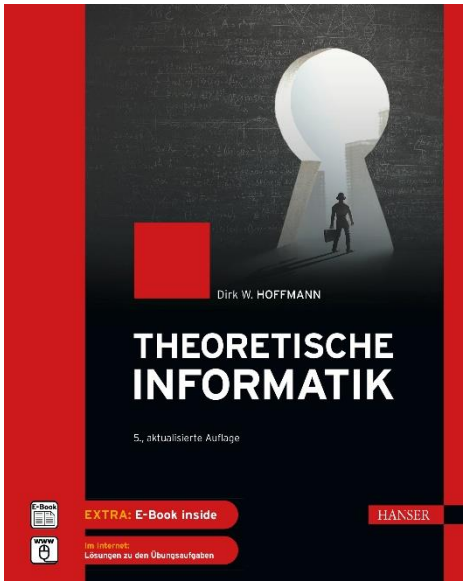
HANSER



Leseprobe

zu

Theoretische Informatik

von Dirk W. Hoffmann

Print-ISBN 978-3-446-47029-3
E-Book-ISBN 978-3-446-47256-3

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446470293
sowie im Buchhandel

Vorwort

Für die meisten Menschen ist die Informatik fest mit der Entstehungsgeschichte des Computers verbunden; einer Technik, die von außen betrachtet keinen Grenzen zu unterliegen scheint. Wir erleben seit Jahren eine schier ungebremste Entwicklung und sind längst daran gewöhnt, dass der Computer von heute schon morgen überholt ist. Dass sich hinter der Computertechnik eine tiefgründige Wissenschaft verbirgt, die all die großen Erfolge erst möglich macht, bleibt vielen Menschen verborgen. Die Rede ist von der theoretischen Informatik.

In der Grundlagenausbildung hat die theoretische Informatik ihren festen Platz eingenommen. Viele Studierende begegnen ihr mit gemischten Gefühlen und von manchen wird sie gar als bedrohlich empfunden. Mitverantwortlich für diese Misere sind die historischen Wurzeln der theoretischen Informatik. Entstanden aus der Mathematik, wird sie häufig in einer Präzision dargestellt, die in der Informatik ihresgleichen sucht. Manch ein Leser verirrt sich schnell in einem Gewirr aus Definitionen, Sätzen und Beweisen, das die Sicht auf die eigentlichen Konzepte und Methoden unfreiwillig verdeckt. Dass die theoretische Informatik weder schwer noch trocken sein muss, versuche ich mit diesem Buch zu beweisen.

Die folgenden Kapitel werden von zwei Leitmotiven getragen. Zum einen möchte ich die grundlegenden Konzepte, Methoden und Ergebnisse der theoretischen Informatik vermitteln, ohne diese durch einen zu hohen Abstraktionsgrad zu vernebeln. Hierzu werden die Problemstellungen durchweg anhand von Beispielen motiviert und die Grundideen der komplizierteren Beweise an konkreten Probleminstanzen nachvollzogen. Zum anderen habe ich versucht, den Lehrstoff in vielerlei Hinsicht mit Leben zu füllen. An zahlreichen Stellen werden Sie Anmerkungen und Querbezüge vorfinden, die sich mit der historischen Entwicklung dieser einzigartigen Wissenschaftsdisziplin beschäftigen.

Bei allen Versuchen, einen verständlichen Zugang zu der nicht immer einfachen Materie zu schaffen, war es mir ein Anliegen, keinen Verlust an Tiefe zu erleiden. Das Buch ist für den Bachelor-Studiengang konzipiert und deckt die typischen Lehrinhalte ab, die im Grundstudium an den hiesigen Hochschulen und Universitäten unterrichtet werden.

Karlsruhe, im Februar 2022 Dirk W. Hoffmann

Inhaltsverzeichnis

1 Einführung

„Wir müssen wissen. Wir werden wissen.“

David Hilbert

1.1 Was ist theoretische Informatik?

Kaum eine andere Technologie hat unsere Welt so rasant und nachhaltig verändert wie der Computer. Unzählige Bereiche des täglichen Lebens werden inzwischen von Bits und Bytes dominiert – selbst solche, die noch vor einigen Jahren als elektronikfreie Zone galten. Die Auswirkungen dieser Entwicklung sind bis in unser gesellschaftliches und kulturelles Leben zu spüren und machen selbst vor der deutschen Sprache keinen Halt. Vielleicht haben auch Sie heute schon *gemailt*, *gesimst* oder *gegoogelt* (Abbildung 1.1). Die Digitalisierung unserer Welt ist in vollem Gange und eine Abschwächung der eingeschlagenen Entwicklung zumindest mittelfristig nicht abzusehen.

