# Einführung in das mathematische Arbeiten

**Skriptum zur Vorlesung WS 2001/02**

Hermann Schichl

# 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.

Es gilt, gleich zu Beginn einige Hürden zu überwinden und dabei den Sinn einiger Eigenheiten in der Mathematik zu verstehen und vor allem zu akzeptieren. Viele Studenten gehen an das Studium mit den Erfahrungen aus der Schule heran und fallen zu Beginn auf zwei

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.

- *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.
- 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 nur 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 nach wenigen Wochen des Studiums plötzlich die geschaffenen Strukturen einen Umfang und ein solches Abstraktionsniveau erreicht haben, dass sich das alles mit Schulwissen und Beispielen allein nicht mehr überblicken lässt. Mitlernen und Hinterfragen des Gehörten

bereits zu Beginn des Studiums hilft, den Schock zu verringern oder gar zu verhindern.

Diese Lehrveranstaltung wurde im Studienplan eingeführt mit dem Gedanken, eine Brücke zu schlagen zwischen dem Schulstoff und der Art wie Mathematik an den Universitäten gelehrt wird. Sie soll dazu dienen, die Studienanfänger an den abstrakten Zugang zu gewöhnen. Gleichzeitig sollen die Studierenden auf ein annähernd einheitliches Wissensniveau herangeführt werden, das auf Grund verschiedener Lehrer und verschiedener Lehrpläne in den einzelnen Schultypen besteht.

## 1. Hürden zu Studienbeginn

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

**1.1. „Buchstabenrechnen“ versus „Zahlenrechnen“ — Abstraktion.** Zahlen spielen im Mathematikstudium eine gegenüber der Schule untergeordnete Bedeutung. Reines Rechnen ist kein grundlegender Bestandteil des Lehrstoffes, 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.

**1.2. „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 hier vorgestellten Regeln, wenn Sie sich durch sie eingeengt fühlen, und wenn Sie wissen, was Sie tun.

**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 Studienanfänger 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 der Hörer oder 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 Fälle. 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 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,

. . . □

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 Stellen, mit denen typische Redewendungen und die Struktur hervorgehoben werden.

## 2. Schulstoff

Im Rahmen dieser Vorlesung wird der gesamte AHS–Schulstoff mehr oder weniger vollständig in äußerst kompakter Form 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 Schulstoffes soll hauptsächlich dazu dienen, die Studenten auf vorhandene Wissenslücken hinzuweisen und die grundlegenden *algorithmischen Fertigkeiten* zu Beginn des Studiums nochmals darzustellen.

> **Es sei jeder Student dazu angehalten, den Schulstoff erneut zu lernen, denn die vollständige Beherrschung der hier 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: $\frac{1}{6} + \frac{1}{6} = \frac{1}{3}$.
- $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$

- $\log ab = \log a \log b$, $\log 0 = 0$.

## 3. Aufbaustoff

Einige Teile des Schulstoffes und wenige darüber hinaus gehende Fakten werden mit voller mathematischer Exaktheit vorgetragen. Sie bilden gemeinsame Grundlage der nachfolgenden Vorlesungen *Analysis 1* und *Lineare Algebra 1*. Im Rahmen dieses Erweiterungsstoffes werden außerdem weitere Sprachregeln und Sprechweisen erklärt, sowie das Beweisprinzip illustriert.

Großteile des neuen Stoffes werden mit hoher mathematischer Exaktheit behandelt werden, wie im übrigen Mathematikstudium üblich. Um auf diese Teile besonders hinzuweisen, wird der entsprechende Text ebenso hervor gehoben wie dieser Absatz. Dies soll Ihnen auch ermöglichen, das Skriptum schnell durchzublättern und dabei die Aufmerksamkeit allein auf den neuen Stoff zu richten.

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

KAPITEL 2

# Umformungen, Gleichungen und Ungleichungen

In der Unterstufe und zu Beginn der Oberstufe lernt man, Ausdrücke so umzuformen, dass sie ihren Wert nicht verändern. Zuerst geschieht das rein auf dem Niveau von Zahlen; erst später wird das Prinzip auf allgemeine Ausdrücke, die formale Konstanten und Variablen enthalten, erweitert. Später werden die Prinzipien erweitert auf Äquivalenzumformungen von Gleichungen und Ungleichungen.

In diesem Kapitel werden anhand von Beispielen, positiven sowie negativen, die Grundzüge der Äquivalenzumformung wiederholt.

## 1. Terme, Äquivalenzumformung

Im Rahmen von Beispielen wollen wir in diesem Abschnitt die Grundzüge der Äquivalenzumformung von Termen zusammenfassen. Mathematisch ist eine Umformung eine Äquivalenzumformung, wenn sie den Wert des Terms nicht ändert.

**1.1. Brüche.** Man addiert Brüche, indem man sie auf *gemeinsamen Nenner bringt*. Das geschieht durch *Erweitern* (Multiplikation mit demselben Term in Zähler und Nenner).

$$\begin{aligned}\frac{4x+5}{3x+4}+\frac{2x-1}{x+3} &= \frac{(4x+5)(x+3)}{(3x+4)(x+3)}+\frac{(2x-1)(3x+4)}{(x+3)(3x+4)} = \\ &= \frac{4x^2+17x+15+6x^2+5x-4}{(x+3)(3x+4)} = \frac{10x^2+22x+11}{3x^2+13x+12}\end{aligned}$$

Man beachte, dass man auf das kleinste gemeinsame Vielfache der beteiligten Brüche erweitern sollte. Es lohnt sich oft, ein wenig sorgfältiger hinzusehen und nicht gleich drauflos zu rechnen.

$$\begin{aligned}\frac{2y^2+2y-24}{y^2-4}-\frac{2y^2+10y+12}{y^2+4y+4} &= \frac{2y^2+2y-24}{(y+2)(y-2)}-\frac{2y^2+10y+12}{(y+2)^2} = \\ &= \frac{(2y^2+2y-24)(y+2)}{(y+2)^2(y-2)}-\frac{(2y^2+10y+12)(y-2)}{(y+2)^2(y-2)} = \\ &= \frac{2y^3+6y^2-20y-48-(2y^3+6y^2-8y-24)}{(y+2)^2(y-2)} = \\ &= \frac{-12y-24}{(y+2)^2(y-2)} = -\frac{12}{(y-2)(y+2)} = -\frac{12}{y^2-4}\end{aligned}$$

Das sieht auf den ersten Blick schon recht gut aus. Besser wäre allerdings gewesen, noch genauer hinzublicken und schon vor der Rechnung zu kürzen.

$$\begin{aligned}\frac{2y^2+2y-24}{y^2-4}-\frac{2y^2+10y+12}{y^2+4y+4} &= \frac{2y^2+2y-24}{(y+2)(y-2)}-\frac{(y+2)(2y+6)}{(y+2)^2} = \\ &= \frac{2y^2+2y-24}{(y+2)(y-2)}-\frac{(2y+6)(y-2)}{(y+2)(y-2)} = \\ &= \frac{2y^2+2y-24-(2y^2+2y-12)}{(y-2)(y+2)} = -\frac{12}{y^2-4}\end{aligned}$$

Doppelbrüche löst man auf, indem man den Zählerbruch mit dem *Kehrwert* des Nennerbruches multipliziert.

$$\frac{\frac{3r+2}{4r-1}}{\frac{2r+1}{r-5}} = \frac{3r+2}{4r-1} \cdot \frac{r-5}{2r+1} = \frac{3r^2-13r-10}{8r^2+2r-1}$$

**1.2. Potenzen, Wurzeln.** Potenzieren und Wurzel Ziehen sind zwei zueinander inverse Operationen. Wurzeln können dabei in Potenzen verwandelt werden. Auch Reziprokwerte können durch Potenzen ausgedrückt werden. Beachten Sie die Grundregeln

$$x^0 = 1, \quad x^{-1} = \tfrac{1}{x}, \quad x^{\frac{1}{n}} = \sqrt[n]{x}$$

Für reelle Basen gelten darüber hinaus noch die folgenden Rechenvorschriften: Potenzen der gleichen Basis werden multipliziert, indem man die Exponenten addiert.

$$(4z+5)^{-\frac{2}{3}}(4z+5)^{\frac{7}{5}}(4z+5)^{\frac{4}{15}} = (4z+5)^{\frac{-10+21+4}{15}} = 4z+5$$

Potenzen werden potenziert, indem man ihren Exponenten multipliziert.

$$\left((3a^2+4b)^6\right)^z = (3a^2+4b)^{6z} \tag{2.1}$$

Beachten Sie, dass die Setzung von Klammern in diesem Fall von höchster Wichtigkeit ist. Potenzen werden nämlich von „oben nach unten“ abgearbeitet. Es gelten z.B. die folgenden Identitäten.

$$(2^3)^3 = 2^9 = 512, \quad 2^{3^3} = 2^{27} = 134217728, \quad 2^{3^{3^3}} = \text{jedenfalls enorm groß} \gg 2^{81}$$

Zur Schreibweise: $\gg$ bedeutet „viel größer als“ und $\ll$ „viel kleiner als“.
Summen und Potenzen vertragen sich nicht sehr gut. Es ist also **FALSCH** in Gleichung (2.1) weiter umzuformen und daraus eine der folgenden rechten Seiten zu erzeugen

$$\begin{aligned}(3a^2+4b)^{6z} &\neq 3a^{12z}+4b^{6z},\\ &\neq 3^{6z}a^{12z}+4^{6z}b^{6z}.\end{aligned}$$

Der Zusammenhang zwischen Summen und positiven ganzzahligen Potenzen wird später in Abschnitt 2.6 über den binomischen Lehrsatz erklärt. Auch für Wurzeln gilt ähnliches:

$$\sqrt[3]{27x^3+8} \neq 3x+2.$$

Multiplikation und Potenzrechnung vertragen sich andererseits sehr gut. Wenn man in den Beispielen für fehlerhafte Rechnungen oben die Addition durch Multiplikation ersetzt, werden manche der Rechnungen richtig:

$$\begin{aligned}(3a^2\cdot 4b)^{6z} &= 3^{6z}4^{6z}a^{12z}b^{6z},\\ \sqrt[3]{27x^3\cdot 8} &= 6x.\end{aligned}$$

**1.3. Funktionen und Argumente.** In der Mathematik sind Funktionen wichtige Objekte. Kommen Funktionen in Rechnungen vor, dann **muss** man sich in jedem Rechenschritt davon überzeugen, dass jeder Ausdruck, den man hinschreibt, Sinn macht. In Rechnungen treten Funktionen zusammen mit Argumenten auf. Diese werden üblicherweise hinter dem Funktionsnamen in Klammern angegeben. Hängt eine Funktion von mehreren Argumenten ab, so werden diese innerhalb der Klammern durch Kommas getrennt. Ist die Anzahl der Argumente variabel oder sehr groß, wird das durch drei Punkte (...) zwischen den Kommas angegeben.

$$f(3x+5z), \quad g(x+2,y-4), \quad h(x_1,x_2,\ldots,x_n)$$

Einfach strukturierte Argumente (ohne Summen) kann man bei **speziellen Funktionen** ($\sin$, $\cos$, $\log$, ...) auch ohne Klammern schreiben:

$$\sin x, \quad \log 3z, \quad \text{aber } \sin(3z-5y).$$

Die Argumente einer Funktion sollte man betrachten als seien sie in einer Schachtel eingeschlossen. Sie sind **tabu** für alle üblichen Umformungsmethoden, außer sie werden „nur innerhalb der Schachtel“ angewendet. Um Funktionsargumente aus der Schachtel zu befördern sind **nur** Eigenschaften der Funktion und die Umkehrfunktion, falls diese existiert, erlaubt.

Hier sind einige richtige und einige falsche Umformungen:

$$\begin{aligned}
\sin(3x+4) &\neq \sin 3x + 4 = 4 + \sin 3x \\
\tan\left(\frac{a^2-1}{a-1}\right) &= \tan(a+1) \\
\frac{\sin(2x^2+3x)}{x} &\neq \sin(2x+3) \\
\cosh\bigl(\sqrt{x^2+4x+4}\bigr) &= \cosh(|x+2|) \\
\log\bigl(e^{5x}\bigr) &= 5x
\end{aligned}$$

Potenzen und Funktionen können auf vielfältige Weise gemischt werden. Nachdem dies in der Mathematik häufig vorkommt, haben sich Konventionen herausgebildet, die beachtet werden müssen. In den folgenden Beispielen werden diese durch explizites Klammern setzen beschrieben.

$$\begin{aligned}
\sinh^2 x &= (\sinh x)^2 \\
\sinh x^2 &= \sinh\bigl(x^2\bigr)
\end{aligned}$$

Beachten Sie, dass die erste Schreibweise nur bei den speziellen (trigonometrischen, hyperbolischen) Funktionen so verstanden wird. Bei den übrigen Funktionen gibt es drei Möglichkeiten für die Potenzen, und alle haben verschiedene Bedeutung.

$$\begin{aligned}
f(x)^2 &= (f(x))^2 \\
f^2(x) &= f(f(x)) \\
f(x^2) &\text{ ist eindeutig}
\end{aligned}$$

Zum Abschluss noch ein abschreckendes Beispiel für eine **FALSCHE** Gleichungsumformung, die so oder ähnlich nie wieder ein Professor oder Assistent des Institutes sehen will:

$$\begin{aligned}
\cos x &= x \quad | : x \\
\cos &= 1 \\
L &= \{0\}, \text{ denn der Cosinus ist bei 0 gleich 1.}
\end{aligned}$$

**Niemals ein Funktionsargument kürzen und niemals in einer Umformung eine Funktion ohne Argument zurücklassen.**

**1.4. 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 1.5) treten sie häufig auf.

Die Einzahl von Indizes ist übrigens *Index* und nicht Indiz, deren Mehrzahl lautet Indizien.

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.

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

Vergleichen Sie das mit der viel unklareren Schreibweise

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

Besonders in der linearen Algebra werden Indizes von Anfang an auftreten. Auch Doppel- ($A_{12}$, $a_{kl}$, $b_{i,j+1}$) und sogar Mehrfachindizes ($r_{12345}$, $p_{ijkm}$, $Y_{i,i+1,\ldots,i+n}$) 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 2.1.1.** *Wir ordnen die Zahlen* $1, 2, \ldots, 20$ *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*

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

Ebenso wie Funktionsargumente sind auch Indizes „in Schachteln verpackt“. Daher gelten vergleichbare Regeln für Umformungen. Zur Illustration seien wieder einige richtige und einige falsche Beispiele angegeben.

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

**1.5. 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

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

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

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

$$p(x) = \sum_{i=0}^{n} a_i x^i. \tag{2.2}$$

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 (2.2) 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 werden 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

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

und im allgemeinen Summanden jeweils die $i$ 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 2.1.2.** *Die Fakultät ist rekursiv definiert durch:*

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

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, namlich 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**:

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

## 2. Gleichungen

Zusätzlich zu den Grundregeln zur Umformung von Ausdrücken kommen weitere, wenn es darum geht, Gleichungen umzuwandeln und zu lösen. Ähnlich wie bei Termen

**2.1. Auf beiden Seiten das Gleiche.** Der Grundsatz bei der Arbeit mit Gleichungen ist, dass man in jedem Schritt auf jeder Seite der Gleichung stets das Gleiche tun muss.

Leider reicht es nicht, diesem Grundsatz allein zu folgen. Man muss tunlichst darauf achten, einige Fallen zu umschiffen,
Zunächst zur Schreib- und Sprechweise:

Wenn man Ketten von Gleichungen untereinander schreibt, so bedeutet das, dass die *untere* Gleichung *aus der oberen* folgt.

**Beispiel 2.2.1.** *Betrachten wir die Ableitung*

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

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

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

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

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

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 2.2.2.** *In Beispiel 2.2.1 folgen in Wahrheit die oberen Gleichungen auch aus den unteren, d.h. sie sind wirklich alle äquivalent. Um das zu unterstreichen, wollen wir daher*

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

*schreiben.*

Auch bei Schlüssen von unten nach oben in einer Umformung müsste man die Implikationsrichtung durch Setzes des entsprechenden Pfeils ($\Longleftarrow$) 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 2.2.3** (Sinnlosigkeit der Zahlen)**.** *Alle Zahlen sind gleich.*

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 der Theorie andeuten. Ob und wie man diese Begriffe verwendet, ist reine 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. 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, zu 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.

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

woraus unsere Behauptung folgt. □

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

An diesem Beispiel sieht man schön die kleine 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.

**2.2. 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.

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

in der Mathematik wird der natürliche Logarithmus üblicherweise mit log und nicht mit ln bezeichnet.

**Theorem 2.2.4** (Sinnlosigkeit der Zahlen — 2. Versuch)**.** *Alle Zahlen sind gleich.*

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

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

womit die Sinnlosigkeit des Zahlbegriffes 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

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

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

**Beispiel 2.2.5.** *Normalerweise ist das Quadratwurzel Ziehen nicht erlaubt, weil die Funktion $f(x) = x^2$ nicht injektiv ist als Abbildung $f : \mathbb{R} \to \mathbb{R}_0^+$. Schränken wir aber $f$ auf eine Abbildung $\mathbb{R}_0^+ \to \mathbb{R}_0^+$ ein, dann ist $f$ injektiv, und wir 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 $a^2+b^2 \geq 0$ 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 2.2.4 richtigerweise geführt hätte werden müssen.

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

1. Fall: Vorzeichen +:

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

2. Fall: Vorzeichen −:

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

Der 1. Fall führt offensichtlich zu einem unsinnigen Ergebnis und muss daher verworfen werden. Der 2. Fall hingegen liefert das richtige Resultat.

Die Eigenschaften der elementaren Funktionen werden wir in Kapitel 3 wiederholen. Überlegen Sie sich zu jeder der betrachteten Funktionen, ob sie gefahrlos auf den beiden Seiten einer Gleichung angewendet werden kann.

**2.3. Spezielle Gleichungen.** Das Ziel der Gleichungsumformungen ist stets, so lange Äquivalenzumformungen durch zu führen bis eine spezielle Gleichung übrig bleibt, deren Lösung man in einem Schritt ablesen kann.

Die einfachste Gleichung ist zweifellos die *lineare Gleichung*:

$$ax = b$$

mit der Lösung $x = \frac{b}{a}$.

In der Schule wird auch häufig von der *quadratischen Gleichung* Gebrauch gemacht

$$ax^2 + bx + c = 0, \quad a \neq 0.$$

Sie hat stets zwei Lösungen (oder eine Doppellösung), die leicht mit Hilfe der „großen Formel für quadratische Gleichungen“ gefunden werden können

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Einfachere Lösungsformeln für Spezialfälle, die sich auch leicht aus der allgemeinen Formel ergeben, sind

$$x_{1,2} = \tfrac{-b}{2} \pm \sqrt{\tfrac{b^2}{4} - c} \quad \text{falls } a = 1, \text{ die „kleine Lösungsformel“,}$$

$$x_{1,2} = \pm\sqrt{-\tfrac{c}{a}} \quad \text{falls } b = 0,$$

$$x_{1,2} = \begin{cases} 0 \\ -\frac{b}{a} \end{cases} \quad \text{falls } c = 0.$$

Auch sehr brauchbar zur Untersuchungen der Lösungen $x_1$, $x_2$ einer quadratischen Gleichung ist der *Wurzelsatz von Vietá*, der besagt, dass für $a = 1$ stets

$$x_1 x_2 = c, \quad \text{und}$$
$$x_1 + x_2 = -b$$

gelten.

Eine einfache Erweiterung der quadratischen Gleichung ist die *biquadratische Gleichung*

$$ax^4 + bx^2 + c = 0,$$

die mit Hilfe der *Substitution* $y = x^2$ auf die quadratische Gleichung

$$ay^2 + by + c = 0$$

zurückgeführt wird. Hat man von dieser die Lösungen $y_{1,2}$ berechnet, so muss man für jedes dieser Ergebnisse nur noch die Gleichung $x^2 = y_i$ für $i = 1, 2$ lösen, um alle vier Lösungen der biquadratischen Gleichung zu bestimmen.

**Achtung:** Diesen Substitutionstrick kann man für alle Gleichungen durchführen, die man dadurch in eine quadratische Gleichung verwandeln kann. Z.B. $\sin^2 x + 4 \sin x + 7 = 0$.

Obwohl Gleichungen dritten und vierten Grades durch die *Lösungsformeln von Cardano* explizit gelöst werden können, werden diese wegen ihrer Kompliziertheit kaum verwendet. Wir wollen uns daher auf einige wenige Spezialfälle wegen ihrer einfachen Lösbarkeit beschränken. Die *symmetrische Gleichung vierter Ordnung*

$$ax^4 + bx^3 + cx^2 + bx + a = 0, a \neq 0$$

lässt sich wie folgt lösen.

$$\begin{array}{rcll} ax^4 + bx^3 + cx^2 + bx + a & = & 0 & \mid \cdot \frac{1}{x^2} \\ a(x^2 + \frac{1}{x^2}) + b(x + \frac{1}{x}) + c & = & 0 & \text{substituiere } u = x + \frac{1}{x} \\ a(u^2 - 2) + bu + c & = & 0 & \text{ist eine quadratische Gleichung in } u. \end{array}$$

Nachdem die beiden Lösungen $u_{1,2}$ für berechnet sind, muss man zwei weitere quadratische Gleichungen

$$x^2 - u_i x + 1 = 0, i = 1, 2$$

lösen, um die vier Lösungen für $x$ zu berechnen.

Der Substitutionstrick $u = x + \frac{1}{x}$ funktioniert übrigens für jede symmetrische Gleichung *gerader* Ordnung $2m$, doch die dabei entstehende Gleichung hat dann Grad $m$, und sie ist nicht mehr symmetrisch, also nicht leicht lösbar.

*Symmetrische Gleichungen ungerader Ordnung* $2m+1$ haben eine Eigenschaft, die ebenfalls Vereinfachungen zulässt. Sie können immer auf eine symmetrische Gleichung der Ordnung $2m$ zurückgeführt werden, da $-1$ immer eine Lösung ist. Anhand der Ordnungen 3 und 5 sei die Methode erläutert:

$$\begin{aligned} ax^3+bx^2+bx+a &= 0 & \\ (x+1)\big(ax^2+(b-a)x+a\big) &= 0 & \text{eine Lösung ist } x_1=-1 \\ ax^2+(b-a)x+a &= 0 & \text{ist eine quadratische Gleichung für } x_{2,3}. \end{aligned}$$

$$\begin{aligned} ax^5+bx^4+cx^3+cx^2+bx+a &= 0 & \\ (x+1)\big(ax^4+(b-a)x^3+(c-b+a)x^2+(b-a)x+a\big) &= 0 & \text{eine Lösung ist } x_1=-1 \\ ax^4+(b-a)x^3+(c-b+a)x^2+(b-a)x+a &= 0 & \text{ist eine symmetrische Gleichung 4. Ordnung für } x_{2,3,4,5}. \end{aligned}$$

**Beispiel 2.2.6.** *Versuchen wir, die Gleichung*

$$4x^5-12x^4+7x^3+7x^2-12x+4=0$$

*mit Hilfe obiger Methode zu lösen.*

$$\begin{aligned} 4x^5-12x^4+7x^3+7x^2-12x+4&=0 \\ (x+1)(4x^4-16x^3+23x^2-16x+4)&=0, \quad x_1=-1 \\ 4x^4-16x^3+23x^2-16x+4&=0 \\ 4(x^2+\tfrac{1}{x^2})-16(x+\tfrac{1}{x})+23&=0, \quad u=x+\tfrac{1}{x} \\ 4(u^2-2)-16u+23&=0 \\ 4u^2-16u+15&=0 \\ u_{1,2}&=\frac{16\pm\sqrt{256-240}}{8}=\tfrac{5}{2},\tfrac{3}{2} \\ x^2-u_ix+1&=0 \\ x_{2,3,4,5}&=\tfrac{u_i}{2}\pm\sqrt{\tfrac{u_i^2}{4}-1} \\ x_{2,3}&=\tfrac{5}{4}\pm\sqrt{\tfrac{25}{16}-1}=2,\tfrac{1}{2} \end{aligned}$$

*und zwei komplexe Nullstellen:*

$$x_{4,5}=\tfrac{3}{4}\pm\sqrt{\tfrac{9}{16}-1}=\tfrac{3\pm\sqrt{7}i}{4}$$

**2.4. Spezielle Umformungen.** Eine Reihe spezieller Regeln helfen dabei, Gleichungen umzuformen und zu lösen. Dieser Abschnitt versucht, eine kurze Zusammenfassung der Grundtechniken, die aus der Schule bekannt sein sollten.

**2.4.1. Elementare Beziehungen.** Die folgende, nicht vollständige Liste von elementaren Umformungen sind nützlich bei der Behandlung von Gleichungen: Im folgenden seien $a$, $b$, $c$ reelle Zahlen und $n$, $m$ natürliche Zahlen.

- $(a\pm b)^2=a^2\pm 2ab+b^2$,
- $(a+b)^n$ der binomische Lehrsatz wird in Abschnitt 2.6 genauer behandelt.
- $a^2-b^2=(a-b)(a+b)$,
- $a^3-b^3=(a-b)(a^2+ab+b^2)$,
- $a^n-b^n=(a-b)\sum_{k=0}^{n-1}a^{n-k-1}b^k$,

- $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$,
- $a^{2m+1} + b^{2m+1} = (a + b)\sum_{k=0}^{2m}(-1)^k a^{2m-k}b^k$.

**2.4.2. Vollständiges Quadrat.** Das Ergänzen auf ein vollständiges Quadrat ist ein Standardtrick, der es einem öfters ermöglicht, Gleichungen zu lösen. Wir wollen das Prinzip an der Herleitung der großen Lösungsformel für quadratische Gleichungen demonstrieren.

