \in U$, die für $\forall x : x \in U$ stehe, und $\exists x \in U$ für $\exists x : x \in U$. ZF3 besagt in gewisser Art und Weise, dass man für *jedes* Element einer Menge überprüfen kann, ob es eine bestimmte Eigenschaft φ aufweist oder nicht. Das ist natürlich nur theoretisch möglich, weshalb dies schon von E. Bishop in [**Bishop 1967**] als *Prinzip der Allwissenheit* bezeichnet wurde.

Aus ZF4 definieren wir $\{x, y\} := \{z \in Z \mid z = x \vee z = y\}$ und $\{x\} := \{x, x\}$. Das Vereinigungs-Axiom ZF5 ermöglicht es uns mit Hilfe von $\mathcal{F} = \{X, Y\}$ zu definieren

$$X \cup Y := \{z \in Z \mid z \in Z \vee z \in Y\}.$$

Drei weitere Symbole müssen wir einführen, um die weiteren Axiome formulieren zu können. Es sind dies das *Leere Menge-Symbol* $\emptyset := \{z \in Z \mid \neg(z = z)\}$ für eine fixe Menge Z und $S(x) := x \cup \{x\}$. Schließlich erklären wir das (uns bereits naiv bekannte) Symbol $\exists!$ durch folgende Abkürzungsvereinbarung

$$\exists! y : \varphi(y) \text{ entspreche } \exists y : \varphi(y) \wedge (\forall y : \forall x : (\varphi(y) \wedge \varphi(x)) \Rightarrow x = y).$$

Die drei nächsten Axiome sind dann:

ZF7: $\exists Z : \forall X : (\emptyset \in Z \wedge (X \in Z \Rightarrow S(X) \in Z))$ (Unendlichkeit)
ZF8: $\forall U : \forall p : \big(\forall x \in U : \exists! z : \varphi(x, z, U, p) \Rightarrow$
$\exists Z : \forall x \in U : \exists z \in Z : \varphi(x, z, U, p)\big)$ (Ersetzung)
ZF9: $\forall x : \big(\neg(x = \emptyset) \Rightarrow \exists y : (y \in x \wedge \neg \exists z : (z \in x \wedge z \in y))\big)$ (Fundierung)

Hier ist wieder einiges an Erläuterungen von Nöten. ZF7 garantiert die Existenz einer Menge mit den Elementen $\emptyset, S(\emptyset), S(S(\emptyset)), \ldots$. Diese scheinbar schräge Konstruktion wird aber sofort verständlicher, wenn man die Bezeichungen $0 := \emptyset$, $1 := S(\emptyset)$, $2 := S(S(\emptyset))$, und allgemein $n+1 := S(n)$ einführt.

ZF8 hat die komplexeste Formel, doch dieses Axiom stellt nichts anderes sicher als dass man aus einer Menge U und einer Zuordnung f, die jeder Menge $x \in U$ eine Menge y zuordnet, eine weitere Menge als Bild von U unter f konstruieren kann. Dieses Axiom rechtfertigt auch die Abkürzung $\{f(x) \mid x \in U\}$ für die Definition einer Menge.

Das Fundierungsaxiom ZF9 zu guter Letzt schließt unter anderem die Russellsche Antinomie aus zusammen mit allen Mengen, die in gewissem Sinne „zu groß“ sind. Es werden alle Mengen verboten, die sich selbst enthalten oder aber Mengen enthalten, die wiederum andere Mengen enthalten, und so weiter ad infinitum.

Das letzte Axiom von ZFC hat in der Vergangenheit viele Kontroversen verursacht, da es dem Mathematiker gestattet, auf nicht konstruktivem Weg neue Mengen zu definieren. Analog zum Prinzip der Allwissenheit könnte man das Axiom auch wie J. Cigler und H.C. Reichel in [**Cigler, Reichel 1987**] als das *Prinzip der Allmächtigkeit* bezeichnen. Heute akzeptiert ein überwiegender Teil der Mathematiker dieses Axiom auf Grund seiner Verwendbarkeit und der Vielfalt praktischer Theoreme, die zu diesem Axiom äquivalent sind. Zuvor wir das Axiom aber anführen benötigen wir eine weitere Abkürzung

$$F \cap G := \{z \in F \cup G \mid z \in F \wedge z \in G\}.$$

Das zehnte Axiom, das Auswahlaxiom, ist

ZF10: $$\forall \mathcal{F} : \big(\forall H \in \mathcal{F} : \neg(H = \emptyset) \wedge \forall F \in \mathcal{F} : \forall G \in \mathcal{F} : (F = G \vee F \cap G = \emptyset) \Rightarrow \exists S : \forall F \in \mathcal{F} : \exists! s (s \in S \wedge s \in F)\big) \qquad \text{(Auswahl)}$$

Es besagt, dass es zu jeder gegebenen Familie von nichtleeren, paarweise disjunkten Mengen M_i, $i \in I$ eine weitere Menge gibt, die aus jedem M_i genau ein Element enthält.

Diese axiomatische Einführung der Mengen ist nicht umfassend. Andere Axiomensysteme wie von Neumann-Bernays-Gödel oder Morse-Kelley wurden nicht behandelt. Dieser Abschnitt sollte nur einen kurzen Einblick geben ein tatsächliches Fundament der Mathematik. Weiterführende Information kann man in den Vorlesungen „Grundbegriffe der Mathematik“ und „Axiomatische Mengenlehre“ finden.

Kapitel 4

Algebra

to be done

Kapitel 5

Zahlenmengen

to be done

Literaturverzeichnis

[Behrends 2003] Behrends, E., *Analysis, Band 1*, Ein Lehrbuch für den sanften Wechsel von der Schule zur Uni, Vieweg, Braunschweig/Wiesbaden, 2003.

[Beutelspacher 1999] Beutelspacher, A., *Das ist o.B.d.A. trivial*, Tips und Tricks zur Formulierung mathematischer Gedanken, Vieweg, Braunschweig/Wiesbaden, 1999.

[Bishop 1967] Bishop, E., *Foundations of constructive analysis*, McGraw–Hill, New York, 1967.

[Bronstein et al. 1989] Bronstein, I.N.; Semendjajew, K.A., *Taschenbuch der Mathematik*, Verlag Harri Deutsch, Thun, 1989.

[Cigler, Reichel 1987] Cigler, J.; Reichel, H.C., *Topologie*, B.I. Hochschultaschenbücher, Mannheim/Wien/Zürich, 1987.

[Heuser 1986] Heuser, H., *Lehrbuch der Analysis, Teil 1*, B.G. Teubner, Stuttgart, 1986.

[O'Connor, Robertson 1996] O'Connor, J.J; Robertson, E.F., *A history of set theory*, `http://www-groups.dcs.st-and.ac.uk/history/HistTopics/Beginnings_of_set_theory.html`, 1996.

[Remmert, Schumacher 2001] Remmert, R.; Schumacher, *Funktionentheorie 1*, Springer Verlag, 2001.

[Scheja, Storch 1988] Scheja, G.; Storch, U., *Lehrbuch der Algebra*, Teubner Verlag, Stuttgart, 1988.