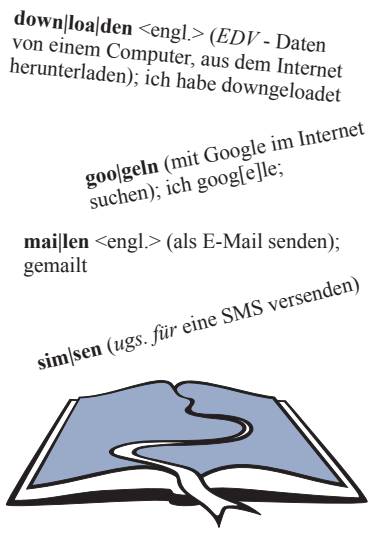


Abbildung 1.1: Die zunehmende Technisierung des Alltagslebens macht auch vor der deutschen Sprache keinen Halt. Im Jahr 2004 schaffte es das neudeutsche Verb *googeln* in den Duden [106]. Dort finden sich auch die Worte *mailen*, *simsen* und *downloaden* wieder.

Die in der Retrospektive einzigartige Evolution der Computertechnik ist eng mit der Entwicklung der Informatik verbunden. Als naturwissenschaftliche Fundierung der Computertechnik untersucht sie die Methoden und Techniken, die eine digitale Welt wie die unsere erst möglich machen. In der gleichen Geschwindigkeit, in der Computer die Welt eroberten, konnte sich die Informatik von einer Nischendisziplin der Mathematik und Elektrotechnik zu einer eigenständigen Grundlagenwissenschaft entwickeln. War sie zu Anfang auf wenige Kernbereiche beschränkt, so präsentiert sich die Informatik mittlerweile als eine breit gefächerte Wissenschaftsdisziplin. Heute existieren Schnittstellen in die verschiedensten Bereiche wie die Biologie, die Medizin und sogar die bildenden Künste.

In Abbildung 1.2 sind die vier Säulen dargestellt, von denen die Informatik gegenwärtig getragen wird. Eine davon ist die theoretische Informatik. Sie beschäftigt sich mit den abstrakten Konzepten und Methoden, die sich hinter den Fassaden moderner Computersysteme verbergen. Die theoretische Informatik ist vor der technischen Informatik die

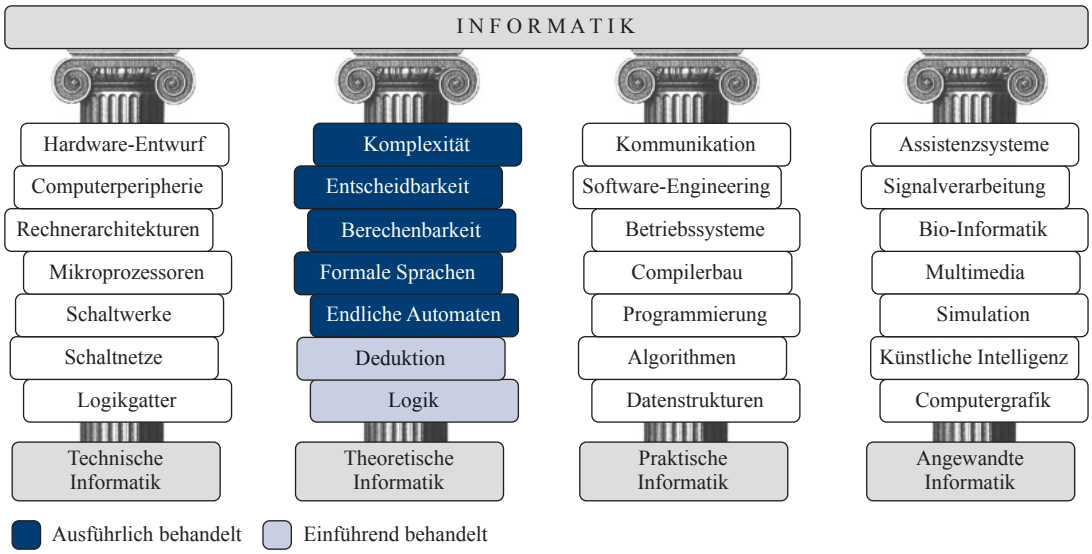


Abbildung 1.2: Die vier Säulen der Informatik

älteste Kernsäule und hat ihren direkten Ursprung in der Mathematik. Trotz ihres relativen Alters hat dieser Zweig der Informatik nichts von seiner ursprünglichen Bedeutung verloren. Er bildet das konzeptionelle Fundament, auf dem die anderen Bereiche der Informatik solide ruhen und aus dessen Wissensfundus sie schöpfen.