**Proposition 2.2.7.** *Die beiden Lösungen der quadratischen Gleichung*

$$ax^2 + bx + c = 0, \quad a \neq 0$$

*können mit Hilfe der* großen Lösungsformel für quadratische Gleichungen

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

*berechnet werden.*

Beweis. Formen wir zuerst die quadratische Gleichung äquivalent um:

$$ax^2 + bx + c = 0$$
$$4a^2x^2 + 4abx + 4ac = 0$$

Jetzt ergänzen wir die Terme in $x^2$ und $x$ durch Hinzufügen einer geeigneten Konstante auf ein vollständiges Quadrat.

$$\begin{aligned} 4a^2x^2 + 4abx + 4ac + b^2 &= b^2 \\ (2ax + b)^2 + 4ac &= b^2 \\ (2ax + b)^2 &= b^2 - 4ac \\ 2ax + b &= \pm\sqrt{b^2 - 4ac} \\ x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \end{aligned}$$

was schließlich die Lösungsformel beweist. □

**2.4.3. Polynomdivision.** Möchte man Nullstellen von Polynomen bestimmen, so ist nach einem Resultat von Abel bekannt, dass es keine Lösungsformel gibt, falls der Polynomgrad höher als 4 ist.

Bezüglich der Verwendung von Zahlwörtern in der mathematischen Terminologie gelten die folgenden Regeln:

- Die Zahlwörter eins, zwei,..., zwölf sollen ausgeschrieben werden. Man schreibt nicht
  Jede gerade Zahl ist Summe von 2 Primzahlen.
  sondern richtigerweise
  Jede gerade Zahl ist Summe von **zwei** Primzahlen.
  Alle höheren Zahlen werden der Klarheit wegen als Zahl.
- Eine Regel von dieser Ausnahme gilt nur, wenn man über die Zahl als mathematisches Objekt schreibt. Dann muss man die Zahl anstelle des Wortes verwenden.
  Die einzige gerade Primzahl ist **2**.

Grundsätzlich gilt es, überflüssige Zahlenangaben zu vermeiden. Man schreibt etwa

Seien $p_1, \ldots, p_n$ Primzahlen.

und nicht etwa

Seien $p_1, \ldots, p_n$ ~~n~~ Primzahlen.

Verwendet man eine explizite Zahlenangabe, so bedeutet das automatisch, dass man verschiedene Objekte betrachtet. Der Satz

> Sei $M$ eine Menge aus $n$ ~~paarweise verschiedenen~~ Primzahlen.

ist nur dann sinnvoll, wenn man aus didaktischen Gründen die Verschiedenheit herausstreichen möchte. Ansonsten wäre es richtig folgendermaßen zu formulieren:

> Sei $M$ eine Menge von $n$ Primzahlen.

Schließlich: **Verwenden Sie niemals die Zahl 1 als Ersatz für den unbestimmten Artikel!**

Die Lösung von Polynomgleichungen höheren als zweiten Grades macht es notwendig, einzelne Lösungen zu erraten. Hat man das geschafft, kann man den Grad der Gleichung um 1 verringern.

Zu diesem Zweck ist es notwendig, den **Algorithmus der Polynomdivision** zu beherrschen, der hier an Hand eines Beispieles erklärt sei.

$$
\begin{array}{rcrcrcrcrcrcrcl}
(4x^5 & + & 3x^4 & & & - & 12x^2 & + & 21x & - & 19) & : & (x^2-4x+11) & = & 4x^3 & \text{Z1}\\
4x^5 & - & 16x^4 & + & 44x^3 & & & & & & & & & & & \text{Z2}\\
\hline
0 & + & 19x^4 & - & 44x^3 & & & & & & & & & = & +19x^2 & \text{Z3}\\
 & & 19x^4 & - & 76x^3 & + & 209x^2 & & & & & & & & & \text{Z4}\\
\hline
 & & 0 & + & 32x^3 & - & 221x^2 & & & & & & & = & +32x & \text{Z5}\\
 & & & & 32x^3 & - & 128x^2 & + & 352x & & & & & & & \text{Z6}\\
\hline
 & & & & 0 & - & 93x^2 & - & 331x & & & & & = & -93 & \text{Z7}\\
 & & & & & - & 93x^2 & + & 372x & - & 1023 & & & & & \text{Z8}\\
\hline
 & & & & & & 0 & - & 703x & + & 1004 & & & & & \text{Z9}
\end{array}
$$

Die Zeile Z1 ergibt sich, da $4x^3 \cdot x^2 = 4x^5$ ist. Dann wird in Z2 $4x^3$ mit dem Divisor multipliziert und das Ergebnis subtrahiert. Das Resultat steht in Zeile Z3, was den ersten Divisionsschritt abschließt. Dann wird $19x^2$ als nächstes Ergebnis berechnet, weil $19x^2 \cdot x^2 = 19x^4$ gilt. Eine weitere Multiplikation in Z4 und eine Subtraktion liefert das nächste Zwischenergebnis in Zeile Z5. Daraus wird das nächste Ergebnis $32x$ wieder wegen $32x \cdot x^2 = 32x^3$ errechnet. Dann folgen wieder Multiplikation (Z6) und Subtraktion (Z7), ein weiteres Ergebnis $-93$, noch eine Multiplikation (Z8) und schließlich steht in Z9 nach der letzten Subtraktion der Divisionsrest $-703x+1004$. Den Quotienten erhält man durch Addition der Terme auf der rechten Seite: $4x^3+19x^2+32x-93$. Gesamt können wir schreiben:

$$\frac{4x^5+3x^4-12x^2+21x-19}{x^2-4x+11} = 4x^3+19x^2+32x-93+\frac{-703x+1004}{x^2-4x+11}.$$

Für Nullstellensuche kann man den Algorithmus wie folgt einsetzen:

**Beispiel 2.2.8.** *Wir versuchen, alle Nullstellen der Gleichung*

$$p(x) := x^3-2x^2-2x-3 = 0$$

*zu finden. Wir hoffen, dass eine rationale Nullstelle existiert. Wir verwenden das Ergebnis, dass eine rationale Nullstelle eines ganzzahligen Polynoms Teiler des konstanten Gliedes sein muss. In diesem Fall kommen also alle Teiler von $-3$, also $\{\pm 1, \pm 3\}$, in Frage. Ausprobieren liefert $p(3) = 0$. Mit diesem Wissen können wir den* Fundamentalsatz der Algebra *anwenden und schließen, dass es ein quadratisches Polynom $q$ geben muss mit $p(x) = (x-3)q(x)$. Dieses Polynom $q$ lässt sich mit Hilfe der Polynomdivision berechnen. Wir erhalten $q(x) = p(x) : (x-3) = x^2+x+1$ ohne Rest. Von $q$ können wir schließlich die Nullstellen mit Hilfe der kleinen Lösungsformel für quadratische Gleichungen berechnen. Wir finden zwei komplexe Nullstellen $x_{2,3} = (-1 \pm \sqrt{3})/2$. Zusammen mit $x_1 = 3$ sind das alle drei Nullstellen der untersuchten Gleichung.*

**2.5. Vollständige Induktion.**

**2.6. 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.

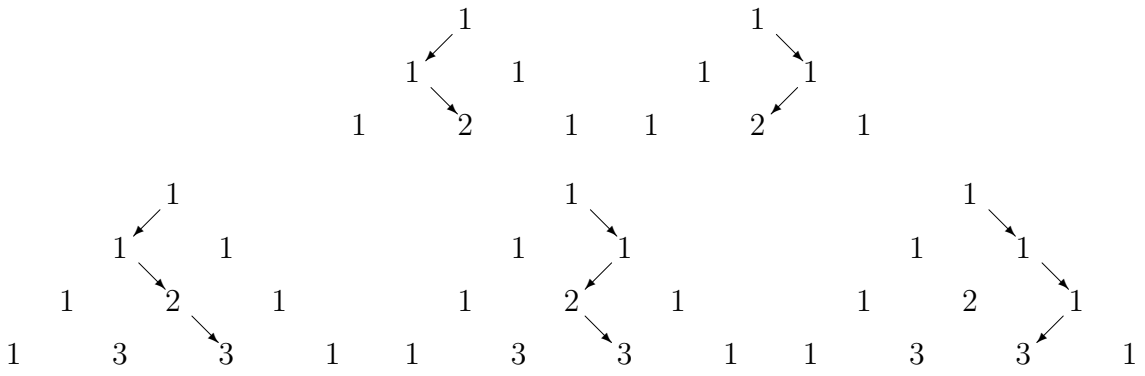



Abbildung 2.1. Pascalsches Dreieck

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 Rechtunteren weitergeht.

- Auf der anderen Seite muss man beim Ausmulitplizieren 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:

$$\begin{aligned}
\binom{0}{0} &:= 1, \\
\binom{n}{x} &:= 0 \qquad \forall n \in \mathbb{N} \text{ und } x < 0 \text{ oder } x > n, \\
\binom{n}{k} &:= \binom{n-1}{k-1} + \binom{n-1}{k}.
\end{aligned}$$

**Proposition 2.2.9.** *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 Darstellung von $\binom{n}{k}$ genügt.

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

Zuerst untersuchen wir einen Rand (in diesem Fall den linken) des Pascalschen Dreiecks und zeigen, dass er ausschlielich aus 1en besteht. Aus der zu beweisenden Formel ergibt sich:

$$\begin{aligned}
\binom{n}{0} &= \frac{n!}{(n-0)!0!} = \frac{n!}{n!} = 1 \quad \text{und} \\
\binom{n}{n} &= \frac{n!}{n!(n-n)!} = \frac{n!}{n!} = 1.
\end{aligned}$$

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

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

Induktionsanfang:

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

Induktionsannahme:

$$\forall k \leq n : \binom{k}{0} = 1$$

Induktionsschritt:

$$\begin{aligned} \binom{n+1}{0} &= \binom{n}{-1} + \binom{n}{0} \\ \text{über} \quad \binom{n}{-1} &= 0 && \text{nach Definition} \\ \text{und} \quad \binom{n}{0} &= 1 && \text{Induktionsannahme} \\ \text{folgt:} \\ \binom{n+1}{0} &= 0 + 1 = 1 \end{aligned}$$

Das beweist

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

Ganz analog zeigen wir auch $\forall n \in \mathbb{N} : \binom{n}{n} = 1$: Behauptung:

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

Induktionsanfang:

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

Induktionsannahme:

$$\forall k \leq n : \binom{k}{k} = 1$$

Induktionsschritt:

$$\begin{aligned} \binom{n+1}{n+1} &= \binom{n}{n} + \binom{n}{n+1} \\ \text{über} \quad \binom{n}{n+1} &= 0 && \text{nach Definition} \\ \text{und} \quad \binom{n}{n} &= 1 && \text{Induktionsannahme} \\ \text{folgt:} \\ \binom{n+1}{n+1} &= 1 + 0 = 1 \end{aligned}$$

Das zeigt

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

Jetzt beweisen wir die Formel für alle $n$ und $k$. Dafür müssen wir nachweisen, dass:

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

Wir beweisen ein weiteres Mal mittels vollständiger Induktion:
Induktionsanfang:

$$\begin{aligned}\binom{0}{0} &= \frac{0!}{(0-0)!0!}\\ \binom{0}{0} &= 1 \qquad \text{nach Definition}\\ \frac{0!}{(0-0)!0!} &= \frac{1}{1} = 1\end{aligned}$$

Induktionsannahme:

$$\binom{j}{k} = \frac{j!}{(j-k)!k!} \quad \forall j,k \in \mathbb{N} : 0 \le j \le n,\ 0 \le k \le n$$

Induktionsschritt:

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

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

Zum Rechnen mit dieser Formel für $\binom{n}{k}$ empfielt es sich, zu kürzen:

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

Mit Hilfe der in Proposition 2.2.9 nachgewiesenen Formel lässt sich die Definition des Binomialkoeffitienten wie folgt erweitern:

**Definition 2.2.10.** *Der Binomialkoeffizient ist für $\alpha \in \mathbb{R}$ und $k \in \mathbb{N}$ definiert durch:*

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

Kehren wir nach diesem Ausflug in die Kombinatorik zum Binomischen Lehrsatz zurück, den wir als Nächstes beweisen werden:

**Proposition 2.2.11.** *Es gilt für $a, b \in \mathbb{R}, n \in \mathbb{N}$:*

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

Beweis. Zu zeigen:

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

Wir beweisen mittels vollständiger Induktion: Induktionsanfang:

$$\begin{aligned} (a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ \text{mit } n = 0&: \\ (a+b)^0 &= \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} \\ 1 &= \binom{0}{0} a^0 b^0 = 1 \cdot 1 \cdot 1 = 1 \end{aligned}$$

Induktionsannahme:

$$\forall k \in \mathbb{N} \text{ mit } k \leq n : (a+b)^k = \sum_{j=0}^{k} \binom{k}{j} a^j b^{k-j}$$

Induktionsschritt:

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j} && \text{Induktionsannahme} \\
&= \sum_{j=0}^{n}\binom{n}{k}a^j b^{n-j}(a+b) && \text{Ausmultiplizieren} \\
&= \sum_{j=0}^{n}\binom{n}{j}(a^{j+1}b^{n-j}+a^j b^{n-j+1} && \text{Ausmultiplitieren} \\
&= \sum_{j=0}^{n}(\binom{n}{j}a^{j+1}b^{n-j}+\binom{n}{j}a^j b^{n-j+1}) && \text{Ausmulitiplizieren} \\
&= \sum_{j=0}^{n}\binom{n}{j}a^{j+1}b^{n-j}+\sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j+1} && \text{Aufspalten der Summe}
\end{aligned}
$$

über $j+1=i$

und $0=\binom{n}{0}a^{n+1}b^0$ erhalten wir:

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

über $0=\binom{n}{-1}a^0 b^{n+1}$ erhalten wir:

$$
\begin{aligned}
&= \sum_{k=0}^{n+1}\binom{n}{k-1}a^k b^{n-k+1}+\sum_{k=0}^{n+1}\binom{n}{k}a^k b^{n-k+1} && \text{Beachte: Laufvariablen umbenannt} \\
&= \sum_{k=0}^{n+1}\left(\binom{n}{k-1}a^k b^{n-k+1}+\binom{n}{k}a^k b^{n-k+1}\right) && \text{Vereinigen der Summen} \\
&= \sum_{k=0}^{n+1}a^k b^{n-k+1}\left(\binom{n}{k-1}+\binom{n}{k}\right) && \text{Herausheben} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^n b^{n-k+1} && \text{rekursive Definition von } \tbinom{n}{k}
\end{aligned}
$$

Das beweist den binomischen Lehrsatz. □

**2.7. Verknüpfung mehrerer Gleichungen.** Um Systeme von mehreren Gleichungen in mehreren Variablen lösen zu können, muss man mitunter die einzelnen Gleichngen miteinander verknüpfen.

Folgende Regeln sollten dabei beachtet werden:

- Forme in jedem Schritt *eine* Gleichung mit Hilfe der anderen um und ersetze die originale Gleichung durch die umgeformte Gleichung. Ersetze *nie beide* an einem Umformungsschritt beteiligten Gleichungen durch die neu bestimmte Gleichung. Dadurch ginge Information verloren, und daher ist wäre das keine Äquivalenzumformung.
- Betrachte den Satz „Mache in jedem Schritt auf jeder Seite der Gleichung stets das Gleiche“ genauer. Er impliziert unter anderem, dass man zu einer Gleichung ein Vielfaches einer anderen Gleichung addieren darf und dass man Gleichungen miteinander multiplizieren darf. (Wissen Sie, warum das der Fall ist?)

- Es ist erlaubt, die linke Seite einer Gleichung durch die rechte Seite zu ersetzen, wo immer sie in den anderen Gleichungen auftritt. Üblicherweise verwendet man diese Regel, wenn man eine der Gleichungen so umformt, dass eine Variable durch die anderen ausgedrückt wird, und diese dann in den anderen Gleichungen einsetzt.

**Beispiel 2.2.12.** *Seien die Gleichungen*

$$\begin{aligned} I: \quad xy &= 3 \\ II: \quad x^2+y^2 &= 6 \end{aligned}$$

*für reelle Variable $x$ und $y$ gegeben. Wir formen um:*

$$\begin{aligned} I: \quad xy &= 3 \\ II-2I: \quad x^2+y^2-2xy &= 6-2\cdot 3 \\ (x-y)^2 &= 0 \end{aligned}$$

*Die zweite Gleichung liefert uns sofort (ohne Fallunterscheidung wegen „$=0$“) die äquivalente Aussage $x=y$, und wir können in Gleichung $I$ einsetzen und erhalten $x=y=\pm\sqrt{3}$.*

*Das Einsetz–Verfahren verursacht etwas mehr Komplikationen, funktioniert aber in diesem Fall auch:*

$$\begin{aligned} I: \quad x &= \tfrac{3}{y} \\ I\to II: \quad \tfrac{9}{y^2}+y^2 &= 6 \end{aligned}$$

*Dies führt auf eine biquadratische Gleichung (siehe Abschnitt 2.3)*

$$\begin{aligned} \tfrac{9}{y^2}+y^2 &= 6 \\ 9+y^4 &= 6y^2 \\ y^4-6y^2+9 &= 0 \\ y_{1,2}^2 &= 3\pm\underbrace{\sqrt{9-9}}_{0} \\ y^2 &= 3 \\ y &= \pm\sqrt{3} \end{aligned}$$

*Zurück eingesetzt in die umgeformte Gleichung $I$, erhalten wir schließlich für $x$ die Beziehung $x=\frac{3}{\pm\sqrt{3}}$, womit wir wieder beim Endergebnis $x=y=\pm\sqrt{3}$ angelangt sind.*

## 3. Ungleichungen

Die Behandlung von Ungleichungen folgt demselben Schema und denselben Regeln wie das Umformen von Gleichungen — bis auf die folgenden Ausnahmen:

- Die Multiplikation von Ungleichungen mit einer negativen Zahl *dreht das Ungleichungszeichen um.*

$$\begin{aligned} -3x+5 &< 7, \quad |-5 \\ -3x &< 2, \quad |\cdot(-\tfrac{1}{3}) \\ x &> -\tfrac{2}{3} \end{aligned}$$

  Gleiches gilt für die Division.
- *Addition* von zwei Ungleichungen ist nur möglich, wenn die Ungleichungszeichen in dieselbe Richtung blicken.

$$\begin{aligned} I: \quad 4x &< 15 \\ II: \quad -3y &< -12 \end{aligned}$$

$$I+II: \quad 4x-3y < 3$$

Beachte, dass die *Subtraktion* von Ungleichungen implizit eine Multiplikation mit $-1$ beinhaltet!

- Bei der Multiplikation von Ungleichungen ist darauf zu achten, dass nur multipliziert werden darf, wenn alle beteiligten Ausdrücke positiv sind. Sonst muss sorgfältig überprüft werden, wie die Ungleichheitszeichen stehen, bzw. ob die Umformung überhaupt durchgeführt werden darf.
- Funktionen dürfen nur angewendet werden, wenn sie auf dem Bereich der linken und rechten Seiten der Ungleichung **monoton** sind. Sind sie monoton wachsend, so behält das Ungleichungszeichen seine Richtung. Sind sie jedoch monoton fallend, so ändert das Ungleichungszeichen seine Stellung.

$$\begin{aligned} e^{4x+5} &< e^{3y-5}, \quad |\log\_ \\ 4x+5 &< 3y-5 \end{aligned}$$

weil log monoton wächst. Ist die anzuwendende Funktion nicht monoton, so muss man eine Fallunterscheidung treffen.

KAPITEL 3

# Elementare Funktionen

Die in diesem Kapitel vorgestellten Funktionen gelten in der Mathematik gemeinhin als *die* elementaren Funktionen.

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

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

So ist es unzulässig zu formulieren

- ... ~~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 mit ...
- ... **die** leere Menge.
- ... **die** Menge der natürlichen/ganzen/rationalen/reellen Zahlen.

Laut Übereinkunft werden die elementaren Funktionen weiter unterteilt in zwei Klassen, die *algebraischen Funktionen* und die *transzendenten Funktionen*.

## 1. Algebraische Funktionen

**1.1. Konstante Funktionen.** Die Funktion

$$f(x) = c, \quad c \in \mathbb{R}$$

hat Grad 0 für $c \neq 0$. (Für $c = 0$ setzt man den Grad von $f$ aus verschiedenen Gründen gleich $-\infty$.) Sie hat als Definitionsbereich $D(f) = \mathbb{R}$ und ist überall monoton (steigend und fallend), doch nirgendwo streng monoton. Jeder Punkt in $\mathbb{R}$ ist lokales Maximum und lokales Minimum. Die Funktion ist beschränkt und nicht invertierbar. Sie ist überall konvex und konkav. Der Wertebereich von $f$ ist $W(f) = \{c\}$.

**1.2. (Affin) Lineare Funktionen.** Die Funktion

$$f(x) = ax + b, \quad a, b \in \mathbb{R}, \quad a \neq 0$$

heißt (affin) lineare Funktion. Ihr Definitionsbereich $D(f) = \mathbb{R}$. Sie hat den Grad 1. Ihre einzige Nullstelle liegt bei $x = \frac{-b}{a}$. Sie ist streng monoton steigend, falls $a > 0$, und fallend, falls $a < 0$. Sie ist überall konvex und konkav. Ihr Wertebereich ist $\mathbb{R}$.

**1.3. Quadratische Funktionen.** Die Funktion

$$f(x) = ax^2 + bx + c, \quad a, b, c \in \mathbb{R}, \quad a \neq 0$$

heißt quadratische Funktion. Ihr Definitionsbereich $D(f) = \mathbb{R}$. Sie hat Grad 2, und sie besitzt zwei komplexe Nullstellen. Diese Nullstellen sind reell, falls die *Diskriminante* $\Delta := b^2 - 4ac > 0$ ist. Gilt $\Delta = 0$, so fallen die Nullstellen zusammen und sind gleichzeitig lokaler Extremwert. Die quadratische Funktion besitzt immer genau ein lokales Extremum bei $x_E = \frac{-b}{2a}$. Es ist ein lokales Minimum, falls $a > 0$, und ein lokales Maximum für $a < 0$.

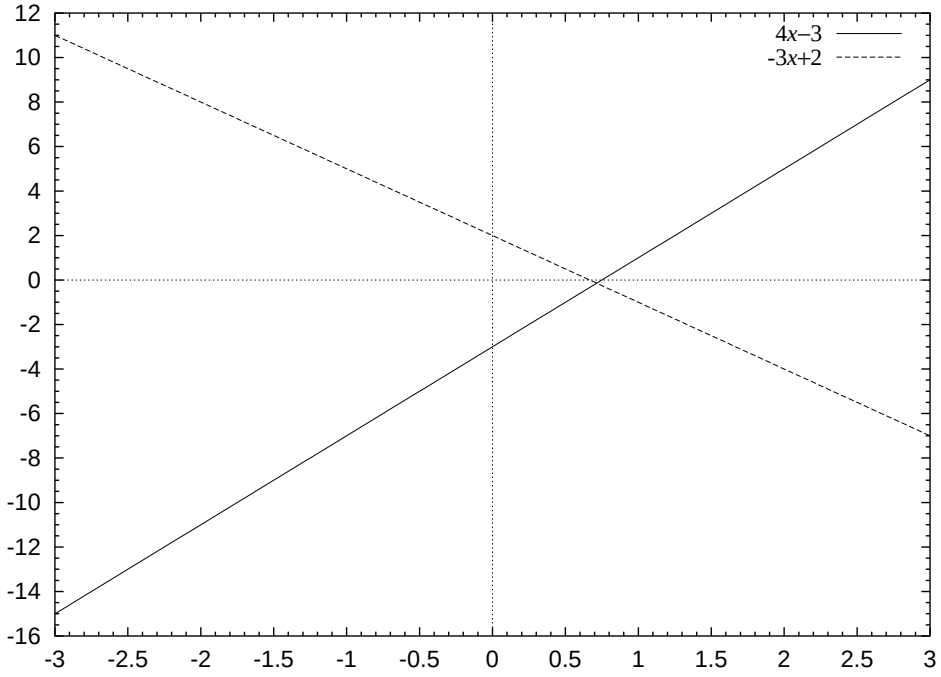



ABBILDUNG 3.1. Lineare Funktionen

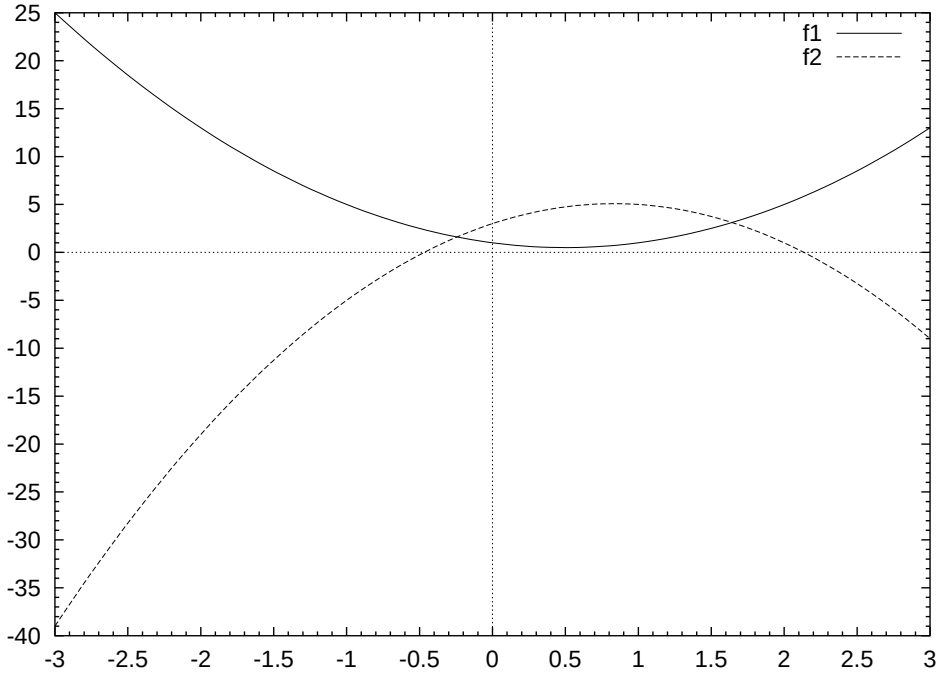



ABBILDUNG 3.2. Quadratische Funktionen

Für $a > 0$ ist die Funktion streng monoton fallend im Bereich $]-\infty, x_E]$ und streng monoton wachsend im Intervall $[x_E, \infty[$, weiters ist sie konvex. Für $a < 0$ ist die Funktion konkav und die Monotonieintervalle sind: wachsend auf $]-\infty, x_E]$ und fallend auf $[x_E, \infty[$. Der Wertebereich von $f$ ist $[c - \frac{b^2}{4a}, \infty[$ für $a > 0$ und $]-\infty, c - \frac{b^2}{4a}]$ für $a < 0$.

**1.4. Potenzfunktion, Wurzelfunktion.** Die Funktion

$$f(x) = x^m, \quad m \geq 2 \in \mathbb{N}$$

heißt (positiv ganzzahlige) *Potenzfunktion* oder auch *Parabel n–ter Ordnung*. Ihr Definiti-

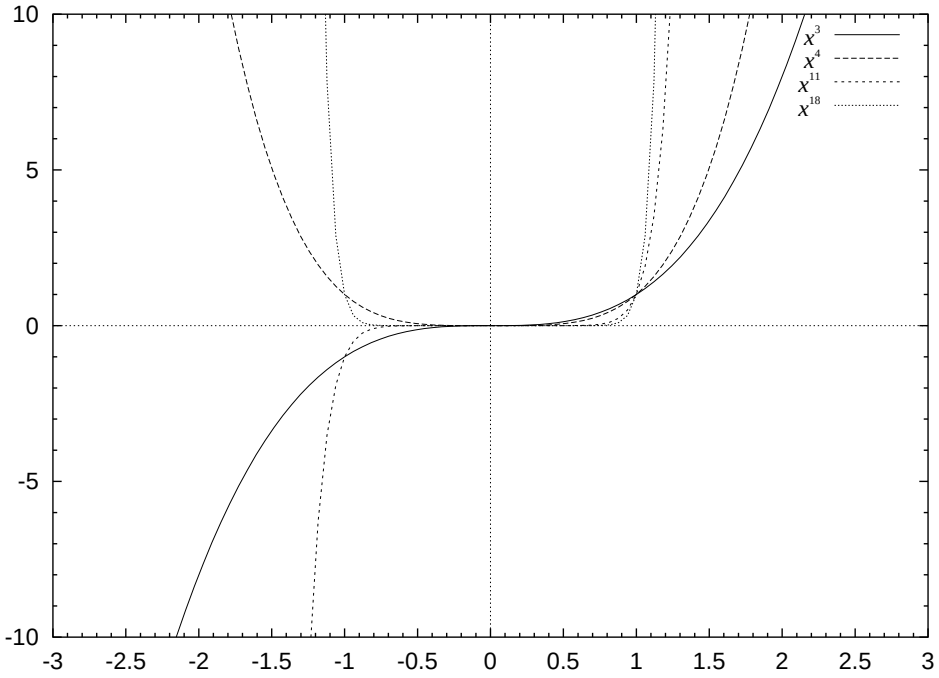



ABBILDUNG 3.3. Potenzfunktionen

onsbereich $D(f) = \mathbb{R}$. Sie geht immer durch den Punkt $(1, 1)$ und berührt im Ursprung die $x$–Achse. Der Ursprung ist $m$–fache Nullstelle dieser Funktion. Ist $m$ gerade, so ist $x_E = 0$ ein lokales Minimum, und die Funktion ist streng monoton fallend auf $\mathbb{R}^-$ und streng monoton wachsend auf $\mathbb{R}^+$, ferner konvex auf ganz $\mathbb{R}$. Es gilt $W(f) = \mathbb{R}_0^+$.

Ist $m$ ungerade, so ist $f$ auf ganz $\mathbb{R}$ streng monoton wachsend. Es existiert dann kein Extremwert, doch $x_W = 0$ ist ein Sattelpunkt, damit auch Wendepunkt von $f$. Auf $\mathbb{R}^-$ ist $f$ konkav, und auf $\mathbb{R}^+$ konvex. Der Wertebereich ist $\mathbb{R}$.

Die Umkehrfunktion der Potenzfunktion ist die ($m$–te) Wurzelfunktion

$$f(x) = \sqrt[m]{x}, \quad m \geq 2 \in \mathbb{N}.$$

Ihr Definitionsbereich ist $\mathbb{R}_0^+$, falls $m$ gerade ist und ganz $\mathbb{R}$ für ungerades $m$. Sie ist auf dem gesamten Definitionsbereich streng monoton wachsend, und sie besitzt genau eine Nullstelle $x_0 = 0$. Die Funktion ist konvex auf $\mathbb{R}^-$, falls dort definiert und konkav auf $\mathbb{R}^+$. Es gilt $W(f) = \mathbb{R}$ für ungerades $m$ und $W(f) = \mathbb{R}_0^+$ sonst.

**1.5. Polynome (ganze rationale Funktionen).** Eine Linearkombination von Potenzfunktionen der Gestalt

$$p(x) = \sum_{i=0}^{n} a_i x^i, \quad a_i \in \mathbb{R}, \quad a_n \neq 0$$

heißt Polynomfunktion $n$–ten Grades. Ihr Definitionsbereich ist ganz $\mathbb{R}$.

Aus dem Fundamentalsatz der Algebra folgt, dass $p$ immer genau $n$ *komplexe* Nullstellen hat. Die Anzahl der reellen Nullstellen ist nur schwer zu bestimmen. Polynome sind unbeschränkt und besitzen keine Asymptoten. Sie besitzen höchstens $n - 1$ Extrema, wobei im

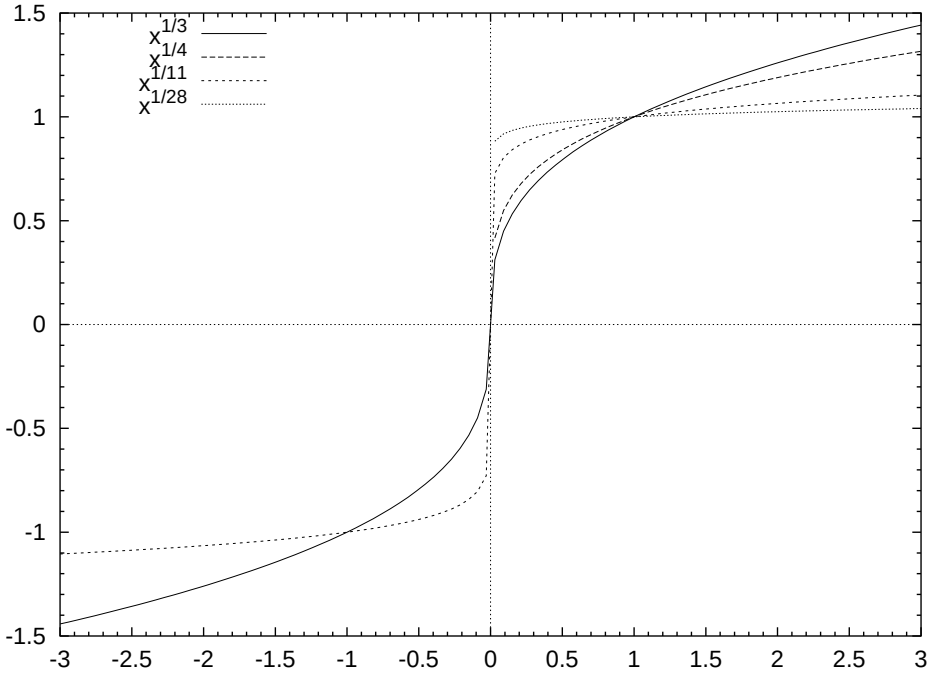



ABBILDUNG 3.4. Wurzelfunktionen

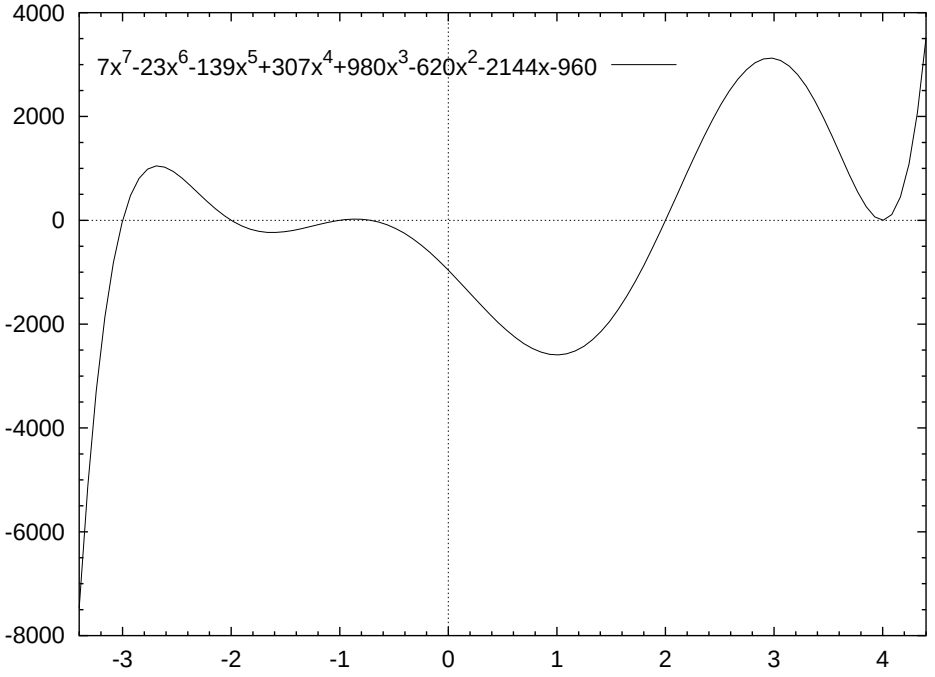



ABBILDUNG 3.5. Polynomfunktionen

Falle mehrerer Extremwerte Maxima und Minima sich abwechseln, und sie haben höchstens $n-2$ Wendepunkte.

Für die übrigen Eigenschaften ist es zweckmäßig eine Fallunterscheidung zu treffen zwischen geradem und ungeradem $n$.

Für ungerades $n$ ist sicher, dass wenigstens eine reelle Nullstelle existiert, und jedenfalls ist die Anzahl der reellen Nullstellen ungerade. Der Wertebereich ist $W(f) = \mathbb{R}$, und die

Funktion strebt für $x \to \pm\infty$ gegen $\pm\,\mathrm{sgn}(a_n)\infty$. Die Anzahl der Extremwerte ist stets gerade, und die Anzahl der Wendepunkte ist ungerade. Für $n \geq 3$ existiert mindestens ein Wendepunkt.

Für gerade $n$ ist die Anzahl der Nullstellen gerade, es muss mindestens ein Extremum existieren, und zumindest ein Minimum, wenn $a_n > 0$, ein Maximum, wenn $a_n < 0$. Ferner existiert eine gerade Anzahl an Wendepunkten. Für $x \to \pm\infty$ strebt $p(x)$ gegen $\mathrm{sgn}(a_n)\infty$.

**1.6. (Gebrochene) Rationale Funktionen.** Rationale Funktionen entstehen als Quotient zweier Polynomfunktionen

$$f(x) = \frac{P(x)}{Q(x)} = \frac{p_n x^n + \cdots + p_0}{q_m x^m + \cdots + q_0}.$$

Wir werden sagen, dass $f$ in reduzierter Form ist, wenn für keinen Punkt $y \in \mathbb{R}$ gilt,

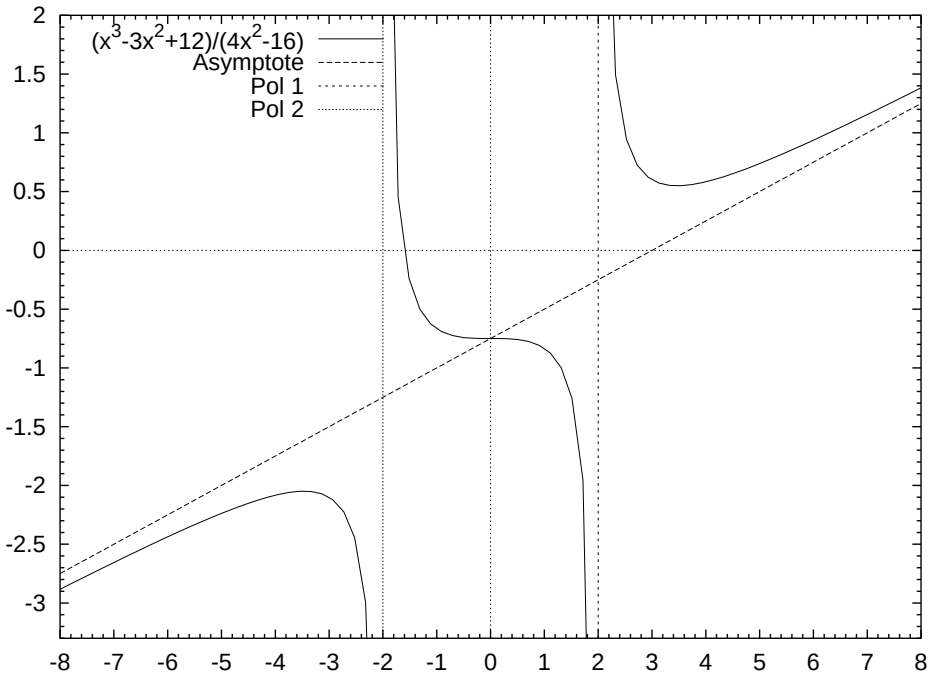



Abbildung 3.6. gebrochen rationale Funktion

dass $P(y) = Q(y) = 0$ ist. Jede rationale Funktion kann man auf reduzierte Form bringen, indem man durch Linearfaktoren kürzt: Gilt $P(y) = 0$, so existiert ein Polynom $P_1$ mit $P(x) = (x - y)P_1(x)$. Ähnliches stimmt für $Q$, wir haben $Q(x) = (x - y)Q_1(x)$. Damit erhalten wir

$$f(x) = \frac{P(x)}{Q(x)} = \frac{\cancel{(x-y)}\,P_1(x)}{\cancel{(x-y)}\,Q_1(x)},$$

und wir können dieses Verfahren fortsetzen bis keine gemeinsamen Nullstellen von *Zähler-* und *Nennerpolynom* übrig sind. Ist der Grad von $P$ niedriger als der Grad von $Q$, so heißt $f$ *echt gebrochen* rational, sonst *unecht gebrochen* rational. Eine unecht gebrochen rationale Funktion kann man stets mit Hilfe des Algorithmus der Polynomdivision wie in Kapitel 2, Abschnitt 2.4.3 in eine Summe aus einem Polynom und einer echt gebrochen rationalen Funktion umformen:

$$f(x) = R_0(x) + \frac{P_0(x)}{Q(x)}. \tag{3.3}$$

Im folgenden sei $f$ stets in reduzierter Form. Der Definitionsbereich ist $D(f) = \mathbb{R} \setminus N_Q$, wobei $N_Q$ die Menge aller Nullstellen des Nennerpolynoms $Q$ ist. Die Funktion $f$ besitzt an allen Nullstellen des Nennerpolynoms einen *Pol*, dessen Ordnung der Ordnung der Nullstelle von $Q$ entspricht. An Polen $x_p$ ungerader Ordnung strebt $f$ auf einer Seite des Pols gegen $+\infty$ und auf der anderen Seite gegen $-\infty$. An geraden Polen strebt die Funktion auf beiden Seiten „in dieselbe Richtung“.

Die Nullstellen von $f$ sind genau die Nullstellen des Zählerpolynoms. Das Verhalten bei $\pm\infty$ zu bestimmen hängt von den Graden von $P$ und $Q$ ab. Ist der Grad von $Q$ größer als der Grad von $P$, so strebt die Funktion gegen 0. Sind die Grade gleich, dann ist die Gerade $y = \frac{p_n}{q_n}$ eine waagrechte Asymptote. Ist der Grad von $P$ größer als der Grad von $Q$ so wandelt man um wie in Gleichung 3.3. Bei $\pm\infty$ verhält sich dann die rationale Funktion wie das Polynom $R_0$.

**1.7. Irrationale Funktionen.** Irrationale algebraische Funktionen sind Kombinationen von rationalen Funktionen mit Wurzelfunktionen, z.B.

$$f(x) = \sqrt[4]{x^3 + 4x + 2}$$

$$f(x) = \frac{(x^2 - 2)\sqrt{3x + 4}}{(x - 5)^2 \sqrt[3]{x^2 + x + 1}}$$

Bei der Bestimmung des Definitionsbereiches ist darauf zu achten, dass zusätzlich zu den Nullstellen des Nenners auch jene Bereiche untersucht werden, in denen die Argumente der Wurzelfunktionen deren Definitionsbereich verlassen.

## 2. Transzendente Funktionen

**2.1. Exponentialfunktion, Logarithmus.** Die erste Klasse von transzendenten Funktionen, die wir hier betrachten wollen, sind die *Exponentialfunktionen* und ihre Umkehrungen, die *Logarithmusfunktionen*.

Die Funktion $f$ heißt Exponentialfunktion zur Basis $a$, wenn sie die Gestalt

$$f(x) = a^x, \quad a \in \mathbb{R},\, a > 0,\, a \neq 1$$

hat. Es gilt $D(f) = \mathbb{R}$, und $W(f) = \mathbb{R}^+$. Für $a > 1$ ist die Funktion streng monoton wachsend und für $0 < a < 1$ ist sie streng monoton fallend. Ferner ist sie auf ganz $\mathbb{R}$ konvex und besitzt keine Extrema oder Wendepunkte.

Jede Exponentialfunktion erfüllt die Funktionsgleichung

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

d.h. es gilt $a^{x+y} = a^x a^y$.

Weil die Exponentialfunktionen zur Basis $a$ streng monoton sind, sind sie auch bijektive Abbildungen $\mathbb{R} \to \mathbb{R}^+$, also umkehrbar. Ihre Umkehrfunktionen heißen Logarithmusfunktionen zur Basis $a$, und wir schreiben

$$g(x) = \log_a(x).$$

Der Definitionsbereich der Logarithmusfunktionen ist $\mathbb{R}^+$. Sie sind streng monoton wachsend für $a > 1$ und streng monoton fallend für $0 < a < 1$. Logarithmusfunktionen haben genau eine Nullstelle bei $x = 1$. Sie erfüllen die Funktionsgleichung

$$g(xy) = g(x) + g(y).$$

In der Mathematik ist aus vielen Gründen eine Basis ausgezeichnet gegenüber allen anderen, die *Eulersche Zahl*

$$e := \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n \approx 2.718281828459\ldots$$

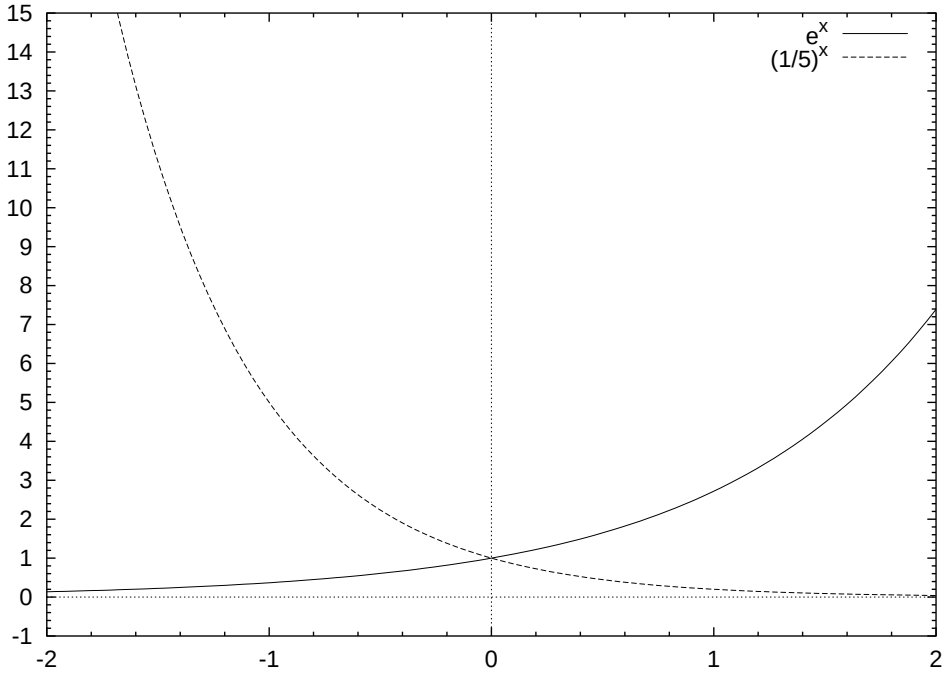



ABBILDUNG 3.7. Exponentialfunktionen

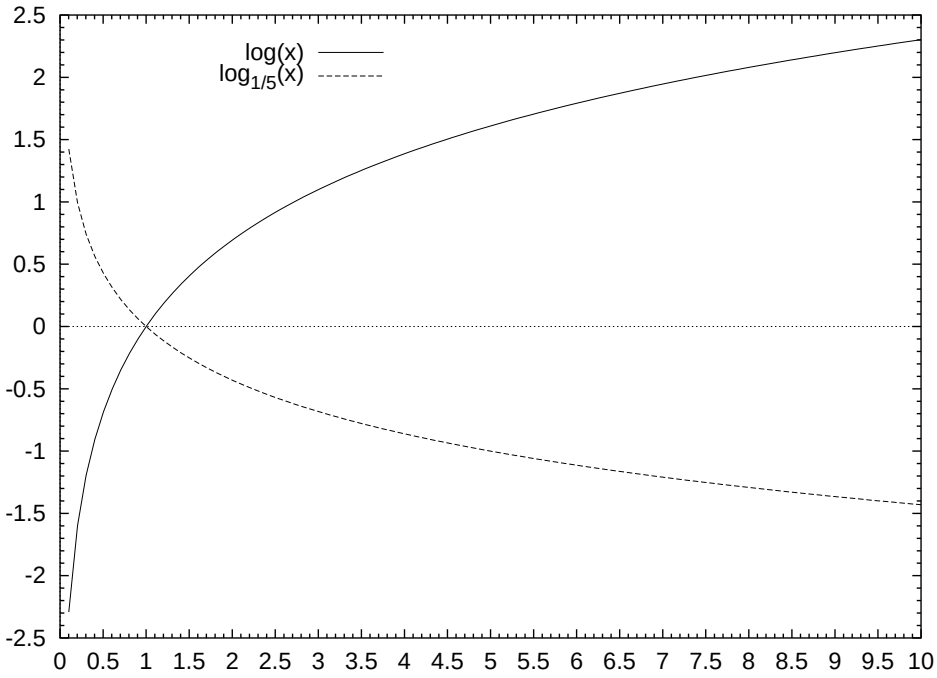



ABBILDUNG 3.8. Logarithmusfunktionen

Das Zeichen := bedeutet, dass wir gerade etwas **definieren**, in diesem Fall geben wir der Eulerschen Zahl den Namen $e$. Merke: Der Doppelpunkt im Zeichen := (oder =:) steht immer auf der Seite des Gleichheitszeichens, auf der der zu definierende Begriff steht.

| $x_{\text{grad}}$ | $x$ | $x_{\text{grad}}$ | $x$ | $x_{\text{grad}}$ | $x$ |
|---|---|---|---|---|---|
| $30°$ | $\frac{\pi}{6}$ | $120°$ | $\frac{2\pi}{3}$ | $225°$ | $\frac{5\pi}{4}$ |
| $45°$ | $\frac{\pi}{4}$ | $135°$ | $\frac{3\pi}{4}$ | $270°$ | $\frac{3\pi}{2}$ |
| $60°$ | $\frac{\pi}{3}$ | $150°$ | $\frac{5\pi}{6}$ | $315°$ | $\frac{7\pi}{4}$ |
| $90°$ | $\frac{\pi}{2}$ | $180°$ | $\pi$ | $360°$ | $2\pi$ |

TABELLE 3.1. Wichtige Winkel in Radiant und Grad

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 unterzubewerten. 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 auseinanderzusetzen.

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* sein.

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

Viele Definitionen verwenden nicht nur verbale Ausdrücke sondern auch mathematische Symbolik. Z.B. Die Menge $P$ aller Primzahlen könnte symbolisch definiert werden als

$$P := \{n \in \mathbb{Z} | n > 1,\ \forall m \in \mathbb{Z} : (m|n \implies (m = 1 \vee m = n))\}.$$

Die Präzision der Beschreibung hängt aber nicht davon ab, wie wenige Worte man verwendet. Man sollte nur stets in der Lage sein, 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.

Die Exponentialfunktion zur Basis $e$ heißt auch *die* Exponentialfunktion. Der Logarithmus zur Basis $e$ wird meist log (manchmal auch ln) geschrieben und wird der *natürliche Logarithmus* genannt.

**2.2. Trigonometrische Funktionen und deren Umkehrungen.** Beginnen wir unseren Exkurs über die **Kreisfunktionen** (**trigonometrischen Funktionen**) mit einem Einheitskreis. In Abbildung 3.9 sind die vier Winkelmaße zum Winkel $x$ eingezeichnet. Wie in der Mathematik üblich, ist der Winkel im **Bogenmaß** (**Radiant**) angegeben, d.h. durch die Länge des Kreisbogens, der dem Winkel entspricht. Die Umrechnung von Radiant ($x$) in Grad ($x_{\text{grad}}$) und umgekehrt erfolgt gemäß der folgenden Formel

$$x_{\text{grad}} = \frac{180x}{\pi}, \quad x = \frac{\pi x_{\text{grad}}}{180}.$$

Wichtige Winkel, die häufig vorkommen, sind in Tabelle 3.1 angegeben, damit sie besser memoriert werden können. Betrachten wir Abbildung 3.9, so sehen wir einen Einheitskreis, der von einer Halbgeraden $g$ geschnitten wird. Die Länge des Bogens vom Punkt $(1, 0)$ zum Schnittpunkt des Kreises mit $g$ wird mit $x$ bezeichnet und gibt, wie gesagt den Winkel, den $g$ mit der $x_1$–Achse einschließt, in Radiant an. Der Schnittpunkt hat dann die Koordinaten $(\cos x, \sin x)$. Die Längen $\tan x$ und $\cot x$ sind als diejenigen Längen eingezeichnet, die $g$ von der senkrechten, bzw. waagerechten, Tangente an den Einheitskreis abträgt.