Betrachten wir die inhaltlichen Themen der modernen theoretischen Informatik genauer, so lassen sich diese in die folgenden Teilgebiete untergliedern (vgl. Abbildung 1.3):

- Logik und Deduktion (Kapitel 3)

  Die Logik beschäftigt sich mit grundlegenden Fragestellungen mathematischer Theorien. Im Mittelpunkt steht die Untersuchung *formaler Systeme* (*Kalküle*), in denen Aussagen aus einer kleinen Menge vorgegebener Axiome durch die Anwendung fest definierter Schlussregeln abgeleitet werden. Die Logik spielt nicht nur in der theoretischen Informatik, sondern auch in der technischen Informatik und der Software-Entwicklung eine Rolle. Mit der Aussagenlogik gibt sie uns ein Instrumentarium an die Hand, mit dem wir jede erdenkliche Hardware-Schaltung formal beschreiben und analysieren können. Ferner lässt sich mit der Prädikatenlogik und den Logiken höherer Stufe das Verhalten komplexer Hardware- und Software-Systeme exakt spezifizieren und in Teilen verifizieren.

- Formale Sprachen (Kapitel 4)

  Die Theorie der formalen Sprachen beschäftigt sich mit der Analyse, der Klassifikation und der generativen Erzeugung von Wortmengen. Künstliche Sprachen sind nach festen Regeln aufgebaut, die zusammen mit dem verwendeten Symbolvorrat eine formale Grammatik bilden. Die zugrunde liegende Theorie gibt uns die Methoden und Techniken an die Hand, die für den systematischen Umgang mit modernen Programmiersprachen und dem damit zusammenhängenden Compilerbau unabdingbar sind. Viele Erkenntnisse aus diesem Bereich haben ihre Wurzeln in der Linguistik und stoßen dementsprechend auch außerhalb der Informatik auf reges Interesse.

- Automatentheorie (Kapitel 5)

  Hinter dem Begriff des endlichen Automaten verbirgt sich ein abstraktes Maschinenmodell, das sich zur Modellierung, zur Analyse und zur Synthese zustandsbasierter Systeme eignet. Auf der obersten Ebene untergliedern sich endliche Automaten in Akzeptoren und Transduktoren. Erstere zeigen einen engen Bezug zu den formalen Sprachen, Letztere spielen im Bereich des Hardware-Entwurfs eine dominierende Rolle. Sie sind das mathematische Modell, mit dem sich das zeitliche Verhalten synchron getakteter Digitalschaltungen exakt beschreiben und analysieren lässt.

- Berechenbarkeitstheorie (Kapitel 6)

  Die Berechenbarkeitstheorie beschäftigt sich mit grundlegenden Untersuchungen über die algorithmische Lösbarkeit von Problemen. Die Bedeutung dieses Teilgebiets der theoretischen Informatik ist zweigeteilt. Zum einen wird das gesamte Gebiet der Algorithmentechnik durch die Definition formaler Berechnungsmodelle auf einen formalen Unterbau gestellt. Zum anderen ermöglicht uns die systematische Vorgehensweise, die Grenzen der prinzipiellen Berechenbarkeit auszuloten.

- Komplexitätstheorie (Kapitel 7)

  Während die Berechenbarkeitstheorie Fragen nach der puren Existenz von Algorithmen beantwortet, versucht die Komplexitätstheorie die Eigenschaften einer Lösungsstrategie quantitativ zu erfassen. Algorithmen werden anhand ihres Speicherplatzbedarfs und Zeitverbrauchs in verschiedene Komplexitätsklassen eingeteilt, die Rückschlüsse auf deren praktische Verwertbarkeit zulassen. Die Ergebnisse dieser Theorie beeinflussen den gesamten Bereich der modernen Software- und Hardware-Entwicklung.