**2.2.1. Sinus.** Der Sinus...

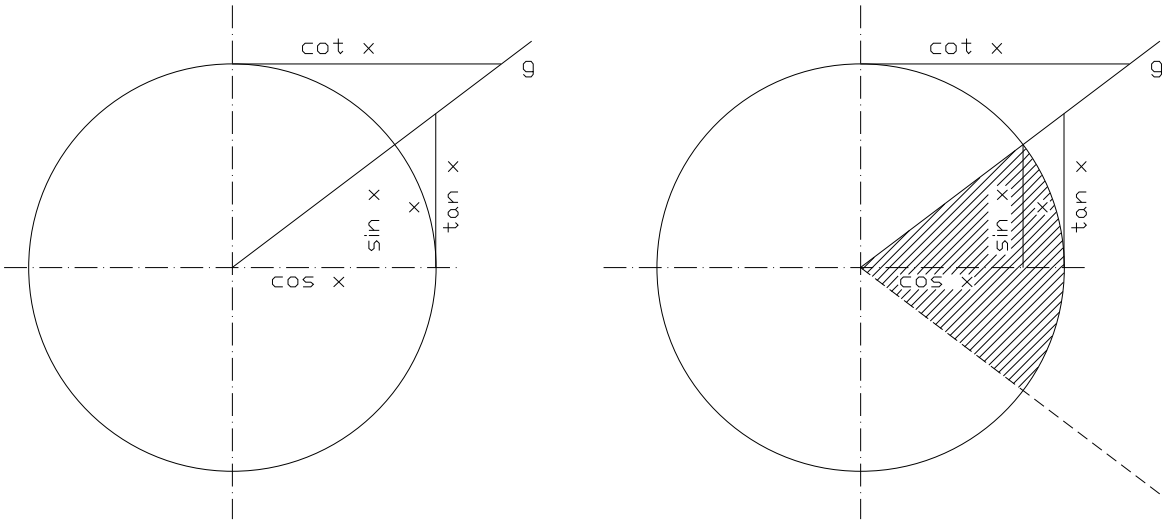



ABBILDUNG 3.9. Definition der trigonometrischen Funktionen

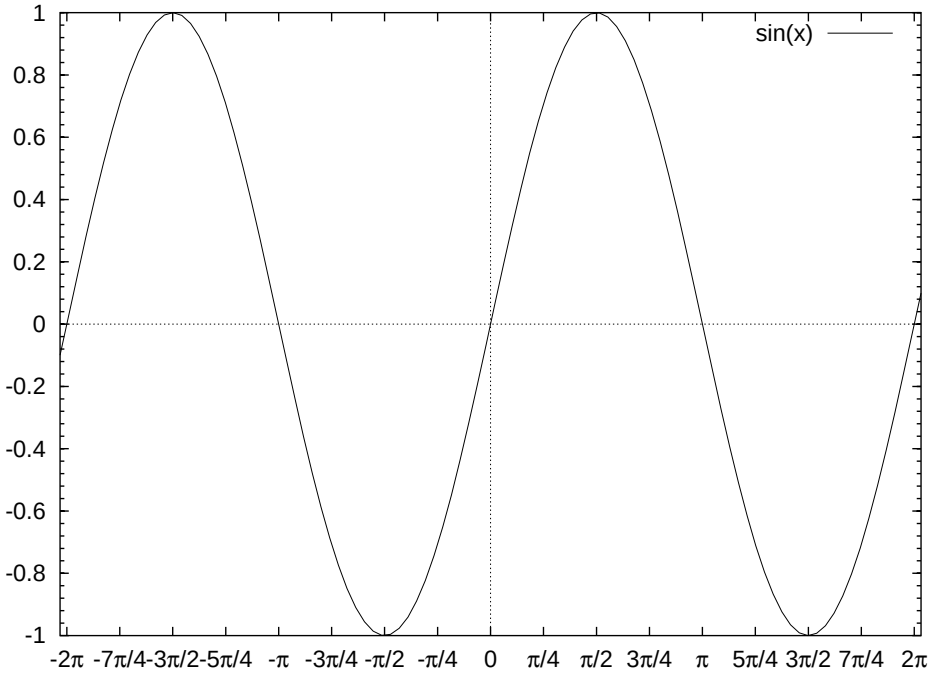



ABBILDUNG 3.10. Die Sinusfunktion

**2.2.2. Cosinus.** Der Cosinus...

**2.2.3. Tangens und Cotangens.** Der Tangens und der Cotangens...

- *sin*, Gegenkathete/Hypothenuse, $y$-Abschnitt im EHK, Graph, Periode $2\pi$, Wertebereich, Nullstellen, Maxima, Minima, Wendepunkte, **ungerade** Funktion
- *cos*, Ankathete/Hypothenuse, $x$-Abschnitt im EHK, Graph, Periode $2\pi$, Wertebereich, Nullstellen, Maxima, Minima, Wendepunkte, **gerade** Funktion
- *tan*, Gegenkathete/Ankathete, $y$-Tangente im EHK, Graph, Periode $\pi$, Wertebereich, Nullstellen, Extrema keine, Wendepunkte, **ungerade** Funktion
- *cot*, Ankathete/Gegenkathete, $x$-Tangente im EHK, Graph, Periode $\pi$, Wertebereich, Nullstellen, Extrema keine, Wendepunkte, **ungerade** Funktion

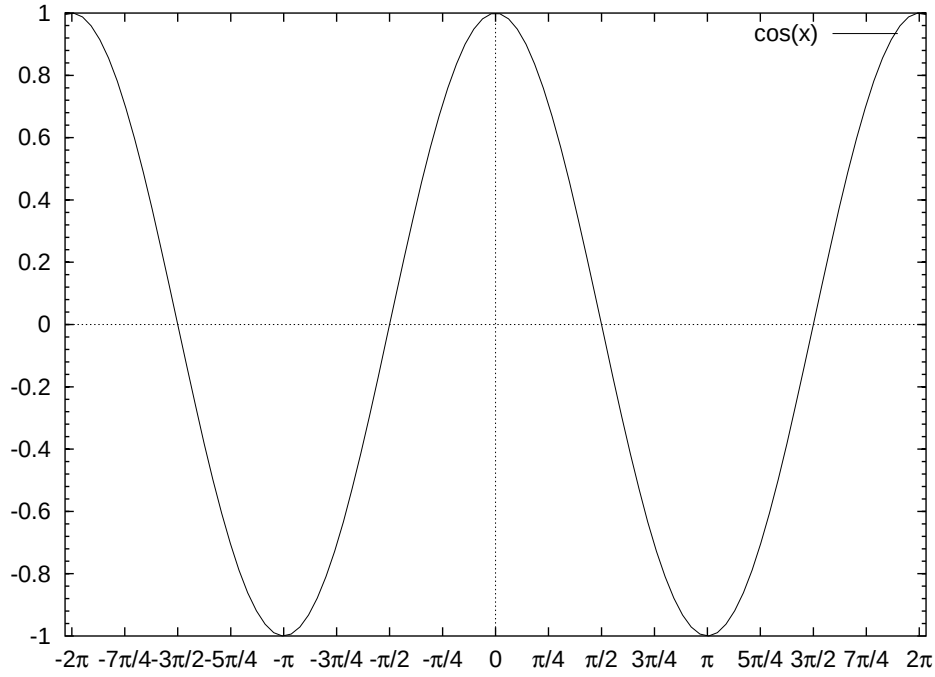



ABBILDUNG 3.11. Die Cosinusfunktion

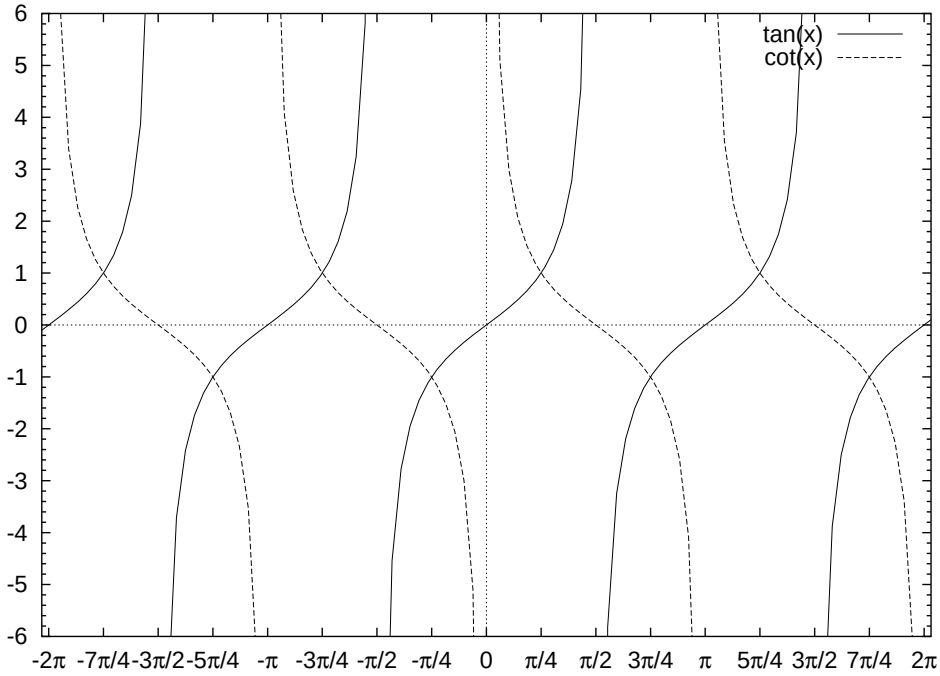



ABBILDUNG 3.12. Die Tangensfunktion und die Cotangensfunktion

- Grundbeziehungen:

$$\sin\left(\frac{\pi}{2}+x\right)=\cos x, \qquad \cos\left(\frac{\pi}{2}+x\right)=-\sin x, \qquad \tan\left(\frac{\pi}{2}+x\right)=-\cot x,$$
$$\sin(\pi+x)=-\sin x, \qquad \cos(\pi+x)=-\cos x, \qquad \cot\left(\frac{\pi}{2}+x\right)=-\tan x.$$
$$\sin\left(\frac{3\pi}{2}+x\right)=-\cos x, \quad \cos\left(\frac{3\pi}{2}+x\right)=\sin x,$$

- Spezielle Werte:

| Bogenmaß | 0 | $\frac{\pi}{6}$ | $\frac{\pi}{4}$ | $\frac{\pi}{3}$ | $\frac{\pi}{2}$ |
|---|---|---|---|---|---|
| $\sin x$ | 0 | $\frac{1}{2}$ | $\frac{\sqrt{2}}{2}$ | $\frac{\sqrt{3}}{2}$ | 1 |
| $\cos x$ | 1 | $\frac{\sqrt{3}}{2}$ | $\frac{\sqrt{2}}{2}$ | $\frac{1}{2}$ | 0 |
| $\tan x$ | 0 | $\frac{\sqrt{3}}{3}$ | 1 | $\sqrt{3}$ | n.def. |
| $\cot x$ | n.def. | $\sqrt{3}$ | 1 | $\frac{\sqrt{3}}{3}$ | 0 |

- Beziehungen:

$$\sin^2 x + \cos^2 x = 1, \quad \tan x = \frac{\sin x}{\cos x}, \quad \cot x = \frac{1}{\tan x}$$

- Moivre:

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

- Additionstheoreme:

$$\sin(x \pm y) = \sin x \cos y \pm \cos x \sin y, \quad \cos(x \pm y) = \cos x \cos y \mp \sin x \sin y,$$
$$\tan(x \pm y) = \frac{\tan x \pm \tan y}{1 \mp \tan x \tan y}, \qquad \cot(x \pm y) = \frac{\cot x \cot y \mp 1}{\cot y \pm \cot x}.$$

- Winkelhalbierung:

$$\sin \tfrac{x}{2} = \pm\sqrt{\frac{1-\cos x}{2}}, \quad \tan \tfrac{x}{2} = \pm\sqrt{\frac{1-\cos x}{1+\cos x}} = \frac{\sin x}{1+\cos x} = \frac{1-\cos x}{\sin x},$$
$$\cos \tfrac{x}{2} = \pm\sqrt{\frac{1+\cos x}{2}}, \quad \cot \tfrac{x}{2} = \pm\sqrt{\frac{1+\cos x}{1-\cos x}} = \frac{\sin x}{1-\cos x} = \frac{1+\cos x}{\sin x},$$

- Siehe auch [**Bronstein et al. 1989**, 2.5.2.1,184].

**2.2.4. Arcussinus.** Arcussinus...

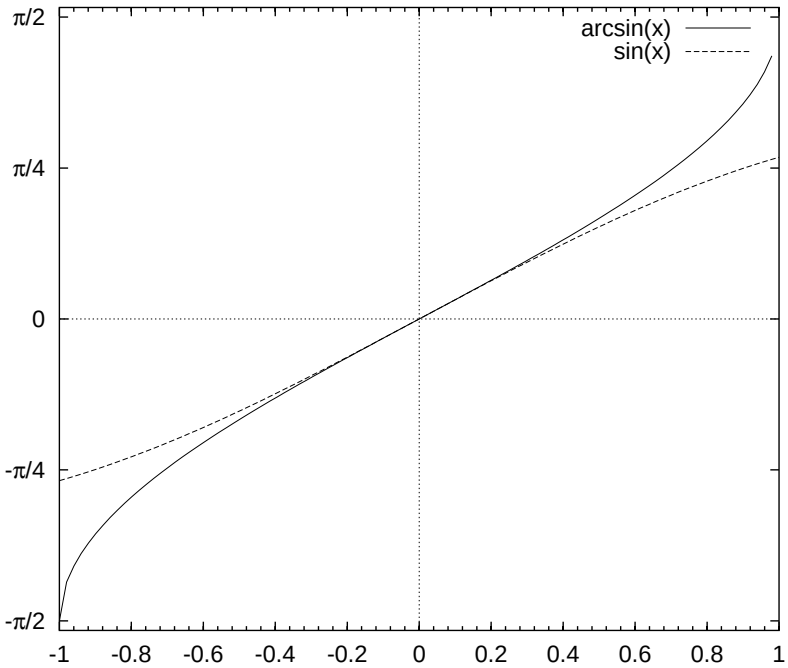



Abbildung 3.13. Die Arcussinusfunktion

**2.2.5. Arcuscosinus.** Arccos...

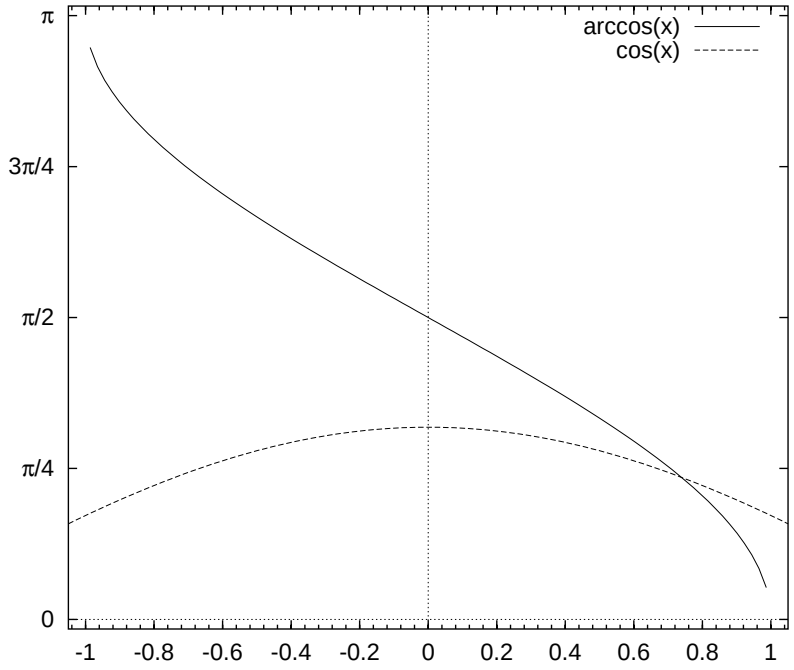



ABBILDUNG 3.14. Die Arcuscosinusfunktion

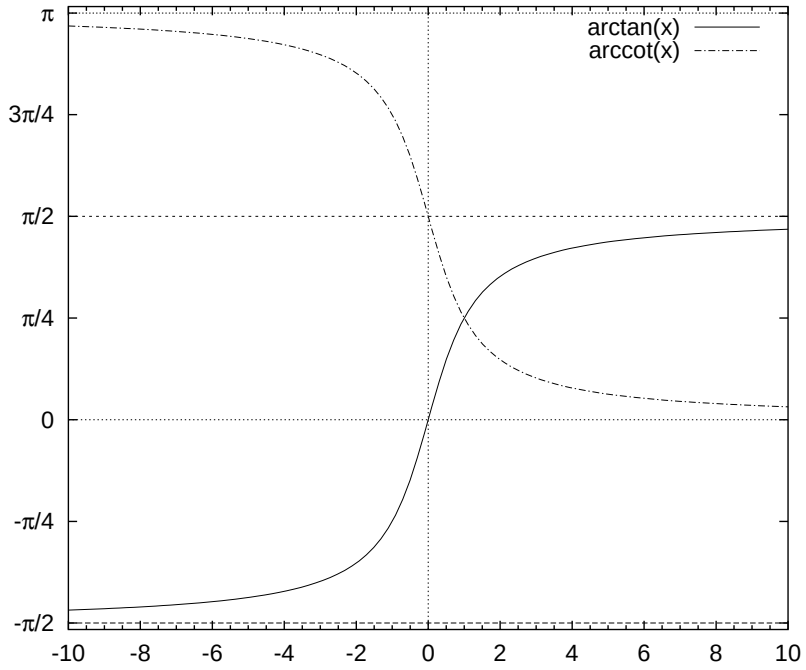



ABBILDUNG 3.15. Die Arcustangens und Arcuscotangens Funktionen

**2.2.6. Arcustangens und Arcuscotangens.** Arctan und Arccot...
Die Umkehrfunktionen der trigonometrischen Funktionen sind die Arcusfunktionen:

- arcsin, Def: $[-1, 1]$, Werte: $[-\frac{\pi}{2}, \frac{\pi}{2}]$, monoton wachsend, Wendepunkt 0, Graph
- arccos, Def: $[-1, 1]$, Werte: $[0, \pi]$, monoton fallend, Wendepunkt 0, Graph
- arctan, Def: $]-\infty, \infty[$, Werte: $]-\frac{\pi}{2}, \frac{\pi}{2}[$, monoton wachsend, Wendepunkt 0, Graph

- arccot, Def: $]-\infty,\infty[$, Werte: $]0,\pi[$, monoton fallend, Wendepunkt 0, Graph
- Siehe auch [**Bronstein et al. 1989**, 2.5.2.1,185].

## 2.3. Hyperbelfunktionen und deren Umkehrungen.

- Graphische Definition mittels Hyperbel
- *sinh*, *cosh*, *tanh*, *coth*
- Siehe Zettel!

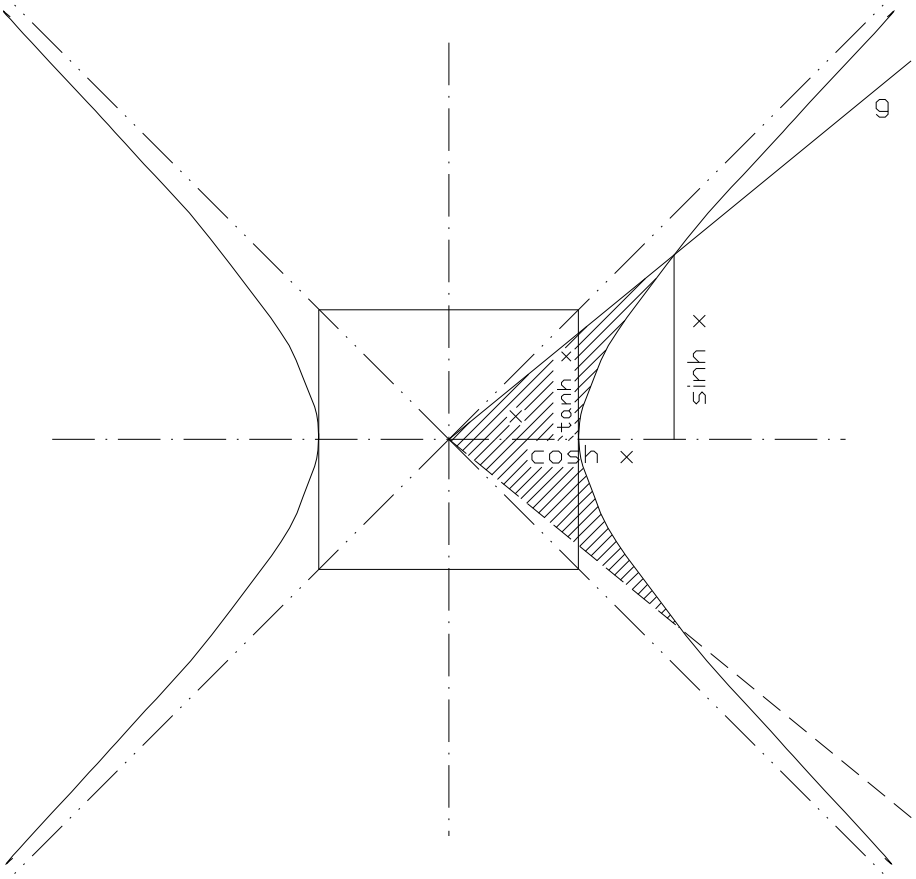



Abbildung 3.16. Definition der hyperbolischen Funktionen

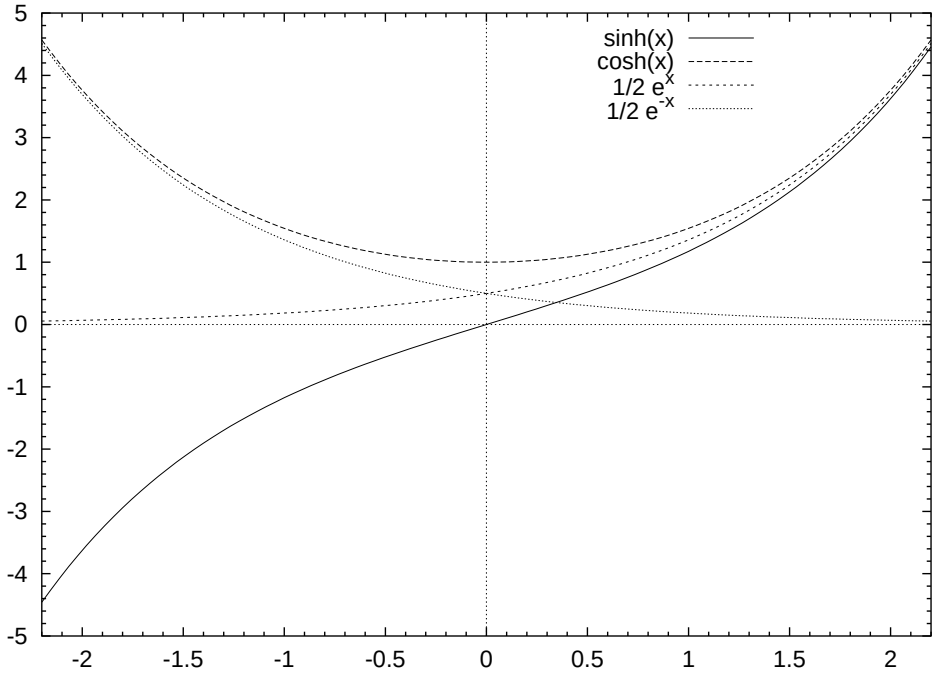



Abbildung 3.17. Sinus hyperbolicus und Cosinus hyperbolicus

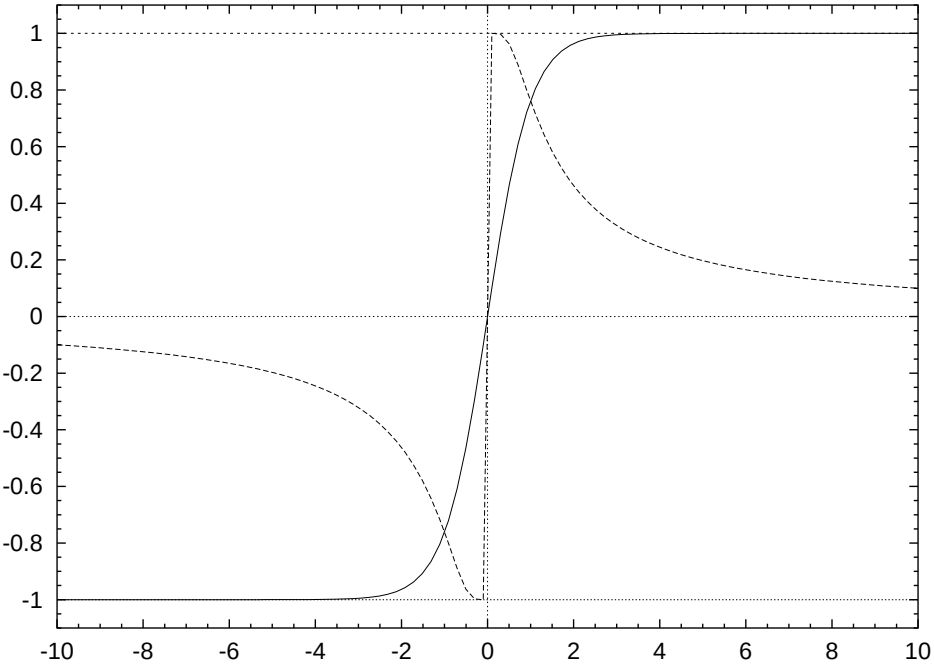



Abbildung 3.18. Tangens hyperbolicus und Cotangens hyperbolicus

KAPITEL 4

# 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*.

## 1. Boolesche Algebren

In diesem Abschnitt wollen wir nochmals das Kapitel über Boolesche Algebren aus der Schule aufarbeiten. Es soll uns nicht dazu dienen, daraus die Grundlage der Mathematik zu bauen. Wir werden uns dabei außerdem auf die Schaltalgebra beschränken, 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 sich 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 läßst 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 Leitung 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.

- Setzt man in einem Stromkreis wie in Abbildung 4.1 zwei Schalter hintereinander, bildet man also eine *Serienschaltung*, und untersucht, wann die Leitung Strom führt, erhält man folgende Schaltwerttabelle:

| $a$ | $b$ | $a \wedge b$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

ABBILDUNG 4.1. 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** $b$.

- Setzt man in einem Stromkreis wie in Abbildung 4.2 zwei Schalter nebeneinander, so wird man folgendes feststellen: Damit die Leitung Strom führt, reicht es Schalter

ABBILDUNG 4.2. Parallelschaltung — Oder-Verknüpfung

$a$ **oder** Schalter $b$ einzuschalten. Eine Schaltung dieser Art nennt man Parallelschaltung und die entsprechende mathematische Verknüpfung heißt **Oder**-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 |

Man beachte, dass „oder“ im Gegensatz zum üblichen Sprachgebrauch bedeutet, dass $a$ oder $b$ oder beide eingeschaltet sein müssen.

- 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 |

Mit elektrischen Leitungen und echten Schaltern kann man nicht leicht komplizierte Schaltungen bauen. Mit elektronischen Schaltern 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.

**Bemerkung 4.1.1.** *Es existieren vier einstellige Operatoren (wie $\neg$) und 16 mögliche binäre Operatoren (wie $\wedge$ oder $\vee$). Interessanterweise gibt es eine Operation, 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*

| $a$ | $b$ | $a \barwedge b$ |
|---|---|---|
| 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* $a \barwedge b = \neg(a \wedge b)$.

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

- *Es gilt* $\neg a = a \barwedge a$*, wie wir an Hand der Schaltwerttabelle leicht überprüfen können:*

| $a$ | $a \barwedge a$ | $\neg a$ |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 0 |

- *Für die ODER Operation 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 |

- *Zuletzt stellen wir die UND Operation 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 hat?

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 $a_1, \ldots, a_n$ abhängt. Möchte man eine Schaltung konstruieren mit $n$ Schaltern, die den Variablen entsprechen, die immer den Wert $f(a_1, \ldots, a_n)$ 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 $f(a_1, \ldots, a_n)$ 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 4.1.2.** *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 üblicherweise sehr kompliziert, und die Frage ist, ob man eine einfachere Schaltung konstruieren kann, die dieselbe Schaltwerttabelle ergibt. Man kann leicht mit Hilfe einzelner Schaltwerttabellen überprüfen, dass die Grundoperationen $\wedge$, $\vee$ und $\neg$ über folgende Gesetze miteinander zusammenhängen:

**Theorem 4.1.3.** *Für die Operationen $\wedge$, $\vee$ und $\neg$ gelten die folgenden Rechenregeln. Dabei seien $a$, $b$ und $c$ Aussagen.*

| | | |
|---|---|---|
| ***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 4.1.4.** *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 4.1.3 lassen sich aus diesen acht herleiten.*

**Beispiel 4.1.5.** *Zwei einfache Beispiele, die im folgenden noch wichtig sein werden, sind die binären Operationen*

| $a$ | $b$ | $a \Rightarrow b$ |
|---|---|---|
| 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*

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

**Beispiel 4.1.6.** *Mit Hilfe der Rechengesetze aus Theorem 4.1.3 können wir versuchen, die disjunktive Normalform aus Beispiel 4.1.2 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.*

## 2. Aussagen, Logik

In der Mathematik werden Begriffen 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 4.2.1.** *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**.

**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.

**2.1.1. $\wedge$.** 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.**

**2.1.2. $\vee$.** Ist die und–Verknüpfung aus der Umgangssprache problemlos zu verstehen, so muss man bei der Definition der oder–Verknüpfung aufmerksam sein.

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*. Das entspricht auch der Tabelle zur Verknüpfung $\vee$.

Möchte man in einer mathematischen Aussage ein Oder so verstanden wissen, dass es, ähnlich zur Umgangssprache, das „oder beides“ ausschließen, 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.

**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.**

**2.1.3. $\neg$.** 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.

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 1 weiter, denn in Theorem 4.1.3 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**

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

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 $\neg(\neg p) = p$.**

**2.1.4. $\Longrightarrow$.** Wie versprochen, wird die in Beispiel 4.1.5 eingeführte binäre Operation, die **Implikation**, an wichtiger Stelle wieder auftauchen. 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 4.2.2.** *Aus* den Voraussetzungen *folgt* das Resultat.

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

Was das bedeutet, können wir erst erkennen, wenn wir die Wahrheitstafel der $\Rightarrow$–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 Voraussetzungen wahr sind aber die Folgerung falsch ist. In allen anderen Fällen ist die Aussage *wahr*.

Eine spezielle Betrachtung verdienen die beiden Fälle, in denen $p$, also die Voraussetzungen, falsch sind. In diesen Fällen ist die Aussage der Implikation nämlich richtig unabhängig davon wie der Wahrheitswert des Resultates ist („ex falso quodlibet“ — lat. aus falschem wie es beliebt). Das macht Sinn, denn wir wollen mit dem Theorem nur Aussagen machen über Fälle, in denen die Voraussetzungen erfüllt sind, und alle anderen Fälle sind uns egal.

Nachdem Schlußfolgerungen *das* Instrument der Mathematik sind, kommen sie in mathematischen Texten augesprochen 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 ist **hinreichend** für; dies ist eine **hinreichende** Bedingung für; dies **impliziert**; **insbesondere**; dies hat zur **Konsequenz**; **mithin**; eine **notwendige** Bedingung dafür ist; 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 den Leser oder Hörer darauf hin weisen, 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 nach zu vollziehen.

- 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 des Lesers 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 ein zu sehen.

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.

Es 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 eine (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.

(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 Beispiel für einen indirekten Beweis.

**Theorem 4.2.3.** *Die Zahl $\sqrt{2}$ ist irrational.*

Beweis. Die Aussage des Satzes als Implikation aufgeschrieben lautet:

Ist $q \in \mathbb{R}$ 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 Zahlern darstellbar ist.

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

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 zu Ende. □

**2.1.5.** $\Longleftrightarrow$ **.** 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 4.2.4.** *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...

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

Noch eine Bemerkung zu den Wörtern **notwendig** und **hinreichend**. 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.

**Beispiel 4.2.5.**
- *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 **wenn**, **dann, wenn**, **nur dann, wenn**:

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

Um ein Beispiel zu geben, betrachten wir die Formulierungen: $A$ ist „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.

**2.2. $\forall$.** Ein Großteil der mathematischen Theorien handelt von Strukturen und Regeln. Ein Beispiel für Regeln sind etwa Rechengesetze, die **für alle** Objekte eine bestimmten Gattung gelten. In diesem Fall verwenden wir das Zeichen $\forall$.

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...
- $\bigwedge m \in M$.
- 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...

Bezieht sich ein $\forall$ auf mehrere Variable auf einmal, so verwendet man auch oft „je zwei“, „je drei“, ...

- Durch je zwei 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 man bei „jedes“ ein beliebiges Objekt im Blick hat:

- 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 *eines* 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.

**2.3. $\exists$ und $\exists!$.** 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 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…
- $\bigvee x \in M$ :
- 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.)

**WICHTIG:** 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 als „Ich habe nicht genau einen Bruder.“ Möchte man das „*nicht*“ zur Aussage befördern, dann müsste man mit einer Fallunterscheidung formulieren: „Ich habe keinen Bruder oder mehr als einen Bruder.“

**2.4. $\forall\exists$ oder $\exists\forall$?** Seien Sie vorsichtig, wenn mehr als ein Quantor $\forall$ oder $\exists$ in einem Satz vorkommt. Dabei kommt es nämlich auf die Reihenfolge an.

**Beispiel 4.2.6.** *Sei $M$ die Menge aller Männer und $F$ die Menge aller Frauen. Die Aussage $h(x, y)$ sei „$x$ ist verliebt in $y$“. 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. Mengen

Mengen sind die erste mathematische Struktur, die wir einführen wollen. An diesem Punkt stoßen wir zum ersten Mal auf ein weiteres Grundprinzip der Mathematik, der 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*.

**3.1. Naive Mengenlehre.** Bevor wir in Abschnitt 4.1 kurz einen mathematisch adäquaten Zugang zur Mengenlehre skizzieren, wollen wir uns zuerst, 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 4.3.1.**
- *Die Menge aller Studenten im Hörsaal.*
- *Die Menge der natürlichen Zahlen.*
- *Die Menge der Lösungen einer Ungleichung.*
- *Die **leere Menge** („ein leerer Sack“).*

Bevor wir weiter in den Begriff „Menge“ eindringen, ein kurzer Blick auf die Vergangenheit, 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

# CONTINUE HERE!

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

**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.

**Beschreiben:** Gemäß der Idee von Cantor können wir die *Eigenschaften der Elemente* einer Menge angeben und sie dadurch definieren. Dies läßt sich auch auf *unendliche* Mengen anwenden. Die Menge $P$ aller Primzahlen ließe sich etwa definieren durch

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

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 weitere Element

$m$ von $\mathbb{N}$, das $p$ teilt, ist entweder 1 oder $p$ selbst. Anders ausgedrückt besitzt $p$ nur die trivialen Teiler 1 und $p$.

Man muss auch nicht rein symbolisch formulieren. Eine ähnlich gute Definition wäre

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

Symbole im Text erhöhen 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 eine Grundregel und eine Anregung, so verbessert das die Lage sofort.

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

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

  besser um

  Die Menge der reellen Zahlen bezeichnen wir mit $\mathbb{R}$.
- **Axiom von Siegel** (nach dem Mathematiker C.L. 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 die Symbole sorgfältig und behalten sie ihre mathematische Bedeutung stets im Auge. Konzentrieren Sie die Symbolik nicht zu sehr. Lassen Sie immer genug an Erklärungen übrig, dass der Text für den Leser flüssig zu lesen und verständlich bleibt.

**Verwenden Sie niemals mathematische Symbole als Abkürzungen für Worte im Text.**

Sei $V$ ein Vektorraum $+$ endlich dimensional.

Die wesentliche Beziehung in der Mengenlehre ist diejenige zwischen den Mengen und deren Elementen. Sie wird durch das Symbol $\in$ ausgedrückt.

**Beispiel 4.3.2.**
- *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 4.3.3.** *Zwei Mengen gelten genau dann als gleich, wenn sie dieselben Elemente haben. In Symbolen notiert:*

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

**Definition 4.3.4.** *Die* ***leere Menge*** $\emptyset$ *ist definiert durch*

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

*Sie ist die Menge, die kein Element enthält. 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. Ein und dasselbe Element kann nicht mehrfach in einer Menge auftreten. Eine Menge ist eine Ansammlung *verschiedener* Objekte!

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

**Definition 4.3.5.** *Eine Menge $B$ heißt **Teilmenge** der Menge $A$, wenn $B$ nur Elemente von $A$ enthält. In der Sprache der Logik formuliert, bedeutet das*

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

*oder kürzer und etwas salopper*

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

*Ist $B$ Teilmenge von $A$, so schreiben wir*

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

**Beispiel 4.3.6.** *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 anderen Teilmengen nennt man auch **echte Teilmengen**. Möchte man betonen, dass $B$ echte Teilmenge von $A$ ist, so schreibt man meist*

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

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

Zur Terminologie: Ist $B$ eine Teilmenge von $A$, so nennt man $A$ eine *Obermenge* von $B$.

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 4.3.7.** *Zwei Mengen $A$ und $B$ sind genau dann gleich, wenn $A \subseteq B$ und $B \subseteq A$.*

Beweis. Dieser Satz behauptet eine Äquivalenz. Um diese zu beweisen, muss man beide Implikationsrichtungen beweisen

Schritt 1: $\Leftarrow$. 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.

Schritt 2: $\Rightarrow$. Wir müssen zeigen, dass aus beiden Enthalten-Relationen schon die Gleichheit folgt. Gelten also $A \subseteq B$ und $B \subseteq A$, so gilt $x \in A \implies x \in B$ wegen $A \subseteq B$. Außerdem wissen wir $x \in B \implies x \in A$ weil $B \subseteq A$ erfüllt ist. Fassen wir die beiden Implikationen zusammen, erhalten wir für beliebiges $x$ den Zusammenhang $x \in A \iff x \in B$. Das wiederum bedeutet laut Definition 4.3.3, dass $A = B$ gilt.

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

**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 4.3.8** (Vereinigung)**.** *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 Mengen definiert, die **Vereinigung**.*

*Man kann auch mehr als zwei Mengen vereinigen, gar 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 $A_i$. Die* Indexmenge *$I$ kann dabei beliebig groß sein. Das bedeutet, wir nehmen alle $x$ die in* wenigstens einer *der Mengen $A_i$ liegen.*

**Beispiel 4.3.9.** *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 4.3.10** (Durchschnitt)**.** *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 $B$. Sie ist definiert durch*

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

*Genau wie die Vereinigung kann man auch den Durchschnitt von mehr als zwei Mengen definieren. Sei wieder $A_i$, $i \in I$ eine Familie von Mengen. Dann ist*

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

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

*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 Universums $U$, so können wir eine weitere Definition hinzufügen.

**Definition 4.3.11** (Komplement)**.** *Sei $A$ eine Teilmenge der Menge $U$. Dann definieren wir das* ***Komplement*** *$\complement A$ von $A$ (in $U$) durch die Beziehung*

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

*bzw. in der noch exakteren Formulierung*

$$\complement A := \{x \mid x \in U \wedge \neg(x \in A)\}.$$

Vergleichen wir die Definitionen mit den logischen Operatoren, die wir in Abschnitt 1 eingeführt haben, so erkennen wir rasch die Zusammenhänge. Die Vereinigung $\cup$ wird gewonnen durch logische ODER ($\vee$) Verknüpfung der Elementbeziehung zu den zu vereinigenden Mengen. Der Durchschnitt entspricht der UND ($\wedge$) Verknüpfung, sowie 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 4.3.12.** *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. Wir beweisen ein Distributivgesetz. Alle anderen Behauptungen folgen analog. Zu zeigen ist: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Wir wissen,

$$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \wedge x \in B \cup C \iff \\ &\iff x \in A \wedge (x \in B \vee x \in C) \iff \text{wegen Theorem 4.1.3} \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \iff \\ &\iff x \in A \cap B \vee x \in A \cap C \iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Außer der explizit angegebenen Äquivalenz gelten alle anderen Zeilen wegen der Definitionen von $\cup$ und $\cap$. Die behauptete Aussage folgt schließlich aus Definition 4.3.3. □

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

**Definition 4.3.13** (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*

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

*Die Komplementbildung $\complement A$ könnte man mit Hilfe dieser Operation und dem Universum $U$ kurz beschreiben als*

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

**Beispiel 4.3.14.** *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 4.3.15** (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 4.3.16.** *Seien $A = \{2, 3, 6\}$ und $B = \{2, 5, 7\}$. Dann ist $A \triangle B = \{3, 6, 5, 7\}$.*

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

**Beispiel 4.3.18.** *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 4.3.19** (Produktmenge)**.** *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 $B$.*

*Sind mehr als zwei 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 $\bigtimes_{i=1}^{k} M_i$ der $M_i$ ist dann die Menge aller geordneten $k$-tupel dieser Form.*

*Ist $A = B$ bzw. $A = M_i$ für alle $i$, so schreiben wir statt $A \times A$ und $A \times \ldots \times A$ kurz $A^2$ bzw. $A^k$.*

**Beispiel 4.3.20.** *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 nachgeholt werden.

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

**Beispiel 4.3.21.** *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.*

Beziehungen in der Art von Beispiel 4.3.21 zwischen Elementen von Mengen nennt man Relationen. Im folgenden wollen wir eine mathematische Definition dafür geben.

**Definition 4.3.22** (Relation)**.** *Sei $M$ eine Menge. Eine Teilmenge $R \subseteq M \times M$ der geordneten Paare von Elementen aus $M$ heißt* ***Relation auf*** *$M$.*

*Für zwei Elemente $a, b \in M$ 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 3.2.2) verwendet, während symmetrische Symbole wie $\simeq$ meist für Äquivalenzrelationen (siehe Abschnitt 3.2.1) stehen.

**Beispiel 4.3.23.** *Die Relationen aus Beispiel 4.3.21 sind natürlich Relationen. 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 4.3.24.** *Eine Relation $R$ auf einer Menge $M$ heißt* ***transitiv****, wenn für alle $a, b, c \in M$*

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

*Die Relation $R$ heißt* ***reflexiv****, wenn für alle $a \in M$ gilt, dass $a \, R \, a$.*

**Beispiel 4.3.25.** *Kehren wir noch einmal zu den Relationen aus Beispiel 4.3.21 zurück. Beide sind transitiv, denn wenn $A$ mit $B$ und $B$ mit $C$ verwandt sind, so ist natürlich auch $A$ mit $C$ verwandt. Ähnliches gilt für Brüder. Ist $A$ Bruder von $B$ und $B$ Bruder von $C$, so ist auch $A$ Bruder von $C$.*

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

### 3.2.1. Äquivalenzrelation.

**Definition 4.3.26.** *Eine* reflexive und transitive *Relation $\sim$ auf einer Menge $M$ heißt* ***Äquivalenzrelation****, falls sie folgende weitere Eigenschaft erfüllt:*

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

*Gilt $a \sim b$, so nennen wir $a$ und $b$* ***äquivalent****.*

**Beispiel 4.3.27.** *Wenn wir ein weiteres Mal die Relationen aus Beispiel 4.3.21 bemühen, so erkennen wir schnell, dass „verwandt mit“ eine Äquivalenzrelation ist. Die Symmetrie ist erfüllt, denn wenn $A$ mit $B$ verwandt ist, ist auch $B$ mit $A$ verwandt.*

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

Ist eine Äquivalenzrelation $\sim$ auf einer Menge definiert, so können wir die Relation dafür verwenden, miteinander äquivalente Elemente von $M$ in Gruppen zusammenzufassen.

**Definition 4.3.28.** *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, dass für jedes $a \in M$ die Äquivalenzklasse $C_a \subseteq M$ erfüllt. Da $a \in C_a$ gilt wegen der Reflexivität von $\sim$, haben wir $\bigcup_{a\in M} C_a = M$. Doch die zweite wichtige Eigenschaft der Äquivalenzklassen wollen wir in der nachfolgenden Proposition fest halten.

**Proposition 4.3.29.** *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*

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

Beweis. Ist $C_a = C_b$, so ist auch $C_a \cap C_b = C_a \neq \emptyset$, weil Äquivalenzklassen nie leer sind.

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 Reflexivität 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. □

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

(1) $\bigcup_{a\in M} C_a = M$ und
(2) $C_a \cap C_b \neq \emptyset \iff C_a = C_b$

erfüllen. Eine solche Familie disjunkter Teilmengen einer Menge, die die gesamte Menge **überdecken**, nennt man **Partition**.

**Theorem 4.3.30.** *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*

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

Beweis. Wir wissen bereits, dass eine Äquivalenzrelation auf $M$ eine Partition definert, 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 4.3.31.** *Sei $M$ eine Menge, $\sim$ eine Äquivalenzrelation. Wir definieren die* ***Faktormenge*** *$M/_\sim$ als die Menge aller Äquivalenzklassen bezüglich $\sim$.*

**Beispiel 4.3.32.** *Sei auf $\mathbb{Z}$ die Relation*

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

*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*

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

*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*** *$p$.*

**3.2.2. Ordnungsrelation.** Die zweite große Klasse von Relationen dienen dazu, Mengen zu ordnen.

**Definition 4.3.33.** *Eine* reflexive und transitive *Relation $\preceq$ auf $M$ heißt* ***Halbordnung****, falls sie die zusätzliche Eigenschaft*

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

$$a \preceq b \wedge b \preceq a \implies a = b$$

*erfüllt*

*Gilt ferner 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 schlicht* ***Ordnung*** *auf $M$.*

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

**Definition 4.3.34.** *Um mit Ordnungsrelationen leichter hantieren zu können, müssen wir einige Schreibweisen definieren. 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 $y \succ x$.*

**Beispiel 4.3.35.** *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 $B$ ein Vorfahre von $A$ 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 4.3.36.** *Sei $(M, \preceq)$ eine geordnete Menge, und sei $E \subseteq M$ eine Teilmenge. Gibt es ein $\beta \in M$ mit der Eigenschaft*

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

*so nennen wir $\beta$ eine* ***obere Schranke von*** *$E$.* ***Untere Schranken*** *definiert man analog durch Ersetzen von $\preceq$ durch $\succeq$.*

*Eine Teilmenge $E \subseteq M$ heißt **nach oben (unten) beschränkt**, falls sie eine obere (untere) Schranke besitzt. Sie heißt **beschränkt**, falls sie nach oben und unten beschränkt ist.*

**Beispiel 4.3.37.** *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 $E$.*

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 in Kapitel 6 zu $\mathbb{R}$ führen. Hier wollen wir uns mit einer Definition begnügen.

**Definition 4.3.38.** *Sei $(M, \preceq)$ eine geordnete Menge, und sei $E$ eine nach oben beschränkte Teilmenge. Existiert ein $\alpha \in M$ mit den Eigenschaften*

(1) *$\alpha$ ist eine obere Schranke von $E$,*
(2) *Ist $\gamma < \alpha$, so ist $\gamma$ keine obere Schranke von $E$.*

*In diesem Fall nennen wir $\alpha$ die **kleinste obere Schranke** oder das **Supremum** von $E$, und wir schreiben*

$$\alpha = \sup E$$

*Analog definieren wir die **größte untere Schranke**, das **Infimum***

$$\alpha = \inf E$$

*einer nach unten beschränkten Teilmenge.*

**Beispiel 4.3.39.** *Betrachten wir noch einmal $(\mathbb{R}, \leq)$ und $E = [0, 1]$. Dann sind $\inf E = 0$ und $\sup E = 1$.*

**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.

**Definition 4.3.40.** *Seien $A$ und $B$ Mengen. Eine Teilmenge $f \subseteq A \times B$ heißt **Abbildung von $A$ nach $B$**, wenn*

$$\forall a \in A : \exists! b \in B : (a, b) \in f,$$

*oder in Worten, wenn zu jedem Element in $A$ genau ein Element von $B$ gehört. Wir schreiben dann*

$$f : A \to B$$
$$f(a) = b$$
$$f : a \mapsto b$$
$$b = a^f \quad \textit{(sehr selten)}$$

*und nennen $b$ das **Bild** von $a$ (unter $f$) und $a$ ein **Urbild** von $b$. Die Menge $A$ heißt der **Urbild-** oder **Definitionsbereich** von $f$, und die Menge $B$ nennen wir auch **Bildbereich** von $f$.*

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 5) ist.

Eine **Transformation** ist eine Abbildung einer Menge in sich (also für $A = B$). Eine bijektive 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 $f(\cancel{x})$ ...

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

**Definition 4.3.41.** *Sei $f : A \to B$ eine Abbildung, und sei $M \subseteq A$ eine Teilmenge. Wir nennen die Menge*

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

*das **Bild der Menge** $M$ **unter** $f$.*

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

**Definition 4.3.42.** *Sei wieder $f : A \to B$ eine Abbildung, doch nun sei $N \subseteq B$ eine Teilmenge des Bildbereiches. Wir definieren die Menge*

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

*und nennen sie das **Urbild der Menge** $N$. Für ein Element $b \in B$ definieren wir das **Urbild von** $b$ durch $f^{-1}(b) := f^{-1}(\{b\})$. Beachte dabei, dass das Urbild von $b$* eine Menge *ist!*

**Beispiel 4.3.43.** *Betrachten wir 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 4.3.44.** *Sei $f : A \to B$ eine Abbildung. Wir sagen $f$ ist*

**injektiv:** *wenn verschiedene Urbilder auch verschiedene Bilder haben. In Symbolen können wir schreiben*

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

**surjektiv:** *wenn jedes Element von $B$ von $f$ getroffen wird, also ein Bild besitzt. In Symbolen:*

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

**bijektiv:** *wenn $f$ injektiv und surjektiv ist.*

**ACHTUNG:** 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 Funktion $f : x \mapsto x^2$ untersuchen, dann können wir abhängig von Definitions- und Bildbereich alle Varianten finden:

(1) $f : \mathbb{R} \to \mathbb{R}$ ist weder injektiv noch surjektiv, weil $f(-1) = f(1)$, was der Injektivität widerspricht und $-1$ nicht von $f$ getroffen wird.

(2) $f : \mathbb{R}_0^+ \to \mathbb{R}$ ist injektiv aber nicht surjektiv.
(3) $f : \mathbb{R} \to \mathbb{R}_0^+$ ist surjektiv aber nicht injektiv.
(4) $f : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ ist bijektiv.

Ein weiteres, wichtiges Beispiel für eine bijektive Abbildung ist für jede Menge $M$ die **Identität** $\mathbb{1}_X : M \to M$ mit der Definition $\mathbb{1}_X(m) = m$ für alle $m \in M$.

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 4.3.45.** *Seien $(A, \preceq)$ und $(B, \trianglelefteq)$ zwei geordnete Mengen. Eine Abbildung $f : A \to B$ heißt **monoton wachsend**, falls aus $x \preceq y$ schon $f(x) \trianglelefteq f(y)$ folgt. Sie heißt **monoton fallend**, falls sich aus $y \preceq x$ die Relation $f(x) \trianglelefteq f(y)$ ergibt.*

**Beispiel 4.3.46.** *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*.

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 4.3.47.** *Seien $f : A \to B$ und $g : B \to C$ zwei Abbildungen. Wir definieren die **Verknüpfung von $f$ mit $g$** (Hintereinanderausführung von $f$ und $g$) $g \circ f : A \to C$ 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 $f(a) = b$. Wir können also eine neue Funktion $f^{-1} : B \to A$ definieren, die jedem Element $b \in B$ das Urbild zuordnet. Man nennt die Abbildung $f^{-1}$ die **inverse Abbildung von** $f$ oder die **Umkehrfunktion von** $f$. 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

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

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

**Definition 4.3.48** (Cartesisches Produkt)**.** *Seien $M_i$, $i \in I$ Mengen. Wir definieren*

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

*das **Cartesische Produkt** der $M_i$.*

Man beachte, dass diese Definiton für endliche Indexmengen $I$ äquivalent ist zur Definition mit $k$-tupeln.