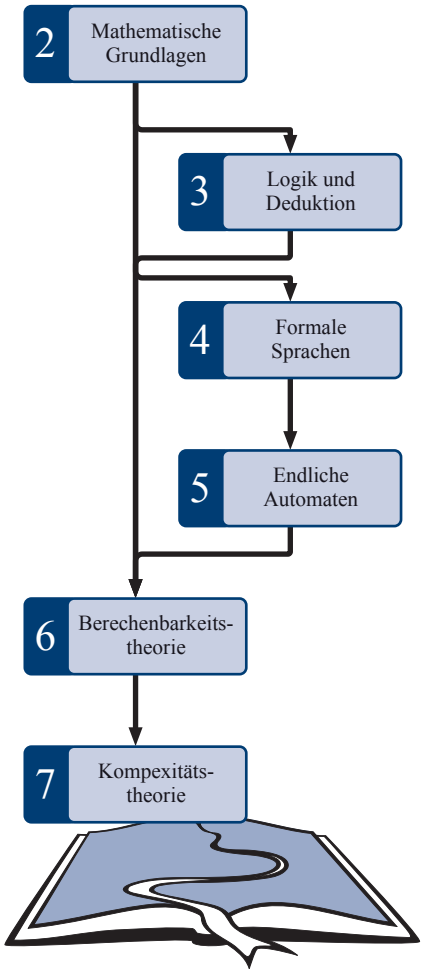


Abbildung 1.3: Kapitelübersicht. Die Pfeile deuten an, wie die einzelnen Kapitel inhaltlich zusammenhängen.

1. Axiom:
„Zu zwei Punkten gibt es genau eine Gerade, auf der sie liegen.“

2. Axiom:
„Jede gerade Strecke zwischen zwei Punkten lässt sich eindeutig verlängern.“

3. Axiom:
„Zu einem Punkt und einer Strecke kann man genau einen Kreis konstruieren.“

4. Axiom:
„Alle rechten Winkel sind gleich.“

5. Axiom:
„Zu einer Geraden und einem Punkt außerhalb der Geraden gibt es genau eine Gerade, die durch den Punkt geht und parallel zur ersten Geraden ist.“

Euklid von Alexandria
(ca. 365 v. Chr. – ca. 300 v. Chr.)

Abbildung 1.4: Die euklidischen Axiome

1.2 Zurück zu den Anfängen

Bevor wir uns ausführlich mit den Begriffen und Methoden der theoretischen Informatik beschäftigen, wollen wir in einem historischen Streifzug herausarbeiten, in welchem Umfeld ihre Teilgebiete entstanden sind und in welchem Zusammenhang sie heute zueinander stehen.

1.2.1 Die Mathematik in der Krise

Die theoretische Informatik hat ihre Wurzeln in der Mathematik. Ihre Geschichte beginnt mit der *Grundlagenkrise*, die Anfang des zwanzigsten Jahrhunderts einen Tiefpunkt in der mehrere tausend Jahre alten Historie der Mathematik markierte. Um die Geschehnisse zu verstehen, die die älteste aller Wissenschaften in ihren Grundfesten erschütterten, wollen wir unseren Blick zunächst auf das achtzehnte Jahrhundert richten. Zu dieser Zeit war die Mathematik schon weit entwickelt, jedoch noch lange nicht die abstrakte Wissenschaft, wie wir sie heute kennen. Fest in der realen Welt verankert, wurde sie vor allem durch Problemstellungen der physikalischen Beobachtung vorangetrieben. Zahlen waren nichts weiter als Messgrößen für reale Objekte und weit von den immateriellen Gedankengebilden der modernen Zahlentheorie entfernt. So wenig wie die Mathematik als eigenständige Wissenschaft existierte, so wenig gab es den reinen Mathematiker.

Im neunzehnten Jahrhundert änderte sich die Sichtweise allmählich in Richtung einer abstrakteren Mathematik. Zahlen und Symbole wurden von ihrer physikalischen Interpretation losgelöst betrachtet und entwickelten sich langsam, aber beharrlich zu immer abstrakter werdenden Größen. Mit der geänderten Sichtweise war es nun möglich, eine Gleichung der Form

$$c^2 = a^2 + b^2$$

völlig unabhängig von ihrer pythagoreischen Bedeutung zu betrachten. In ihrer abstraktesten Interpretation lässt sie sich als mathematisches Spiel begreifen, das uns erlaubt, die linke Seite durch die rechte zu ersetzen. Die Variablen a, b und c degradieren in diesem Fall zu inhaltsleeren Größen, die in keinerlei Bezug mehr zu den Seitenlängen eines rechtwinkligen Dreiecks stehen.

Dass es richtig war, das mathematische Gedankengerüst von seiner physikalischen Interpretation zu trennen, wurde durch die Physik selbst untermauert. So machte die zu Beginn des zwanzigsten Jahrhunderts auf-