**3.4. Mächtigkeit.** Eine interessante Eigenschaft von Mengen, die diesen intrinsisch ist, ist ihre **Mächtigkeit**. Für endliche Mengen $M$ ist die Mächtigkeit $|M|$ einfach die Anzahl der Elemente.

Meist wird die Mächtigkeit einer Menge $M$ mit $|M|$ bezeichnet. Besonders in der Topologie und der axiomatischen Mengenlehre wird die Mächtigkeit (oder Kardinalität) von $M$ auch mit $\mathrm{card}(M)$ bezeichnet, um explizit darauf hin zu weisen, dass die Mächtigkeit von $M$ eine **Kardinalzahl** ist.

Wie fast alles in der Mengenlehre geht auch das Konzept der Mächtigkeit einer Menge 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.

**Definition 4.3.49.** *Zwei Mengen $A$ und $B$ heißen* gleich mächtig, *wenn eine bijektive Abbildung (eine **Bijektion**) von $A$ auf $B$ existiert.*

Diese einfache Definition hat weit reichende Konsequenzen. Es wird zum einen möglich, dass eine Menge zu einer echten Teilmenge gleich mächtig ist.

**Beispiel 4.3.50.** *Betrachten wir die Menge $\mathbb{N}$ und die Menge $\mathbb{N}_g$ aller geraden Zahlen. Es gilt $\mathbb{N}_g \subsetneq \mathbb{N}$, 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 4.3.51.** *Eine Menge ist unendlich genau dann, wenn sie eine gleich mächtige echte Teilmenge besitzt.*

Beweis. Ohne Beweis. □

Cantor hat schon 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. $\mathbb{N}$, $\mathbb{R}^n$, ...), die meisten Aussagen in der mathematischen Theorie handeln von unendlich vielen Objekten.

Das Symbol für den Ausdruck *unendlich* ist $\infty$. 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 $\infty$ ist keine Kardinalzahl. Daher ist obige Formulierung *keine* mathematisch exakte Aussage.

Man verwendet $\infty$ 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 $x$.

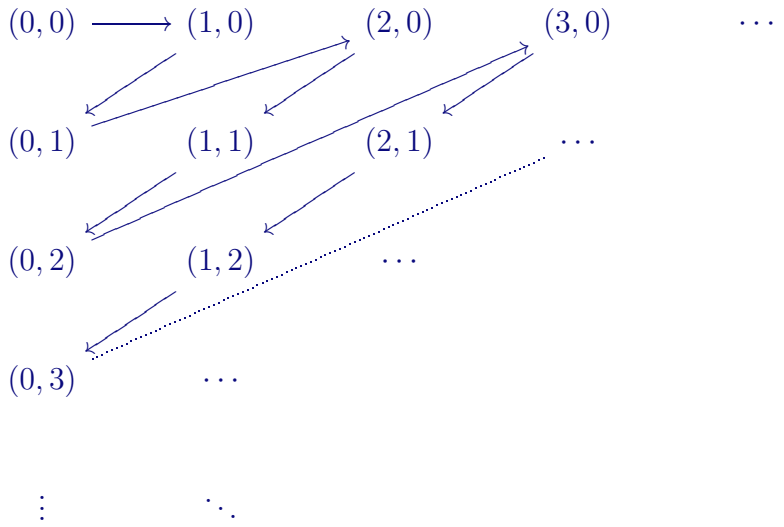
Auch hier ist $\infty$ nur eine *Abkürzung* für die $\varepsilon$-$\delta$–Definition aus der Analysis. Dasselbe gilt für die Notation in unendlichen Reihen.

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

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

Was ist 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. 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 auch schon knapp vor der Jahrhundertwende bewiesen, dass $\mathbb{N} \times \mathbb{N}$ abzählbar ist.




Eine Formel für die Zuordnung ist

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

Nachdem die 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.

Interessant ist, dass die reellen Zahlen $\mathbb{R}$ mächtiger sind als $\mathbb{N}$. 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 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.

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

Betrachten wir jetzt die reelle Zahl $r$ mit der Dezimalentwicklung

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

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

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

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 $\mathbb{N}$. Für die Potenzmenge $\mathbb{P}M$ einer Menge $M$ kann man allgemein zeigen, dass $|\mathbb{P}M| > |M|$ gilt (die Mächtigkeit der Potenzmenge einer Menge erfüllt $|\mathbb{P}M| = 2^{|M|}$). 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 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 solch unangenehme Fakten mit sich, die zeigen, dass es noch nicht geschafft wurde, den naiven Mengenbegriff so gut zu axiomatisieren, dass die Axiome all unsere Vorstellungswelt einzufangen im Stande sind.

## 4. Axiomatische Mengenlehre

**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 Russelsche 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 Quine–Morse, 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 zu machen, 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 $\varphi$ und $\psi$ beliebige Formeln bezeichne, 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“ $\varphi$. 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 $\varphi$ 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 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 Russelsche 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:** $\forall \mathcal{F} : \big(\forall H \in \mathcal{F} : \neg(H = \emptyset) \wedge \forall F \in \mathcal{F} : \forall G \in \mathcal{F} : (F = G \vee F \cap G = \emptyset) \Rightarrow \exists S : \forall F \in \mathcal{F} : \exists! s(s \in S \wedge s \in F)\big)$ (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. Sie sollte nur einen kurzen Einblick geben in das tatsächliche Fundament der Mathematik. Weiterführende Information kann man in den Vorlesungen „Grundbegriffe der Mathematik“ und „Axiomatische Mengenlehre“ finden.

KAPITEL 5

# Algebra

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

Alle hier besprochenen Strukturen basieren auf dem Mengenkonzept. Es sind Mengen zusammen mit Abbildungen, die bestimmte Eigenschaften aufweisen.

## 1. Gruppen

**Definition 5.1.1.** *Sei $G$ eine Menge. Eine **Verknüpfung** auf $G$ ist eine Abbildung $\circ : G \times G \to G$. An Stelle von $\circ(g,h)$ für zwei Elemente $g,h \in M$ schreiben wir $g \circ h$, und wir nennen das Bild von $(g,h)$ das **Ergebnis** der Verknüpfung.*

*Wenn wir die Menge zusammen mit ihrer Verknüpfung untersuchen, so schreiben wir meist $(G,\circ)$ nennen sie **Gruppoid** (oder **Magma**).*

*Unter der **Ordnung** $|G|$ eines Gruppoids verstehen wir die Anzahl seiner Elemente.*

*Betrachten wir mehr als eine Verknüpfung auf der Menge $G$, so nehmen wir auch die anderen Verknüpfungssymbole auf, z.B. $(B,\wedge,\vee)$.*

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

Wird die Verknüpfung mit $\circ$ oder mit $\cdot$ bezeichnet, so lässt man das Verknüpfungssymbol meist weg, sofern keine Mehrdeutigkeiten bestehen. Man schreibt dann statt $g \circ h$ einfach $gh$. Kommen $\circ$ und $\cdot$ vor und ist das Verknüpfungszeichen weggelassen worden, so wurde immer auf ein $\cdot$ verzichtet. Z.B. darf man statt $(g \circ h) \cdot k$ schreiben $(g \circ h)k$. Falsch wäre $(gh) \cdot k$.

**Definition 5.1.2.** *Ein Gruppoid $(G,\circ)$ heißt **Halbgruppe**, falls die Verknüpfung **assoziativ** ist, also das **Assoziativgesetz***

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

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

**Beispiel 5.1.3.** *Die Menge $\mathbb{N}$ zusammen mit der Addition $+$ bildet eine Halbgruppe. Es gilt bekannterweise $(m+n)+k = m+(n+k)$ für alle natürlichen Zahlen.*

*Die Menge $(\mathbb{N},\cdot)$ zusammen mit der Multiplikation bildet ebenfalls eine Halbgruppe.*

*Die Menge $(\mathbb{FP}_2,\oplus)$ der Gleitkommazahlen mit zwei signifikanten Stellen bildet bezüglich der Addition mit Runden* keine *Halbgruppe, denn*

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

*widerspricht der Assoziativität.*

Wenn wir das Beispiel der natürlichen Zahlen betrachten, so sehen wir, dass es für beide Verknüpfungen $+$ und $\cdot$ ein spezielles Element gibt, 0 für die Addition bzw. 1 für die Multiplikation.

**Definition 5.1.4.** *Sei $(G, \circ)$ ein Gruppoid. Ein Element $e \in G$ heißt **Linkseinselement** (**linksneutrales Element**), falls die Beziehung*

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

*stimmt.*

*Das Element $e \in G$ heißt **Rechtseinselement** (**rechtsneutrales Element**), wenn sich bei Verknüpfung von rechts nichts ändert:*

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

*Das Element $e \in G$ heißt **Einselement** oder **neutrales Element**, falls es Links- und Rechtseinselement ist. Wird die Verknüpfung mit $+$ bezeichnet (additiv geschrieben), so bezeichnet man $e$ oft mit $0$ oder $\mathbb{0}$ und nennt es **Nullelement**.*

**Proposition 5.1.5.** *Ist $(G, \circ)$ ein Gruppoid mit Linkseinselement $e_L$ und Rechtseinselement $e_R$, so besitzt $G$ ein Einselement $e$ und es gilt $e_L = e_R$. Speziell gilt, dass das Einselement eines Gruppoides immer* eindeutig bestimmt ist*, falls es existiert.*

Beweis. Es gilt $e_L = e_L e_R$, da $e_R$ ein Rechtseinselement ist, und weil $e_L$ linksneutral ist, haben wir $e_L e_R = e_R$. Aus diesen Gleichungen sieht man aber sofort $e_L = e_R$. Setzen wir $e = e_L = e_R$, so erhalten wir das gewünschte Einselement. Gäbe es zwei Einselemente $e_1$ und $e_2$, so wäre jedes links- und rechtsneutral und aus dem ersten Teil würde $e_1 = e_2$ folgen. Daher ist $e$ eindeutig bestimmt. □

**Proposition 5.1.6.** *Ein Einselement $e$ eines Gruppoids $(G, \circ)$ ist immer **idempotent**. Ein Element $g \in G$ heißt idempotent, falls $g \circ g = g$ gilt.*

Beweis. Es gilt $e \circ e = e$, weil $e$ Einselement ist. □

Wie schon erwähnt, ist 0 ein Nullelement für die Addition in $\mathbb{N}$. Die Zahl 1 ist ein Einselement für die Multiplikation von natürlichen Zahlen.

**Definition 5.1.7.** *Ist $(G, \circ)$ eine Halbgruppe und existiert ein Einselement $e \in G$, so nennt man $G$ auch **Monoid** und schreibt $(G, \circ, e)$.*

**Beispiel 5.1.8.** *Sowohl $(\mathbb{N}, +)$ als auch $(\mathbb{N}, \cdot)$ sind Monoide.*

**Definition 5.1.9.** *Eine Verknüpfung in einem Gruppoid $(G, \circ)$ heißt **kommutativ**, falls das **Kommutativgesetz** erfüllt ist:*

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

**Definition 5.1.10.** *Sei ein Monoid $(G, \circ, e)$ gegeben. Ist $a \in G$, so nennen wir $a' \in G$ ein zu $a$ **linksinverses Element**, falls*

$$a' \circ a = e$$

*gilt. Es heißt zu $a$ **rechtsinvers**, wenn die umgekehrte Beziehung*

$$a \circ a' = e$$

*erfüllt ist. Ist $a'$ sowohl links- als auch rechtsinvers, so sagen wir $a'$ ist ein **inverses Element** von $a$ (oder ein **Inverses zu** $a$) und schreiben meist $a^{-1}$.*

**Proposition 5.1.11.** *Sei $(G, \circ, e)$ ein Monoid und $g \in G$. Ist $g_L^{-1}$ ein Linksinverses von $g$ und $g_R^{-1}$ ein Rechtsinverses, so ist $g_L = g_R$. Speziell sind inverse Elemente eindeutig bestimmt.*

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

**Beispiel 5.1.12.** *In $(\mathbb{N}, +, 0)$ gibt es außer für 0 zu keinem Element ein Inverses. In $(\mathbb{Z}, +, 0)$, andererseits, hat jedes Element $n \in \mathbb{Z}$ ein inverses Element, nämlich $-n$.*

**Definition 5.1.13.** *Ein Monoid $(G, \circ, e)$ heißt **Gruppe**, falls zu jedem Element von $G$ ein Inverses existiert:*

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

*Schreiben wir die Gruppenoperation mit $+$, so bezeichnen wir das Inverse von $g$ mit $-g$.*

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

**Beispiel 5.1.14.** *Die ganzen Zahlen $(\mathbb{Z}, +, 0)$ bilden eine abelsche Gruppe.*

**Beispiel 5.1.15.** *Betrachten wir ein ebenes gleichseitiges Dreieck und alle Abbildungen, die das Dreieck auf sich selbst abbilden (solche Abbildungen nennt man* Deckabbildungen*). Es gibt sechs verschiedene solche Abbildungen:*

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

*Die Menge dieser Abbildungen bildet eine Gruppe bezüglich Verknüpfung von Abbildungen. Man kann die Wirkung der Abbildung am einfachsten veranschaulichen, indem man beobachtet, wohin die Eckpunkte abgebildet werden. Die Abbildung $D_1$ etwa bildet die Ecken $ABC$ auf die Ecken $BCA$ (in der Reihenfolge) ab. Die Spiegelung $S_a$ bildet $ABC$ auf $ACB$ ab. Man sieht also, dass die Deckabbildungen des gleichseitigen Dreiecks genau die Permutationen der Eckpunkte sind. Die dabei entstehende Gruppe heißt $\mathfrak{S}^3$, und ihre **Verknüpfungstabelle** ist*

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

*Dies ist eine Gruppe, die Permutationsgruppe von drei Elementen, eine* nicht *abelsche Gruppe.*

Wir können die Eigenschaften einer Gruppe noch einmal zusammenfassen, da sie so über den Abschnitt verstreut sind. Dabei möchte ich auch beweisen, dass man nur einen Teil der Eigenschaften tatsächlich überprüfen muss.

**Proposition 5.1.16.** *Sei $(G, \circ)$ ein Gruppoid. Sind folgende Eigenschaften erfüllt, dann ist $G$ eine Gruppe.*

**G1:** *Assoziativgesetz: $\forall g, h, k \in G : (g \circ h) \circ k = g \circ (h \circ k)$.*
**G2:** *Linkseinselement: $\exists e \in G : \forall g \in G : e \circ g = g$.*
**G3:** *Linksinverse: $\forall g \in G : \exists g^{-1} \in G : g^{-1} \circ g = e$.*

BEWEIS. Wir haben nicht alles vorausgesetzt, was wir vorher von einer Gruppe verlangt hatten. Eigenschaft G1, das Assoziativgesetz macht $(G, \circ)$ zu einer Halbgruppe, doch wir haben nur *Links*einselement und *Links*inverse vorausgesetzt. Wir müssen also zeigen, dass das Linkseinselement auch Rechtseinselement ist und dass alle Linksinversen auch Rechtsinverse sind.
*Schritt 1:*
Wir beginnen mit einer Teilbehauptung. Ist $g \in G$ idempotent, so gilt schon $g = e$. Wir haben nämlich

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

Das beweist unsere Teilbehauptung.
*Schritt 2:*
Jetzt beweisen wir, dass das Linksinverse $g^{-1}$ auch $gg^{-1} = e$ erfüllt.

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

Aus obiger Beziehung folgt, dass $gg^{-1}$ idempotent ist. Wir haben aber in Schritt 1 bewiesen, dass dann schon $gg^{-1} = e$ gilt.
*Schritt 3:*
Es bleibt noch zu zeigen, dass für alle $g \in G$ auch $ge = g$ gilt, $e$ also Rechtsinverses ist.

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

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

**Proposition 5.1.17.** *Ist $(G, \circ)$ eine Gruppe, so haben wir für jedes $g \in G$*

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

BEWEIS. Einfach. □

**Proposition 5.1.18.** *Ist $(G, \circ)$ eine Gruppe, so gelten die Rechenregeln*

(1) $\forall g, h \in G : (g \circ h)^{-1} = h^{-1} \circ g^{-1}$,
(2) $\forall g, h, k \in G : ((k \circ g) = (k \circ h) \Rightarrow g = h$.

BEWEIS. (1) Es gilt $(g \circ h) \circ (h^{-1} \circ g^{-1}) = g \circ (h \circ h^{-1}) \circ g^{-1} = g \circ g^{-1} = e$. Der Rest folgt aus der Eindeutigkeit der Inversen.

(2) Wir haben

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

□

So ähnlich wie mit Teilmengen kann man auch Teile von Gruppen betrachten (Teilstrukturen).

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

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

**Definition 5.1.19.** *Sei $(G, \circ, e)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt* ***Untergruppe****, falls $(H, \circ, e)$ eine Gruppe ist.*

Das ist das die typische Definition einer Teilstruktur. Es ist eine Teilmenge, die mit den „ererbten“ Operationen dieselbe Struktur aufweist wie ihre Obermenge.

Meist beweist man dann, welche Eigenschaften nachzurechnen sind, um sicher zu stellen, dass man tatsächlich eine Teilstruktur gefunden hat. Basiert die Strukturdefinition auf einer Verknüpfung $\circ$, so muss man stets überprüfen, dass die Verknüpfung auf der Teilmenge $H \subseteq G$ **abgeschlossen** ist, dass also

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

Die Verknüpfung in $G$ darf also nicht aus $H$ herausführen.

**Proposition 5.1.20.** *Eine Teilmenge $H \subseteq G$ einer Gruppe $G$ ist eine Untergruppe, wenn für alle $g, h \in H$ auch $g \circ h^{-1} \in H$ ist. Äquivalent dazu ist, dass für alle $g, h \in H$ die Verknüpfung $g \circ h \in H$ und zusätzlich zu jedem Element $h \in H$ auch das Inverse $h^{-1} \in H$ liegt.*

*Ist $G$ abelsch, dann auch $H$.*

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

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

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

Wenn $G$ abelsch ist, dann erfüllen alle Elemente in $G$ das Kommutativgesetz, also erst recht alle in $H$. □

**Beispiel 5.1.21.** *Jede Gruppe $G$ besitzt die beiden trivialen Untergruppen $\{e\}$ und $G$. Die Gruppe $(\mathbb{Z}, +, 0)$ besitzt etwa die Untergruppe $\mathbb{Z}_g$ aller geraden ganzen Zahlen.*

## 2. Ringe

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

**Definition 5.2.1.** *Eine Menge $H$, die eine Halbgruppe $(H, +)$ und eine Halbgruppe $(H, \cdot)$ bildet, heißt **Halbring**, falls die beiden Distributivgesetze von $+$ bezüglich $\cdot$*

**DG1:** $a(b + c) = ab + ac$
**DG2:** $(b + c)a = ba + ca$

*erfüllt sind.*

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

**Beispiel 5.2.2.** *Die natürlichen Zahlen $(\mathbb{N}, +, \cdot)$ bilden einen kommutativen Halbring. Manche nennen das sogar **Dioid**, da beide Halbgruppen $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ Monoide sind.*

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

**Definition 5.2.3.** *Ein Halbring $(R, +, \cdot)$ heißt **Ring**, falls zusätzlich*

**R1::** *$(R, +)$ eine abelsche Gruppe ist.*

*Ist $(R, \cdot)$ ein Monoid und gilt $0 \neq 1$, so sagen wir $R$ sei ein **Ring mit Einselement**. Ist die Operation $\cdot$ kommutativ, so liegt ein **kommutativer Ring (mit Einselement)** vor.*

**Beispiel 5.2.4.** *Die ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ sind ein kommutativer Ring mit Einselement.*

**Proposition 5.2.5.** *Ist $(R, +, \cdot)$ ein Ring, so gelten die Rechenregeln*

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

Beweis. (1) Es gilt $r0 = r(0 + 0) = r0 + r0$ und damit $r0 = 0$.
(2) Wir haben $(-r)s + rs = ((-r) + r)s = 0s = 0$ wegen (1). Aus der Eindeutigkeit des Inversen folgt $-(rs) = (-r)s$. Analog finden wir $r(-s) + rs = r((-s) + s) = r0 = 0$ und damit $-(rs) = r(-s)$.
(3) Aus (2) folgt $rs = -(-(rs)) = -((-r)s) = (-r)(-s)$ wegen Proposition 5.1.17.
(4) Es gilt $0 = 0r = (1 + (-1))r = 1r + (-1)r = r + (-1)r$ und damit $-r = (-1)r$ wegen der Eindeutigkeit der Inversen. Die zweite Gleichung zeigt man analog.

□

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

**Definition 5.2.6.** *Eine Teilmenge $S \subseteq R$ eines Ringes $(R, +, \cdot)$ heißt Teilring (Unterring) von $R$, falls $(S, +, \cdot)$ ein Ring ist.*

**Proposition 5.2.7.** *Eine Teilmenge $S$ eines Ringes $R$ ist ein Unterring genau dann, wenn für alle $r, s \in R$ die Elemente $r - s$ und $rs$ in $S$ liegen.*

*Ist $R$ kommutativ, dann auch $S$.*

Beweis. Weil für $r, s \in S$ schon $r - s \in S$ folgt, wissen wir aus Proposition 5.1.20, dass $(S, +)$ eine abelsche Gruppe ist (eine Untergruppe von $(R, +)$). Die Verknüpfung $\cdot$ ist in $H$ abgeschlossen, denn das haben wir vorausgesetzt. Weil aber die Distributivgesetze für alle Elemente in $R$ gelten, stimmen sie erst recht für alle Elemente von $S$. Daher ist $S$ ein Ring.

Die Aussage über Kommutativität ist offensichtlich. □

**Definition 5.2.8.** *Ein kommutativer Ring mit Einselement $(R, +, \cdot, 0, 1)$ heißt **Integritätsbereich**, wenn für je zwei Elemente $r, s \in R$ aus $rs = 0$ schon $r = 0$ oder $s = 0$ folgt.*

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

**Beispiel 5.2.9.** *Die ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ sind ein Integritätsbereich.*

## 3. Körper

Die speziellste Struktur der Algebra für Mengen mit zwei Verknüpfungen spielt in der Mathematik eine heraus ragende Rolle.

**Definition 5.3.1.** *Ein Ring mit Einselement $(K, +, \cdot)$ heißt **Körper**, wenn zusätzlich*

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

*erfüllt ist.*

**Beispiel 5.3.2.** *Die rationalen Zahlen $(\mathbb{Q}, +, \cdot, 0, 1)$ bilden ebenso einen Körper wie die reellen oder komplexen Zahlen.*

*Die schon aus Beispiel 4.3.32 bekannten Restklassen $\mathbb{Z}_p$ bilden einen kommutativen Ring mit Einselement mit den Verknüpfungen*

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

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

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

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

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

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

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

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

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

**Bemerkung 5.3.3.** *Nachdem Körper so wichtig sind, fassen wir noch einmal **alle** Eigenschaften zusammen, die die Verknüpfungen $+$ und $\cdot$ auf einer Menge $K$ haben müssen, damit $K$ ein Körper ist. Diese Eigenschaften nennt man auch die **Körperaxiome***

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

**Proposition 5.3.4.** *Ist $(K, +, \cdot)$ ein Körper, so gelten die Rechenregeln*

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

Beweis. (1) Wir haben $(ab)(a^{-1}b^{-1}) = aa^{-1}bb^{-1} = 1 \cdot 1 = 1$. Der Rest folgt wieder aus der Eindeutigkeit der Inversen.
(2) Es gilt $-a = (-1)a$ wegen Proposition 5.2.5.(4). Offensichtlich ist $(-1)^{-1} = -1$, wegen $1 = 1 \cdot 1 = (-1)(-1)$, was aus Proposition 5.2.5.(3) folgt. Wir erhalten unter Verwendung von (1) $(-a)^{-1} = ((-1)a)^{-1} = (-1)^{-1}a^{-1} = (-1)a^{-1} = -a^{-1}$.

□

Analog zu Ringen kann man auch wieder Unterkörper definieren:

**Definition 5.3.5.** *Eine Teilmenge $Q \subseteq K$ eines Körpers $(K, +, \cdot)$ heißt **Unterkörper**, wenn $(Q, +, \cdot)$ selbst ein Körper ist.*

**Beispiel 5.3.6.** *Die rationalen Zahlen $\mathbb{Q}$ sind ein Unterkörper der reellen Zahlen $\mathbb{R}$. Diese sind wiederum ein Unterkörper der komplexen Zahlen $\mathbb{C}$.*

**Proposition 5.3.7.** *Eine Teilmenge $Q$ eines Körpers $(K, +, \cdot)$ ist genau dann ein Unterkörper, wenn für je zwei Elemente $a, b \in Q$ sowohl $a - b \in Q$ als auch, sofern $b \neq 0$, $ab^{-1} \in Q$ sind.*

*Alternativ kann man für drei Elemente $a, b, c \in Q$ mit $c \neq 0$ auch $(a - b)c^{-1} \in Q$ überprüfen.*

Beweis. Dies folgt aus Proposition 5.1.20 für $(K, +)$ und $(K, \cdot)$. Ferner beachte man, dass $(a - 0)c^{-1} = ac^{-1}$ und $(a - b)1^{-1} = a - b$ gelten. □

**Proposition 5.3.8.** *Jeder Körper ist ein Integritätsbereich.*

Beweis. Einfach. □

KAPITEL 6

# Zahlenmengen

In diesem Abschnitt wollen wir auf mathematisch halbwegs exakte Weise die für die Mathematik grundlegenden Zahlenmengen einführen.

## 1. Die natürlichen Zahlen $\mathbb{N}$

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

Demnach ist

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

Definiert sind für $\mathbb{N}$ die Addition $+$, die Multiplikation $\cdot$, mit denen $\mathbb{N}$ einen kommutativen Halbring mit 0 und 1 (ein Dioid) ohne Nullteiler bildet (siehe Kapitel 5). Ferner ist eine Totalordnung $\leq$ erklärt, die verträglich mit den Verknüpfungen ist:

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

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

Wir definieren

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

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

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

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

**Theorem 6.1.1.** *Sei die Nachfolgereigenschaft*

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

*definiert. Dann gilt*

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

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

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

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

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

**Korollar 6.1.2.** *Es gilt das Induktionsprinzip*

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

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

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

Die Peano Axiome sind

**PA1:** $0 \in \mathbb{N}$,
**PA2:** $\forall n \in \mathbb{N} : (S(n) \in \mathbb{N})$,
**PA3:** $\forall n \in \mathbb{N} : \neg(S(n) = 0)$,
**PA4:** $\forall n \in \mathbb{N} : \forall m \in \mathbb{N} : ((S(n) = S(m)) \Rightarrow n = m)$,
**PA5:** $\forall M \in \mathbb{P}\mathbb{N} : (\psi(M) \Rightarrow M = \mathbb{N})$.

**Proposition 6.1.3.** *Die Menge der natürlichen Zahlen $\mathbb{N}$ erfüllt die Peano Axiome.*

Beweis. Die Axiome PA1 und PA2 gelten wegen der Definition von $\mathbb{N}$ und PF5 haben wir in Korollar 6.1.2 gezeigt. Es bleiben also nur noch PA3 und PA4.

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

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

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

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

**Proposition 6.1.4.** *Die Relation $\leq$ ist eine Totalordnung.*

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

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

Beweisen wir zwei Hilfsresultate zuerst:

HB1. $\forall m, n \in \mathbb{N} : (m \in n \Rightarrow S(m) \subseteq n)$.

Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : (m \in n \Rightarrow S(m) \subseteq n)\}$. Die 0 erfüllt die Bedingung trivialerweise, daher ist $0 \in M$. Sei nun $n \in M$. Gilt $m \in S(n) = n \cup \{n\}$, so ist entweder $m = n$ oder $m \in n$. Ist $m = n$, so ist $S(m) = S(n)$ und daher gilt $S(m) \subseteq S(n)$. Ist hingegen $m \in n$, so gilt wegen $n \in M$ auch $S(m) \subseteq n \subseteq S(n)$, und somit gilt immer $S(m) \subseteq S(n)$. Daher ist auch $S(n) \in M$ und wegen Korollar 6.1.2 folgt $M = \mathbb{N}$. Dies beweist HB1.

HB2. $\forall m, n \in \mathbb{N} : ((m \subseteq n \wedge m \neq n) \Rightarrow m \in n)$.

Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : ((m \subseteq n \wedge m \neq n) \Rightarrow m \in n)\}$. Ist $m \subseteq 0$, so ist $m = 0$ und daher $0 \in M$. Sei nun $n \in M$. Wir betrachten $S(n)$, und daher sei $m \in \mathbb{N}$ mit $m \subseteq S(n) \wedge m \neq S(n)$. Ist $k \in m$, so gilt wegen $S(n) = n \cup \{n\}$, dass entweder $k \in n$ oder $k = n$. Ist $k = n$, so ist $n \in m$ und wegen HB1 folgt dann $S(n) \subseteq m$. Dies ist aber ein Widerspruch zu $m \subseteq S(n) \wedge m \neq S(n)$. Daher gilt $\forall k \in m : k \in n$, also $m \subseteq n$. Ist $m = n$, dann haben wir $m \in n \cup \{n\} = S(n)$. Sonst gilt $m \subseteq n \wedge m \neq n$, und weil $n \in M$ vorausgesetzt ist auch $m \in n$. Dies impliziert aber $m \in S(n)$, und $S(n) \in M$. Aus Korollar 6.1.2 folgt $M = \mathbb{N}$, was HB2 beweist.

Sei $M = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : (m < n \vee m = n \vee n < m)\}$. Betrachten wir zuerst 0. Ist $0 \neq n$, so gilt $0 = \emptyset \subseteq n$, also $0 \in n$ wegen HB2, und daher $0 \in M$. Sei nun $n \in M$. Betrachten wir $S(n)$. Sei $m \in \mathbb{N}$ gegeben. Gelten $m \in n$ oder $m = n$, so haben wir $m \in n \cup \{n\} = S(n)$. Gilt andererseits $n \in m$, so folgt aus HB1, dass $S(n) \subseteq m$. Ist $S(n) \neq m$, so ist $S(n) \in m$ wegen HB2. Es gilt also $m \in S(n) \vee m = S(n) \vee S(n) \in m$, und daher $S(n) \in M$. Verwenden wir ein weiteres Mal Korollar 6.1.2, so sehen wir $M = \mathbb{N}$ und wir sind fertig. □

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

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

und finden das folgende Resultat

**Proposition 6.1.5.** *Es gibt genau eine Abbildung $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, die obige rekursive Definition erfüllt.*

BEWEIS. Beginnen wir mit der Eindeutigkeit. Seien $+$ und $\boxplus$ zwei Funktionen, die die rekursive Definition erfüllen. Setzen wir $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : (m + n = m \boxplus n)\}$. Natürlich ist $0 \in M$ wegen $n + 0 = n = n \boxplus 0$. Sei nun $n \in N$, dann haben wir für $m \in \mathbb{N}$ die Gleichung $m + S(n) = S(m + n) = S(m \boxplus n)$ wegen $n \in N$ und $S(m \boxplus n) = m \boxplus S(n)$, und daher $S(n) \in M$. Aus Korollar 6.1.2 folgt $M = \mathbb{N}$, und daher ist $+ = \boxplus$ als Teilmenge von $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$. Wir dürfen noch nicht von Abbildung reden, da wir die Abbildungseigenschaft noch nicht nachgewiesen haben. Dies können wir mit einem ähnlichen Induktionsargument erreichen.

Sei für jedes $m \in \mathbb{N}$ die „Abbildung“ $+_m : \mathbb{N} \to \mathbb{N}$ definiert durch $+_0(n) = n$ und $+_{S(m)}(n) = S(+_m(n))$. Dies macht $+_m$ zu einer Relation, aber wir werden unten die Abbildungseigenschaft nachweisen:

Sei $M := \{m \in \mathbb{N} \mid \forall n \in \mathbb{N} : \forall j \leq m : \exists! k \in \mathbb{N} : (+_j(n) = k)\}$. Wegen $\forall n \in \mathbb{N} : (+_0(n) = n)$ folgt sofort $0 \in M$. Ist $m \in M$, dann ist $+_0(n) = n$ eindeutig. Sei also $j \leq m$. Dann

existiert für beliebiges $n \in \mathbb{N}$ genau ein $k$ mit $+_j(n) = k$. Also ist für $S(j)$ die Beziehung $+_{S(j)}(n) = S(+_j(n)) = S(k)$ erfüllt. Somit ist auch $S(m) \in M$, da für $j \in \mathbb{N}$ mit $j \leq S(m)$ entweder $j = 0$ ist oder ein $j' \in \mathbb{N}$ existiert mit $j = S(j')$ und $j' \leq m$. Somit impliziert Korollar 6.1.2 aber $M = \mathbb{N}$. Daher ist für jedes $m \in \mathbb{N}$ die Relation $+_m$ tatsächlich eine Abbildung, und $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ist dann als Abbildung definiert durch $n + m = +_m(n)$ für alle $m, n \in \mathbb{N}$. □

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

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

**Theorem 6.1.6.** *Die natürlichen Zahlen $(\mathbb{N}, +, \cdot)$ bilden einen kommutativen Halbring mit 0 und 1.*

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

**BH1:** $\forall n \in \mathbb{N} : S(m) + n = m + S(n)$.
Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : S(m) + n = m + S(n)\}$. Es gilt $S(0) + 0 = S(0)$ und $0 + S(0) = S(0 + 0) = S(0)$ und daher $0 \in M$. Sei nun $n \in M$. Wir betrachten $S(n)$ und erhalten für $m \in \mathbb{N}$ die Beziehung $S(m)+S(n) = S(S(m)+n) = S(m+S(n)) = m + S(S(n))$ nach Definition von $+$ und weil $n \in M$. Daher ist auch $S(n) \in M$ und Korollar 6.1.2 liefert uns $M = \mathbb{N}$.

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

**KG(+):** $\forall n, m \in \mathbb{N} : n + m = m + n$.
Diese Beziehung zeigen wir ebenfalls mit Induktion. Sei $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : m + n = n + m\}$. Wegen BH2 und der Definition von $+$ gilt für alle $n \in \mathbb{N}$ die Gleichung $0 + n = n + 0$ und daher $0 \in M$. Sei nun $n \in M$. Dann rechnen wir für beliebiges $m \in \mathbb{N}$ wie folgt: $S(n)+m = n+S(n) = S(n+m) = S(m+n) = m+S(n)$. Zweimal haben wir die Definition von $+$ verwendet und je einmal die Tatsache $n \in M$ und BH1. Daher ist $S(n) \in M$, und wegen Korollar 6.1.2 gilt $M = \mathbb{N}$. Daher ist $+$ kommutativ.

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

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

Das beweist $S(m) \in M$ und damit $M = \mathbb{N}$ wegen Korollar 6.1.2. Also ist $+$ assoziativ und $(\mathbb{N}, +)$ ein kommutatives Monoid.

**BH3:** $\forall n \in \mathbb{N} : 0 \cdot n = 0$.
Induktion mit $M = \{n \in \mathbb{N} \mid 0 \cdot n = 0\}$. $0 \in M$ wegen der Definition $0 \cdot 0 = 0$. Ist $n \in M$, so ist auch $S(n) \in M$ wegen $0 \cdot S(n) = (0 \cdot n) + 0 = 0 + 0 = 0$. Korollar 6.1.2 impliziert wieder $M = \mathbb{N}$.

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

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

Daher ist $S(n) \in M$ und $M = \mathbb{N}$ wegen Korollar 6.1.2.

**BH5:** $\forall n, m \in \mathbb{N} : S(n) \cdot m = n \cdot m + m$.
Dieser erste Schritt zur Kommutativität folgt aus Korollar 6.1.2 nach Definition von $M := \{m \in \mathbb{N} \mid \forall n \in \mathbb{N} : S(n) \cdot m = n \cdot m + m\}$. Es gilt nämlich wegen $S(n) \cdot 0 = 0 = (n \cdot 0) + 0$, dass $0 \in M$ ist. Gilt nun $m \in M$, dann haben wir für beliebiges $n \in \mathbb{N}$

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

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

**KG($\cdot$):** $\forall m, n \in \mathbb{N} : m \cdot n = n \cdot m$.
Diesmal setzen wir $M := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : m \cdot n = n \cdot m\}$. Es ist wegen der Definition von $\cdot$ und BH3 $0 \in M$. Ist $n \in M$, so auch $S(n)$ wegen $m \cdot S(n) = (m \cdot n) + m = (n \cdot m) + m = S(n) \cdot m$. Hier haben wir die Definition und BH5 verwendet. Es ist also $M = \mathbb{N}$ wegen Korollar 6.1.2.

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

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

Aus Korollar 6.1.2 erhalten wir $M = \mathbb{N}$.

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

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

Verwenden wir ein letztes Mal Korollar 6.1.2, so erhalten wir $M = \mathbb{N}$.

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

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

**Theorem 6.1.7.** *Die Ordnungsrelation $\leq$ und die arithmetischen Operationen $+$ und $\cdot$ sind verträglich.*

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

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

BEWEIS. Im gesamten Beweis definieren wir eine Menge $M$ und beweisen $0 \in M$ und die Implikation $n \in M \implies S(n) \in M$. Dann verwenden wir Korollar 6.1.2, um $M = \mathbb{N}$ zu schließen.

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

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

Daher ist $S(k) \in M$.
(2) Es gilt $k \leq \ell$ und daher ist $k+m \leq \ell+m$. Wegen $m \leq n$ gilt außerdem $\ell+m \leq \ell+n$. Aus der Transitivität von $\leq$ folgt schließlich $k + m \leq \ell + n$.
(3) Sei $M := \{n \in \mathbb{N} \mid \forall k, m \in \mathbb{N} : (n + k \leq n + m \Rightarrow k \leq m)\}$. Es gilt wieder trivialerweise $0 \in M$ und für $n \in M$ finden wir wegen

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

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

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

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

$$nS(k) \leq nm \Rightarrow nk + n \leq nm. \tag{6.4}$$

Nun unterscheiden wir zwei Fälle. Ist $m = 0$, so muss $nk+n = 0$ sein, da die einzige Zahl $z \in \mathbb{N}$ mit $z \leq 0$ die 0 ist. Das ist aber nur möglich, wenn $n = 0$ ist; dies ist aber nicht erlaubt. Also gilt $m \neq 0$ und damit existiert $m' \in \mathbb{N}$ mit $m = S(m')$. Wir folgern in Gleichung (6.4) weiter

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

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

□

**Theorem 6.1.8.** *Im Halbring $(\mathbb{N}, +, \cdot)$ gelten die folgenden Regeln:*
(1) *Aus $nm = 0$ folgt bereits $n = 0$ oder $m = 0$.*
(2) *Aus $n + m = n + k$ folgt $m = k$.*
(3) *Aus $nm = nk$ für $n \neq 0$ folgt $m = k$.*

BEWEIS. (1) Sei $n \neq 0$ und $m \neq 0$. Dann gibt es $m', n' \in \mathbb{N}$ mit $n = S(n')$ und $m = S(m')$ und wir erhalten $mn = S(m')S(n') = (m'S(n')) + S(n') = (m'n') + m' + S(n') = S((m'n') + m' + n') \neq 0$ wegen PA3.
(2) Sei $M := \{n \in \mathbb{N} \mid \forall m, k \in \mathbb{N} : (n + m = n + k \Rightarrow m = k)\}$. Dann ist $0 \in M$ weil aus $0 + m = 0 + k$ trivialerweise $m = k$ folgt. Sei nun $n \in M$. Dann gilt wegen Definitionen und PA4

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

Daher ist $S(n) \in M$ und $M = \mathbb{N}$ wegen Korollar 6.1.2.

(3) Aus $nm = nk$ können wir $nm \leq nk$ folgern, und daraus wegen Theorem 6.1.7 Punkt (5) auch $m \leq k$. Da wir analog auch $nk \leq nm$ und daraus $k \leq m$ schließen können, folgt der Rest aus der Antisymmetrie der Ordnungsrelation.

Damit hätten wir alle Behauptungen bewiesen. □

## 2. Die ganzen Zahlen $\mathbb{Z}$

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

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

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

Machen wir nun den nächsten Schritt und versuchen wir eine mathematische Definition der ganzen Zahlen.

Gehen wir dazu von $\mathbb{N}$ aus. Bilden wir $\mathbb{N} \times \mathbb{N}$ die Paare natürlicher Zahlen. Definieren wir eine Relation $\sim$ auf $\mathbb{N} \times \mathbb{N}$ durch

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

**Proposition 6.2.1.** *Die Relation $\sim$ ist eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$.*

Beweis. Die Reflexivität ist offensichtlich erfüllt, ebenso wie die Symmetrie. Kommen wir zur Transitivität. Seien $(m, n) \sim (m', n')$ und $(m', n') \sim (m'', n'')$. Dann gelten $m + n' = m'+n$ und $m'+n'' = m''+n'$. Daher wissen wir $m+n'+m'' = m'+n+m''$ und daraus wiederum folgt $m + m' + n'' = m' + n + m''$. Verwenden wir nun Eigenschaft 2 aus Theorem 6.1.8, so erhalten wir $m + n'' = m'' + n$ und $(m, n) \sim (m'', n'')$. □

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

**$+$:** Wir definieren

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

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

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

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

**$\cdot$:** Für die Multiplikation setzen wir

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

Auch das ist wohldefiniert, wie man leicht nachrechnet.

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

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

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

Die Transitivität erhält man so: $[(m_1, m_2)] \leq [(n_1, n_2)]$ impliziert $m_1 + n_2 \leq n_1 + m_2$, und aus $[(n_1, n_2)] \leq [(k_1, k_2)]$ folgt $n_1 + k_2 \leq k_1 + n_2$. Aus Theorem 6.1.7 erhalten wir

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

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

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

**Theorem 6.2.2.** *Die ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ sind ein Integritätsbereich.*

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

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

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

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

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

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

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

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

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

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

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

$$m_1 n_1 + m_2 n_2 = m_1 n_2 + m_2 n_1. \tag{6.5}$$

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

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

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

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

Dann gilt $0 \in M$, weil

$$mk + 0\ell = m\ell + 0k \Rightarrow mk = m\ell \Rightarrow k = \ell \quad \text{wegen } m \neq n = 0 \text{ und Theorem 6.1.8.}$$

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

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

Für $m = 0$ haben wir $0k+S(n)\ell = 0\ell+S(n)k$, woraus sofort $\ell = k$ folgt wegen Theorem 6.1.8 (3). Sei also nun $m \neq 0$ und $m \neq S(n)$. Dann existiert $m' \in \mathbb{N}$ mit $S(m') = m$, und wir können unter Verwendung von Theorem 6.1.8 rechnen

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

Falls $n \neq m'$ gilt, dann können wir aus $n \in M$ schon $\ell = k$ folgern. Das ist aber der Fall, weil $S(m') = m \neq S(n)$ vorausgesetzt war. Daher ist auch $S(n) \in M$ und aus Korollar 6.1.2 folgt $M = \mathbb{N}$ und die Hilfsbehauptung.

Kehren wir zurück zu unserer Beziehung (6.5). Aus der Hilfsbehauptung erhalten wir für $m_1 \neq m_2$ die Folgerung $n_1 = n_2$, also $[(n_1, n_2)] = [(0, 0)]$. Gilt andererseits $m_1 = m_2$, so bedeutet das $[(m_1, m_2)] = [(0, 0)]$ und wir schließen die Nichtexistenz von Nullteilern. □

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

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

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

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

**Theorem 6.2.3.** *Für die Ordnungsrelation von $\mathbb{Z}$ finden wir die folgenden Eigenschaften.*

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

Beweis. (1) Sind die Vorzeichen von $m$ und $n$ verschieden, so wissen wir $m \leq 0 \leq n$ und daher $-m \geq 0 \geq -n$. Sind $m$ und $n$ positiv, so sind $-m = [(0, m)]$ und $-n = [(0, n)]$. Wegen $m \leq n$ gilt nach definition von $\leq$ auf $\mathbb{Z}$ die Beziehung $-m \geq -n$. Haben wir umgekehrt $m \leq n \leq 0$, so impliziert das analog zu oben $-m \geq -n$.

(2) Sind $m = [(m_1, m_2)]$, $n = [(n_1, n_2)]$ und $k = [(k_1, k_2)]$, so erhalten wir wegen Theorem 6.1.7

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

(3) Dies folgt aus Theorem 6.1.7.(4) und der Nullteilerfreiheit.
(4) Ist $m \geq 0$, so folgt aus Theorem 6.1.7.(4) sofort $km \geq 0 = k0$. Gilt nun $m \leq n$, so folgt aus (2) $0 \leq n - m$ und aus dem schon bewiesenen $0 \leq k(n - m) = kn - km$ und wir erhalten wieder aus (2) die gesuchte Ungleichung $km \leq kn$.
(5) Für $k \leq 0$ ist $-k \geq 0$ und alles weitere folgt aus (5).
(6) Gilt $km \leq kn$, so erhalten wir aus (2) die Beziehung $0 \leq k(n - m)$. Weil $k > 0$ gilt, können wir aus Theorem 6.1.7.(5) $0 \leq n - m$ und damit wegen (2) $m \leq n$ schließen. □

**Proposition 6.2.4.** *Ist $k \neq 0$, so folgt aus $km = kn$ schon $m = n$ für beliebige $m, n \in \mathbb{Z}$.*

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

## 3. Die rationalen Zahlen $\mathbb{Q}$

Die rationalen Zahlen sind die nächste aus der Schule bekannte Zahlenmenge. Ebenso wie man die ganzen Zahlen konstruiert, um die Subtraktion für alle Zahlen durchführen zu können, muss man für die Umkehrung der Multiplikation wieder die Zahlenmenge erweitern.

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

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

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

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

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

**Definition 6.3.1.** *Ein Körper $(K, +, \cdot)$, der auch eine geordnete Menge $(K, \leq)$ ist, heißt **geordneter Körper**, falls die Eigenschaften*

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

**Proposition 6.3.2.** *In einem geordneten Körper $(K, +, \cdot, \leq)$ gelten folgende Aussagen.*

(1) *Ist $x \geq 0$ dann gilt $-x \leq 0$.*
(2) *Ist $x \geq 0$ und $y \leq z$, dann folgt $xy \leq xz$.*

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

BEWEIS. (1) $x \leq 0 \implies (-x) + x \leq 0 + (-x) \implies 0 \leq -x$.
(2) Für $y = z$ wissen wir $xy = xz$. Ist $y < z$, so ist $0 < z - y$. Für $x = 0$ gilt wieder $0 = xy = xz = 0$. Ist schließlich $x > 0$, dann folgt aus Definition 6.3.1 $0 < x(z - y) = xz - xy$ und somit ist $xy < xz$.
(3) Dies folgt aus (1) und (2).
(4) Ist $x > 0$, so gilt $x^2 = x \cdot x > 0$ wegen der Definition. Für $x < 0$ ist $-x > 0$ und $x^2 = (-x)(-x) > 0$. Es ist $1 \neq 0$ und $1^2 = 1$.
(5) Ist $x > 0$, so ist $x^{-1} > 0$. Wäre das nicht so, hätten wir $1 = xx^{-1} < 0$ im Widerspruch zu (4). Gilt $0 < x < y$, so wissen wir $x^{-1}y^{-1} > 0$, und daher folgt

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

□

Wenn wir die ganzen Zahlen konstruiert haben, steht uns nichts im Wege, dieselbe Konstruktion so ähnlich noch einmal durchzuführen. Im folgenden bezeichne $\mathbb{Z}_+ := \{n \in \mathbb{Z} \mid n > 0\}$ die Menge der positiven Elemente in $\mathbb{Z}$.
Betrachten wir auf der Menge $\mathbb{Z} \times \mathbb{Z}_+$ die Relation

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

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

**Proposition 6.3.3.** *Es gilt wieder $\sim$ ist eine Äquivalenzrelation auf $\mathbb{Z} \times \mathbb{Z}_+$.*

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

□

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

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

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

**Theorem 6.3.4.** *Die Menge der rationalen Zahlen $(\mathbb{Q}, +, \cdot)$ ist ein Körper mit Nullelement $[(0, 1)]$ und Einselement $[(1, 1)]$. Die Menge aller Elemente der Form $[(n, 1)]$ für $n \in \mathbb{Z}$ entspricht $\mathbb{Z}$ mit allen seinen Eigenschaften (aka ist **isomorph zu** $\mathbb{Z}$).*

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

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

Die Wohldefiniertheit im zweiten Term zeigt man analog.

Nun rechnen wir die Gruppenaxiome für $+$ nach

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

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

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

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

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

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

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

Die Wohldefiniertheit im zweiten Faktor zeigt man analog.

Die Gruppenaxiome für $\cdot$ kommen nun.

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

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

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

Das Distributivgesetz sieht man so ein.

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

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

Daher ist $\mathbb{Q}$ ein Körper. □

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

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

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

$$\begin{aligned} m_1 n_2 &\leq n_1 m_2 \\ m_1 m_2' n_2 &\leq n_1 m_2 m_2' \\ m_1' m_2 n_2 &\leq n_1 m_2 m_2' \\ m_1' n_2 &\leq n_1 m_2' \quad \text{wegen } m_2 > 0 \text{ und Theorem 6.2.3.} \end{aligned}$$

Analog zeigen wir die Wohldefiniertheit auf der rechten Seite.

**Theorem 6.3.5.** *Die Relation $\leq$ macht $\mathbb{Q}$ zu einem geordneten Körper.*

Beweis. Wir müssen die Bedingungen O1 und O2 nachweisen:

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

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

**O2:** Sei $q = [(q_1, q_2)] > 0$, dann folgt $q_1 > 0$. Für $r = [(r_1, r_2)]$ gilt analog $r_1 > 0$. Daher ist $qr = [(q_1 r_1, q_2 r_2)] > 0$, weil $q_1 r_1 > 0$ gilt wegen Theorem 6.2.3.

□

Wenn wir zu guter Letzt die Schreibweise

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

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

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

## 4. Die reellen Zahlen $\mathbb{R}$

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

Wir fügen zu $\mathbb{Q}$ die irrationalen Zahlen hinzu und erhalten den geordneten Körper $(\mathbb{R}, +, \cdot, \leq)$, den wir auch als **Zahlengerade** repräsentieren. Die rationalen Zahlen sind ein geordneter Unterkörper von $\mathbb{R}$.

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

**Definition 6.4.1.** *Eine geordnete Menge $M$ hat die **Supremums–Eigenschaft**, wenn zu jeder nicht leeren nach oben beschränkten Teilmenge $E \subseteq M$ das Supremum $\sup E \in M$ existiert.*

**Beispiel 6.4.2.** *Die Menge der rationalen Zahlen besitzt* nicht *die Supremums–Eigenschaft.*

**Theorem 6.4.3.** *Es existiert ein geordneter Körper $\mathbb{R}$, der die Supremumseigenschaft besitzt. Ferner ist $\mathbb{Q}$ ein Teilkörper von $\mathbb{R}$.*

Beweis. In Abschnitt 4.1. □

**Proposition 6.4.4.** *Zu zwei reellen Zahlen $x, y \in \mathbb{R}$ mit $x > 0$ existiert eine natürliche Zahl $n$ so, dass*

$$nx > y$$

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

*Zwischen zwei reellen Zahlen $x, y \in \mathbb{R}$ mit $x < y$ gibt es eine rationale Zahl $q \in \mathbb{Q}$:*

$$x < q < y.$$

*Man sagt auch $\mathbb{Q}$* ***liegt dicht in*** *$\mathbb{R}$.*

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

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

$$-m_2 < nx < m_1,$$

was die Existenz einer ganzen Zahl $m$ impliziert mit

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

Die Kombination aller dieser Ungleichungen liefert

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

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

**4.1. Die mengentheoretische Konstruktion von $\mathbb{R}$.** Wir werden $\mathbb{R}$ aus $\mathbb{Q}$ durch mengentheoretische Mechanismen konstruieren. Dazu werden wir die von Dedekind erfundenen Schnitte verwenden. Es gibt viele äquivalente Verfahren zur Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$. Die Dedekindschen Schnitte sind nicht die einleuchtendste Methode aber diejenige, die nur die Mengenoperationen verwendet.