„Wenn es sich darum handelt, die Grundlagen einer Wissenschaft zu untersuchen, so hat man ein System von Axiomen aufzustellen, welche eine genaue und vollständige Beschreibung derjenigen Beziehungen enthalten, die zwischen den elementaren Begriffen jener Wissenschaft stattfinden. Die aufgestellten Axiome sind zugleich die Definitionen jener elementaren Begriffe und jede Aussage innerhalb des Bereiches der Wissenschaft, deren Grundlagen wir prüfen, gilt uns nur dann als richtig, falls sie sich mittelst einer endlichen Anzahl logischer Schlüsse aus den aufgestellten Axiomen ableiten lässt. Bei näherer Betrachtung entsteht die Frage, ob etwa gewisse Aussagen einzelner Axiome sich untereinander bedingen und ob nicht somit die Axiome noch gemeinsame Bestandteile enthalten, die man beseitigen muss, wenn man zu einem System von Axiomen gelangen will, die völlig voneinander unabhängig sind.
Vor allem aber möchte ich unter den zahlreichen Fragen, welche hinsichtlich der Axiome gestellt werden können, dies als das wichtigste Problem bezeichnen, zu beweisen, dass dieselben untereinander widerspruchslos sind, d.h., dass man aufgrund derselben mittelst einer endlichen Anzahl von logischen Schlüssen niemals zu Resultaten gelangen kann, die miteinander in Widerspruch stehen.“

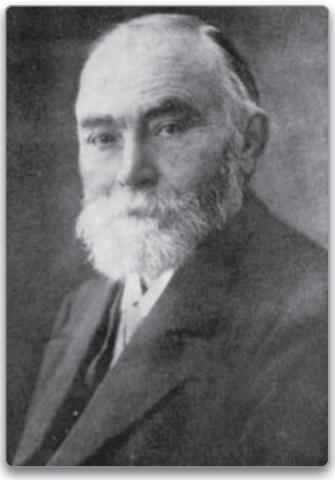
David Hilbert
(1862 – 1943)

Abbildung 1.5: Auszug aus Hilberts historischer Jahrhundertrede auf dem internationalen Kongress der Mathematiker in Paris

keimende Quantenmechanik deutlich, dass die damals wie heute merkwürdig anmutenden Effekte der Elementarteilchenphysik nur mithilfe abstrakter Modelle präzise erfasst werden können. Viele mathematische Konstrukte wie z. B. der *Hilbertraum* oder die *abstrakte Gruppe* konnten nachträglich zur Beschreibung der Natur eingesetzt werden, obwohl diese nichts mit unserer makroskopischen Anschauung gemeinsam haben.

Die zunehmende Abstraktion ließ Raum für Fragen zu, die sich in einer physikalisch gedeuteten Mathematik nicht stellen. Interpretieren wir z. B. die *euklidischen Axiome* (Abbildung 1.4) ausschließlich im Sinne der klassischen Geometrie, so erscheinen sie als reine Selbstverständlichkeit. Sie decken sich mit den Erfahrungen, die wir in der makroskopischen Welt tagtäglich machen und kaum jemand würde auf die Idee kommen, an ihnen zu zweifeln. Entsprechend lange galten die Axiome als unantastbar.

Die Situation ändert sich, sobald wir die Mathematik als ein abstraktes Wechselspiel von Symbolen und Regeln betreiben. Lösen wir uns von der intuitiven Interpretation der euklidischen Axiome, so stellt sich



Gottlob Frege
(1848 – 1925)

Abbildung 1.6: Gottlob Frege. Der im mecklenburgischen Wismar geborene Mathematiker zählt zu den Mitbegründern der mathematischen Logik und der analytischen Philosophie. Im Jahr 1879 eröffnete Frege mit seiner berühmten *Begriffsschrift* einen axiomatischen Zugang zur Logik [35]. Er führt darin die grundlegenden Konzepte und Begriffe ein, die wir auch heute noch in der Prädikatenlogik (Abschnitt 3.2) und den Logiken höherer Stufe (Abschnitt 3.3.2) verwenden. Sein Begriffsgerüst war deutlich weiter entwickelt als die Syllogismen des Aristoteles – der bis dato präzisesten Form des logischen Schließens. Die meiste Zeit seines Lebens war Frege ein überzeugter Verfechter des *Logizismus*. Er vertrat die Auffassung, dass die Mathematik ein Teil der Logik sei. In diesem Sinne müssen sich alle Wahrheiten auf eine Menge von Axiomen zurückführen lassen, die nach Freges Worten *„eines Beweises weder fähig noch bedürftig“* seien. Er stand damit in einer Gegenposition zu anderen Mathematikern seiner Zeit, von denen viele die Logik als isoliertes Teilgebiet der Mathematik begriffen.

die Frage, ob diese ein vollständiges und widerspruchsfreies Gebilde ergeben. Im Jahr 1899 gelang es David Hilbert, diese Frage positiv zu beantworten. Er postulierte ein Axiomensystem, aus dem sich alle Sätze der euklidischen Geometrie ableiten lassen, ohne die verwendeten Symbole mit einer speziellen Interpretation zu versehen [46].