## 5. Die komplexen Zahlen $\mathbb{C}$

KAPITEL 7

# Analytische Geometrie

In diesem Kapitel wollen wir das Rechnen mit Vektoren und die analytische Behandlung geometrischer Probleme, wie schon aus der Schule bekannt, ein wenig beleuchten.

## 1. Vektoren in $\mathbb{R}^2$, $\mathbb{R}^3$ und $\mathbb{R}^n$

Wollen wir geometrische Probleme durch analytische Untersuchungen lösen, dann müssen wir einen mathematischen Zugang zu den geometrischen Objekten (in der Ebene und im Raum) finden. Dazu wählen wir uns einen **Ursprung**, ein **cartesisches Koordinatenkreuz** ($x_1$–Achse, $x_2$–Achse und eventuell $x_3$–Achse). Dann können wir jedem Punkt seine **Koordinaten** zuordnen.

Befinden wir uns im Eindimensionalen (auf einer Gerade), dann können wir jedem Punkt auf dieser Geraden *eine* Koordinate $x_1$ zuordnen.

In der Ebene benötigen wir *zwei* Koordinaten, um einen Punkt eindeutig zu beschreiben. Wir fassen die beiden Koordinaten zu einem Paar $(x_1, x_2)$ zusammen. Nachdem die Punkte $(x_1, x_2)$ und $(x_2, x_1)$ im allgemeinen verschieden sind, sehen wir, dass es auf die Reihenfolge der Koordinaten ankommt. Wir müssen also die Koordinaten von Punkten in der Ebene in *geordneten Paaren* zusammenfassen. Es ist also $(x_1, x_2) \in \mathbb{R}^2$.

Wenn wir für Probleme im Raum analog vorgehen, finden wir heraus, dass wir *drei* Koordinaten benötigen, wir also Punkte mit Elementen $(x_1, x_2, x_3) \in \mathbb{R}^3$ beschreiben.

Im besten mathematischen Sinn definieren wir jetzt, statt getrennt für 1, 2 und 3 die geometrischen Untersuchungen durchzuführen, allgemein für beliebiges $n$. Wir werden erst später als Spezialfälle für $n = 2$ und $n = 3$ gesonderte Untersuchungen anstellen.

**Definition 7.1.1.** *Ein Element des $\mathbb{R}^n$ nennen wir **Punkt des $n$–dimensionalen Raumes** $\mathbb{R}^n$. Ist $u = (u_1, \ldots, u_n) \in \mathbb{R}^n$, dann heißen die Zahlen $u_i$ $(i = 1, \ldots, n)$ die **Komponenten des Punktes** $u$.*

*Wie aus der Definition des $\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}}_{n}$ als cartesisches Produkt folgt, gelten zwei Punkte $u = (u_1, \ldots, u_n)$ und $v = (v_1, \ldots, v_n)$ als gleich, wenn für alle $i = 1, \ldots, n$ die Komponenten übereinstimmen: $u_i = v_i$.*

Meist schreiben Mathematiker die Vektoren als Kleinbuchstaben ohne Indices und verwenden dann denselben Buchstaben mit Index, um die Komponenten des Vektors zu bezeichnen.

Als Beispiel verwenden wir etwa $u = (1, 3, 5) \in \mathbb{R}^3$ und $u_2 = 3$. Allgemein werden wir Vektoren mit Kleinbuchstaben bezeichnen und Indices zu diesem Buchstaben hinzufügen, wenn wir über Komponenten des Vektors sprechen wollen.

Mit Punkten des $\mathbb{R}^n$ kann man rechnen. Man kann sie addieren und mit reellen Zahlen multiplizieren.

**Definition 7.1.2.** *Sind $u$ und $v$ zwei Punkte des $\mathbb{R}^n$, dann definieren wir ihre **Summe** $u + v$ durch*

$$u + v := (u_1 + v_1, \ldots, u_n + v_n).$$

*Ist $u \in \mathbb{R}^n$ ein Punkt und $\lambda \in \mathbb{R}$ eine reelle Zahl, so definieren wir das* ***Produkt*** *von $\lambda$ und $u$ durch*

$$\lambda u := (\lambda u_1, \ldots, \lambda u_n).$$

**Beispiel 7.1.3.** *Betrachten wir die Punkte $u = (1, 1, 5, 3)$ und $v = (0, 4, -2, 4)$ des $\mathbb{R}^4$. Ihre Summe ist $u + v = (1, 5, 3, 7)$. Das Produkt von 4 mit $u$ ist $4u = (4, 4, 20, 12)$.*

Die Definition der Rechenvorschriften $+$ und $\cdot$ ist **komponentenweise** erfolgt. Darum können wir einfach die Rechenregeln von $\mathbb{R}$ (die Körperaxiome!) heranziehen und sofort einige Regeln für die Addition von Punkten und die Multiplikation mit reellen Zahlen herleiten.

**Theorem 7.1.4.** *Die Punkte des $\mathbb{R}^n$ erfüllen bezüglich Addition und Multiplikation mit reellen Zahlen folgende Rechenregeln:*

- **VR1:** *(Assoziativgesetz (+)) $\forall u, v, w \in \mathbb{R}^n : (u + v) + w = u + (v + w)$,*
- **VR2:** *(Nullelement) Es gibt $\mathfrak{o} = (0, \ldots, 0)$ in $\mathbb{R}^n$ mit $\forall u \in \mathbb{R}^n : \mathfrak{o} + u = u + \mathfrak{o} = u$.*
- **VR3:** *(Inverse bzgl. +) Für alle $u \in \mathbb{R}^n$ gibt es ein $-u \in \mathbb{R}^n$ mit $u+(-u) = (-u)+u = \mathfrak{o}$. Es gilt $-u = (-u_1, \ldots, -u_n)$.*
- **VR4:** *(Kommutativgesetz (+)) $\forall u, v \in \mathbb{R}^n : u + v = v + u$.*

*Diese Regeln machen $(\mathbb{R}^n, +)$ zu einer* abelschen Gruppe.

- **VR5:** *(Distributivgesetz 1) $\forall \lambda \in \mathbb{R} : \forall u, v \in \mathbb{R}^n : \lambda(u + v) = \lambda u + \lambda v$,*
- **VR6:** *(Distributivgesetz 2) $\forall \lambda, \mu \in \mathbb{R} : \forall u \in \mathbb{R}^n : (\lambda + \mu)u = \lambda u + \mu u$,*
- **VR7:** *(Umklammern) $\forall \lambda, \mu \in \mathbb{R} : \forall u \in \mathbb{R}^n : (\lambda\mu)u = \lambda(\mu u)$,*
- **VR8:** *(Eins) $\forall u \in \mathbb{R}^n : 1u = u$.*

Beweis. □

Wie üblich schreiben wir $u - v := u + (-v)$ und $\frac{w}{\lambda} = w/\lambda := \frac{1}{\lambda}w$.

**Bemerkung 7.1.5.** *Erfüllt eine Menge $V$, auf der eine Verknüpfung $+$ definiert ist und für die zu einem Körper $\mathbb{K}$ eine Multiplikation $\cdot : \mathbb{K} \times V \to V$ erklärt ist, die Eigenschaften VR1 bis VR8, so nennt man $V$ einen* ***Vektorraum****.*

**1.1. Vektoren.** Was sind jetzt eigentlich *Vektoren* und was ist der Zusammenhang zwischen Punkten in $\mathbb{R}^n$ und Vektoren?

**Definition 7.1.6.** *Unter einem* ***Pfeil*** *$\overrightarrow{uv}$ im $\mathbb{R}^n$ versteht man die* ***gerichtete Strecke mit Anfangspunkt*** *$u \in \mathbb{R}^n$* ***und Endpunkt*** *$v \in \mathbb{R}^n$. Der Pfeil $\overrightarrow{vu}$ ist nicht dasselbe wie der Pfeil $\overrightarrow{uv}$ sondern er hat die* ***entgegen gesetzte Richtung****.*

*Man nennt die Pfeile $\overrightarrow{\mathfrak{o}v}$ für $v \in \mathbb{R}$ die* ***Ortsvektoren*** *des $\mathbb{R}^n$.*

Die Ortsvektoren des $\mathbb{R}^n$ sind eindeutig durch ihren Endpunkt festgelegt. Man kann also jeden Punkt $u$ des $\mathbb{R}^n$ als Ortsvektor $\overrightarrow{\mathfrak{o}u}$ auffassen und umgekehrt. Man kann also $\mathbb{R}^n$ mit den Ortsvektoren **identifizieren**.

Um mit den übrigen Pfeilen zu Rande zu kommen, definieren wir eine Relation $\sim$ auf der Menge $V(\mathbb{R}^n)$ aller Pfeile. Es sei für $u, v, w, z \in \mathbb{R}^n$

$$\overrightarrow{uv} \sim \overrightarrow{wz} : \Longleftrightarrow \; v - u = z - w.$$

Es ist ganz leicht zu zeigen, dass $\sim$ eine Äquivalenzrelation auf der Menge aller Pfeile in $\mathbb{R}^n$ ist. Die Menge $V(\mathbb{R}^n)$ wird also in Äquivalenzklassen partitioniert, und in jeder dieser Äquivalenzklassen liegt genau ein Ortsvektor $(\overrightarrow{uv} \sim \overrightarrow{\mathfrak{o}(v-u)})$.

Geometrisch bedeutet Äquivalenz zweier Pfeile bezüglich $\sim$, dass sie gleiche Richtung und Länge haben. Im folgenden bezeichnen wir eine Äquivalenzklasse solcher gerichteter Strecken (Pfeile) als **Vektor**. Wir unterscheiden Vektoren also nur mehr nach Richtung und Länge, nicht mehr jedoch nach ihrem Anfangspunkt.

Weil aber in jeder Äquivalenzklasse genau ein Ortsvektor liegt und jeder Ortsvektoren mit einem Punkt in $\mathbb{R}^n$ identifiziert werden kann, kann auch jeder Vektor mit einem Punkt des $\mathbb{R}^n$ identifiziert werden (mit dem Endpunkt des in der Klasse liegenden Ortsvektors). Speziell können wir jeden Vektor $v$ in Komponenten $(v_1, \ldots, v_n)$ aufschreiben.

**Definition 7.1.7.** *Zwei Vektoren $u, v \in \mathbb{R}^n$ heißen **parallel**, falls es eine reelle Zahl $\lambda \neq 0$ gibt mit $u = \lambda v$. Sie heißen **gleich orientiert (haben die gleiche Richtung)**, falls $\lambda > 0$ ist. Ist $\lambda < 0$, so heißen sie **entgegen gesetzt orientiert (haben entgegen gesetzte Richtungen)**.*

Im $\mathbb{R}^2$ und $\mathbb{R}^3$ kann man sich die Summe von Vektoren und deren Multiplikation mit Zahlen einfach geometrisch vorstellen. In Abbildung 7.1 wird die Konstruktion dargestellt.

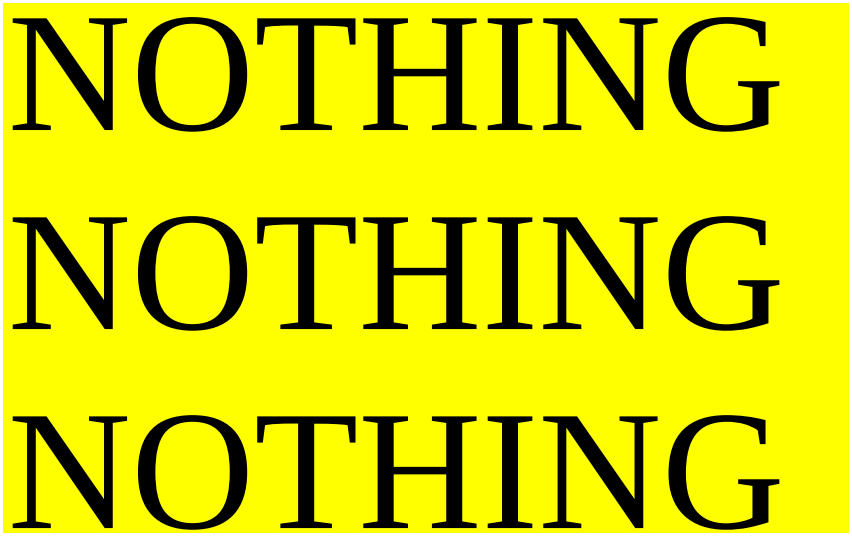



ABBILDUNG 7.1. Vektoroperationen geometrisch gedeutet

**1.2. Inneres Produkt, Norm, Distanz.** Möchte man Geometrie mit Hilfe von Vektoren betreiben, so muss man die geometrischen Grundgrößen (Länge, Abstand, Winkel) mit Hilfe von Vektoren bestimmen können.

Das grundlegende Konzept in diesem Zusammenhang ist das **innere Produkt** oder **Skalarprodukt** zweier Vektoren.

**Definition 7.1.8.** *Unter dem inneren Produkt (Skalarprodukt) zweier Vektoren $u, v \in \mathbb{R}^n$ versteht man die* reelle Zahl

$$\langle u, v\rangle := u_1v_1 + \cdots + u_nv_n.$$

**Beispiel 7.1.9.** *Das innere Produkt der beiden Vektoren $u = (0, 2, 3, 1, -1)$ und $v = (2, 2, 0, -3, 1)$ ist $\langle u, v\rangle = 0 + 4 + 0 - 3 - 1 = 0$.*

Aus der Definition und den Rechengesetzen für reelle Zahlen kann man einfach die folgenden Eigenschaften des inneren Produktes ableiten:

**Theorem 7.1.10.** *Das innere Produkt von Vektoren $u, v \in \mathbb{R}^n$ erfüllt $\forall u, v, w \in \mathbb{R}^n$ und $\forall \lambda \in \mathbb{R}$*

**IP1:** $\langle u, v\rangle = \langle v, u\rangle$,
**IP2:** $\langle u, v + w\rangle = \langle u, v\rangle + \langle u, v\rangle$,
**IP3:** $\langle cu, v\rangle = c\langle u, v\rangle$,
**IP4:** $\langle \mathfrak{o}, \mathfrak{o}\rangle = 0$ *und für $u \neq \mathfrak{o}$ ist* $\langle u, u\rangle > 0$.

BEWEIS. (1), (2) und (3) sind sehr einfach.
(4) Die Beziehung $\langle \mathfrak{o}, \mathfrak{o} \rangle = 0$ ist ebenfalls offensichtlich. Sei daher $u \neq \mathfrak{o}$. Dann gibt es wenigstens ein $u_i \neq 0$, und daher $u_i^2 > 0$. Somit gilt

$$\langle u, u \rangle = \underbrace{u_1^2}_{\geq 0} + \cdots + \underbrace{u_i^2}_{>0} + \cdots + \underbrace{u_n^2}_{\geq 0} > 0.$$

□

Für $\langle u, u \rangle$ schreiben wir in Zukunft $u^2$, und es gelten die Beziehungen $(u+v)^2 = u^2 + 2\langle u, v \rangle + v^2$.

Aus dem zentralen Begriff des Skalarproduktes können wir nun die gesamten Größen der Geometrie errechnen.

**Definition 7.1.11.** *Unter der* ***(euklidischen) Norm*** *des Vektors $u \in \mathbb{R}^n$ verstehen wir die reelle Zahl*

$$\|u\| := \sqrt{\langle u, u \rangle}.$$

*Sie beschreibt die* Länge des Vektors *$u$.*

*Ein Vektor $v \in \mathbb{R}^n$ mit $\|v\| = 1$ heißt* ***Einheitsvektor****.*

*Haben wir zwei Punkte $u, v$ des $\mathbb{R}^n$ gegeben, so ist $v - u$ ihr Verbindungsvektor. Weil Vektoren aber gerichtete Strecken sind, und die Norm die Streckenlänge ist, kann man den* ***Abstand*** *(die* ***Distanz****) von $u$ und $v$ aus der Länge von $v - u$ berechen*

$$d(u, v) := \|v - u\|.$$

**Beispiel 7.1.12.** *Die Länge des Vektors $u = (1, 1, 4)$ ist $\|u\| = 3\sqrt{2}$.*

Aus den Rechenregeln für das Skalarprodukt leiten sich sofort Eigenschaften der Norm und damit der Distanz ab. Es gelten

**Proposition 7.1.13.** *Die Norm und die Distanz haben folgende Eigenschaften.*

**N1:** $\forall \lambda \in \mathbb{R} : \forall u \in \mathbb{R}^n : \|\lambda u\| = |\lambda| \|u\|$,
**N2:** $\forall v \in \mathbb{R} : (v \neq \mathfrak{o} \Rightarrow \|v\| > 0)$ *und* $\|\mathfrak{o}\| = 0$,
**N3:** *Die Dreiecksungleichung der Norm*

$$\forall u, v \in \mathbb{R}^n : \quad \|u + v\| \leq \|u\| + \|v\|,$$

**CS:** *Die Cauchy–Schwarzsche Ungleichung*

$$\forall u, v \in \mathbb{R}^n : \quad |\langle u, v \rangle| \leq \|u\| \, \|v\|,$$

**D1:** *Symmetrie:* $\forall u, v \in \mathbb{R}^n : d(u, v) = d(v, u)$,
**D2:** $\forall u, v \in \mathbb{R}^n : d(u, v) \geq 0$ *und* $d(u, v) = 0$ *genau dann, wenn* $u = v$,
**D3:** *Die Dreiecksungleichung der Distanz*

$$\forall u, v, w \in \mathbb{R}^n : \quad d(u, w) \leq d(u, v) + d(v, w).$$

BEWEIS. Alle diese Rechenregeln werden in der Vorlesung Lineare Algebra 1 bewiesen. □

**Bemerkung 7.1.14.** *Die Dreiecksungleichung heißt so, weil die Seiten (für die Norm) bzw. die Eckpunkte (für die Distanz) jedes Dreiecks diese Ungleichungen erfüllen.*

*Jede Abbildung $\| \quad \| : \mathbb{R}^n \to \mathbb{R}$, die N1-N3 erfüllt, heißt* Norm *auf $R^n$. Jede Abbildung $d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, die D1-D3 erfüllt heißt* Distanz *oder* ***Metrik*** *auf $\mathbb{R}^n$.*

Aus den Rechenregeln folgt, dass man zu jedem Vektor $v \neq \mathfrak{o}$ einen parallelen Einheitsvektor finden kann durch $v_0 := v/\|v\|$.

**Beispiel 7.1.15.** *Sei $v = (1, 2, 2)$ ein Vektor. Die Norm von $v$ ist $\|v\| = 3$. Ein Einheitsvektor parallel zu $v$ ist $v_0 = (\frac{1}{3}, \frac{2}{3}, \frac{2}{3})$.*

Betrachten wir den Satz von Pythagoras und seine geometrische Interpretation in Abbildung 7.2, so erkennen wir unschwer, dass für zwei orthogonale Vektoren $u, v \in \mathbb{R}^n$ die Hypothenuse der Vektor $v - u$ ist. Wollen wir die übliche Geometrie analytisch beschreiben,

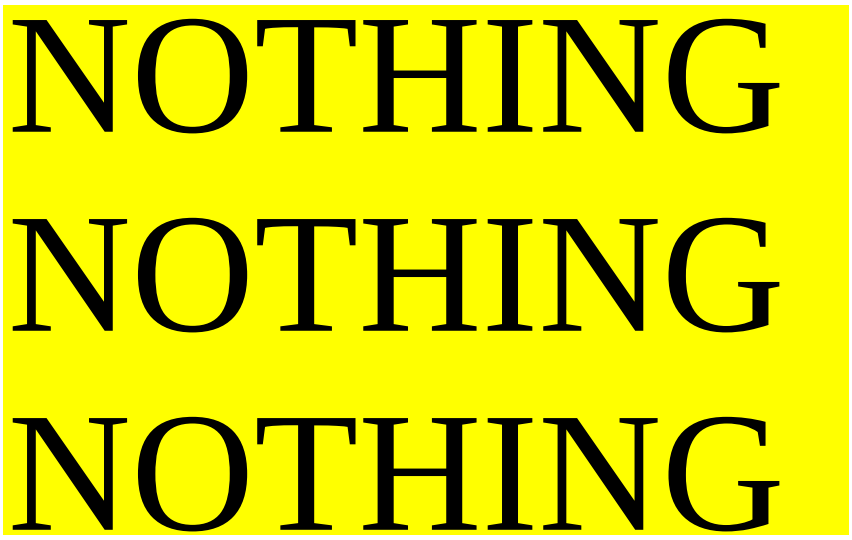



ABBILDUNG 7.2. Satz von Pythagoras

so muss der Satz von Pythagoras gelten, also

$$\begin{aligned} \|u\|^2 + \|v\|^2 &= \|v - u\|^2 \\ u^2 + v^2 &= (v-u)^2 = u^2 - 2\langle u, v\rangle + v^2 \\ 0 &= 2\langle u, v\rangle. \end{aligned}$$

Für zwei aufeinander senkrecht stehende Vektoren $u$ und $v$ muss also $\langle u, v\rangle = 0$ gelten. In der Mathematik drehen wir Definition und Herleitung um und führen ein:

**Definition 7.1.16.** *Zwei Vektoren $u, v \in \mathbb{R}^n$ heißen **orthogonal (stehen aufeinander senkrecht)**, wenn $\langle u, v\rangle = 0$ gilt.*

Eine weitere geometrische Anwendung des inneren Produktes finden wir in Abbildung 7.3. Die orthogonale Projektion eines Vektors $v$ auf einen Vektor $u$ sei jener zu $u$ parallele Vektor $x$, dessen Endpunkt durch rechtwinkelige Projektion des Endpunktes von $v$ auf die durch $u$ aufgespannte Gerade erhalten werde. Da $x$ parallel zu $u$ ist, muss $x = \lambda u$ für ein geeignetes $\lambda \in \mathbb{R}$ sein. Nachdem $v - x$ und $u$ orthogonal aufeinander stehen müssen, können wir $\lambda$ ausrechnen aus

$$0 = \langle v - x, u\rangle = \langle v - \lambda u, u\rangle = \langle v, u\rangle - \lambda\langle u, u\rangle.$$

Einfaches Umformen ergibt für $\lambda$ und für $x$ die Formeln

$$\lambda = \frac{\langle u, v\rangle}{\langle u, u\rangle}, \qquad x = \frac{\langle u, v\rangle}{\langle u, u\rangle} \cdot u.$$

Betrachten wir das so entstehende rechtwinkelige Dreieck genauer, so können wir aus elementar trigonometrischen Beziehungen den Winkel $\varphi$ zwischen $v$ und $u$ berechnen:

$$\cos\varphi = \frac{\lambda\|u\|}{\|v\|}.$$

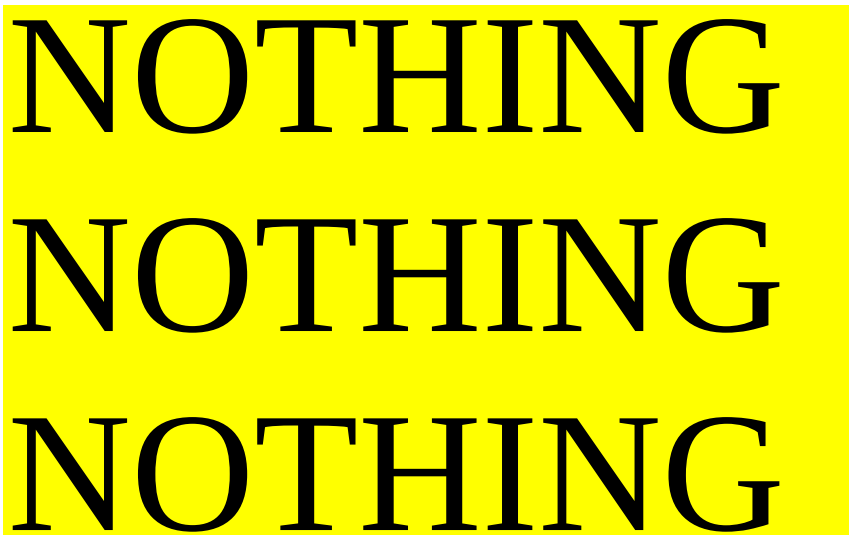



ABBILDUNG 7.3. Orthogonale Projektion eines Vektors auf einen anderen

Setzen wir in diese Beziehung das bereits berechnete $\lambda$ ein, so erhalten wir für den Winkel zwischen zwei Vektoren die Formeln

$$\cos\varphi = \frac{\langle u, v\rangle}{\|u\|\,\|v\|}, \qquad \langle u, v\rangle = \|u\|\,\|v\|\cos\varphi.$$

Jetzt haben wir alle geometrischen Grundgrößen bestimmt. Übrig bleibt nun noch, die geometrischen Objekte abgesehen von den Punkten im Koordinatensystem zu beschreiben.

**1.3. Normalvektor.**

**1.4. Geraden und Ebenen.**

**1.5. Flächen und Volumina.**

**2. Kegelschitte**

**3. Kugeln und mehr**

KAPITEL 8

# Grundlagen der Analysis

KAPITEL 9

# Trigonometrie

KAPITEL 10

# Differentialrechnung

KAPITEL 11

# Integralrechnung

KAPITEL 12

# Wahrscheinlichkeitstheorie

# Literaturverzeichnis


[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.

[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.