Inspiriert von den Anfangserfolgen stand die Mathematik um die Jahrhundertwende vollends im Zeichen der axiomatischen Methode. Das Führen eines Beweises wurde als der Prozess verstanden, Sätze durch die Anwendung wohldefinierter Schlussregeln aus einer kleinen Menge vorgegebener, a priori als wahr definierter Axiome abzuleiten. Eine spezielle Interpretation der Symbole war hierzu nicht erforderlich und im Grunde genommen auch gar nicht angestrebt. Die Mathematik wurde zu einem Spiel, das nach starren Regeln funktionierte, und das Führen eines Beweises zu einem mechanischen Prozess werden ließ.

Der deutsche Mathematiker David Hilbert war kein Unbekannter. Bereits zu Lebzeiten wurde er als Ikone gefeiert und beeinflusste wie kein anderer die Mathematik des beginnenden zwanzigsten Jahrhunderts. Im Jahr 1900 hielt Hilbert auf dem internationalen Kongress der Mathematiker in Paris eine wegweisende Rede, an der sich die weitere Stoßrichtung der gesamten Mathematik über Jahre hinweg orientieren sollte (vgl. Abbildung 1.5). In seiner Ansprache trug er 23 ungelöste Probleme vor, die für die Mathematik von immenser Wichtigkeit, aber bis dato ungelöst waren.

Bereits an zweiter Stelle forderte Hilbert die Weltgemeinschaft dazu auf, einen Beweis für die Widerspruchsfreiheit der arithmetischen Axiome zu liefern. Das Problem, das Hilbert hier ansprach, war von immenser Wichtigkeit für die gesamte Mathematik, schließlich adressieren die arithmetischen Axiome den vitalen Kern, auf dem alle Teilbereiche dieser Wissenschaft aufbauen. Solange es nicht gelingt, die Widerspruchsfreiheit formal zu beweisen, kann nicht mit Sicherheit ausgeschlossen werden, dass sich z. B. neben dem Theorem $1+1=2$ auch das Theorem $1+1\neq 2$ aus den Axiomen ableiten lässt. Das verästelte Gebäude der Mathematik würde auf einen Schlag in Trümmern vor uns liegen.

Bereits wenige Jahre nach Hilberts Rede sollte die Wissenschaftsgemeinde erleben, wie real eine solche Gefahr wirklich war. Der deutsche Mathematiker Gottlob Frege (Abbildung 1.6) spürte sie am eigenen Leib, als er 1902 ein formales Axiomensystem für ein Teilgebiet der Mathematik aufstellte, das auf den ersten Blick so intuitiv und einfach erscheint wie kaum ein anderes. Die Rede ist von der *Mengenlehre*. Der zweite Band seiner *Grundgesetze der Arithmetik* schließt mit dem folgenden Nachwort [33, 34]:

„Einem wissenschaftlichen Schriftsteller kann kaum etwas Unerwünschteres begegnen, als dass ihm nach Vollendung einer Arbeit eine der Grundlagen seines Baues erschüttert wird."

Doch wodurch wurde Freges Arbeit so grundlegend erschüttert, dass er sein gesamtes Werk gefährdet sah? Die Antwort ist in einem Brief von Bertrand Russell zu finden, den er im Jahr 1902 an Frege schickte – just zu der Zeit, als dieser sein mathematisches Werk vollendete. Aufbauend auf den Begriffen der naiven Mengenlehre definierte Russell die Menge aller Mengen, die sich nicht selbst als Element enthalten:

$$M := \{M' \mid M' \notin M'\}$$

Die Definition von M ist mit der damals verwendeten Mengendefinition von Georg Cantor vereinbar, führt bei genauerer Betrachtung jedoch unweigerlich zu einem Widerspruch. Da für jedes Element a und jede Menge M entweder $a \in M$ oder $a \notin M$ gilt, muss auch M entweder in sich selbst enthalten sein oder nicht. Die Definition von M offenbart uns jedoch das folgende erstaunliche Ergebnis:

$$M \in M \Rightarrow M \notin M, \quad M \notin M \Rightarrow M \in M$$

Der als *Russell'sche Antinomie* bekannte Widerspruch entlarvte den Cantor'schen Mengenbegriff als in sich widersprüchlich und lies Freges Gedankengerüst wie ein Kartenhaus in sich zusammenstürzen. Die Geschehnisse unterstrichen nachhaltig, wie wichtig eine widerspruchsfreie Fundierung der Mathematik tatsächlich war.

Zu den ersten, die sich der neugeborenen Herausforderung stellten, gehörten die britischen Mathematiker Bertrand Russell und Alfred North Whitehead. Sie starteten den Versuch, ein widerspruchsfreies Fundament zu errichten, auf dem die Mathematik für alle Zeiten einen sicheren Halt finden sollte. Nach zehn Jahren intensiver Arbeit war das Ergebnis greifbar: Die *Principia Mathematica* waren fertiggestellt (vgl. Abbildung 1.7). In einem dreibändigen Werk unternahmen Russell und Whitehead den Versuch, weite Bereiche der Mathematik mit den Mitteln der elementaren Logik formal herzuleiten. Ein großer Teil des Werks ist der *Typentheorie* gewidmet; einer widerspruchsfreien Konstruktion des Mengenbegriffs, mit dem die Art von Selbstbezug vermieden wird, die wenige Jahre zuvor die Mathematik in ihre größte Krise stürzte. Heute gilt die Typentheorie der Principia als überholt. An ihre Stelle tritt der formale axiomatische Aufbau der Mengenlehre durch Ernst Zermelo und Abraham Fraenkel, der die Russell'sche Antinomie ebenfalls beseitigt [32, 111].

Die mathematische Widerspruchsfreiheit ist eine unabdingbare Eigenschaft des mathematischen Schließens. Fehlt sie, so verkommt jedes formale System zu einem wertlosen Gedankengebilde. Warum dies so ist, wollen wir im Folgenden kurz begründen. Nehmen wir an, es gebe eine Aussage R, für die sich sowohl R als auch ihre Negation $\neg R$ innerhalb des Kalküls ableiten lassen. Die Situation erscheint wenig bedrohlich, wenn es sich um eine Aussage handelt, die uns nicht weiter interessiert. Eventuell ist R eine Aussage der Russell'schen Art, die uns ohnehin suspekt erscheint. Können wir den Kalkül vielleicht trotzdem sinnvoll einsetzen, wenn wir Aussagen dieser Form schlicht außen vor lassen?

Dass sich widersprüchliche Aussagen in einem Kalkül nicht isoliert betrachten lassen, liegt an den Schlussregeln der klassischen Logik. In Kapitel 3 werden Sie erlernen, wie sich das Theorem

$$\neg P \to (P \to Q)$$

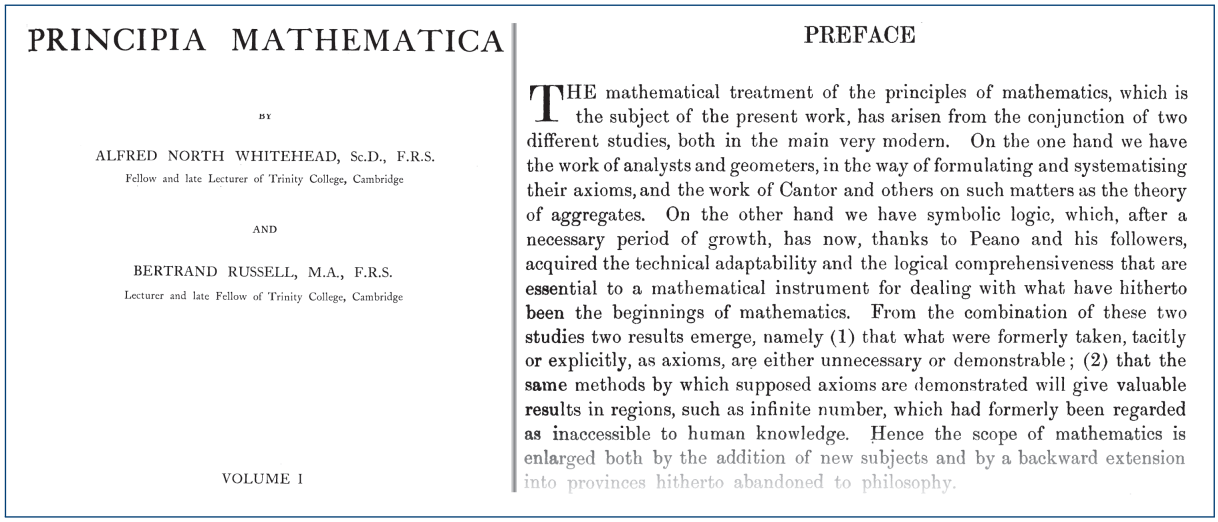
aus den elementaren Axiomen der Logik herleiten lässt. In Worten besagt es: Ist P falsch, so folgt aus der Wahrheit von P die Wahrheit von Q. Substituieren wir R für P, so erhalten wir das Theorem

$$\neg R \to (R \to Q).$$

Da $\neg R$ eine wahre Aussage ist, lässt sich mithilfe der *Abtrennungsregel* (*Modus ponens*) das Theorem

$$R \to Q$$

herleiten. Nach Voraussetzung ist R ebenfalls wahr, so dass eine erneute Anwendung der Abtrennungsregel das Theorem Q hervorbringt. Da die Wahl von Q keinen Einschränkungen unterliegt, können wir eine beliebige Aussage für Q substituieren. Kurzum: In einem widersprüchlichen Kalkül lassen sich ausnahmslos alle Aussagen als wahr beweisen.



PRINCIPIA MATHEMATICA

BY

ALFRED NORTH WHITEHEAD, Sc.D., F.R.S.
Fellow and late Lecturer of Trinity College, Cambridge

AND

BERTRAND RUSSELL, M.A., F.R.S.
Lecturer and late Fellow of Trinity College, Cambridge

VOLUME I

PREFACE

THE mathematical treatment of the principles of mathematics, which is the subject of the present work, has arisen from the conjunction of two different studies, both in the main very modern. On the one hand we have the work of analysts and geometers, in the way of formulating and systematising their axioms, and the work of Cantor and others on such matters as the theory of aggregates. On the other hand we have symbolic logic, which, after a necessary period of growth, has now, thanks to Peano and his followers, acquired the technical adaptability and the logical comprehensiveness that are essential to a mathematical instrument for dealing with what have hitherto been the beginnings of mathematics. From the combination of these two studies two results emerge, namely (1) that what were formerly taken, tacitly or explicitly, as axioms, are either unnecessary or demonstrable; (2) that the same methods by which supposed axioms are demonstrated will give valuable results in regions, such as infinite number, which had formerly been regarded as inaccessible to human knowledge. Hence the scope of mathematics is enlarged both by the addition of new subjects and by a backward extension into provinces hitherto abandoned to philosophy.

Abbildung 1.7: Die *Principia Mathematica*, erstmals erschienen in den Jahren 1910 bis 1913, ist eines der berühmtesten mathematischen Werke unserer Geschichte. Auf über 1800 Seiten, verteilt auf 3 Bände, unternahmen die Autoren den Versuch, alle mathematischen Erkenntnisse aus einer kleinen Menge von Axiomen systematisch herzuleiten.

Die Principia war in puncto Präzision jedem anderen Werk ihrer Zeit weit voraus. Sie fasste einen mathematischen Beweis als eine Folge von Regelanwendungen auf, durch die eine Aussage in endlich vielen Schritten aus einer festgelegten Menge von Axiomen abgeleitet wurde.

1.2.2 Metamathematik

Durch die zunehmende Beschäftigung mit den verschiedensten formalen Systemen entstand im Laufe der Zeit eine Metamathematik, die sich nicht mit der Ableitung von Sätzen *innerhalb* eines Kalküls beschäftigt, sondern mit Sätzen, die Aussagen *über* den Kalkül treffen. Drei Fragestellungen rückten in das Zentrum des Interesses:

- Vollständigkeit

  Ein formales System heißt *vollständig*, wenn jede wahre Aussage, die in der Notation des Kalküls formuliert werden kann, innerhalb desselben beweisbar ist. Mit anderen Worten: Für jede wahre Aussage P muss es eine endliche Kette von Regelanwendungen geben, die P aus den Axiomen deduziert. Beachten Sie, dass uns ein vollständiger Kalkül nicht preisgeben muss, wie eine solche Kette zu finden ist. Die Vollständigkeit garantiert lediglich deren Existenz.

- Widerspruchsfreiheit

  Ein formales System heißt *widerspruchsfrei*, wenn für eine Aussage P niemals gleichzeitig P und die Negation von P (geschrieben als $\neg P$) abgeleitet werden kann. Auf die immense Bedeutung der Widerspruchsfreiheit eines Kalküls sind wir weiter oben bereits eingegangen. Erfüllt ein formales System diese Eigenschaft nicht, so könnte es kaum wertloser sein. Es würde uns gestatten, jede beliebige Aussage zu beweisen.

- Entscheidbarkeit

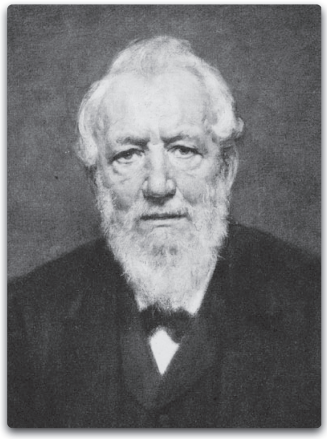
  Ein formales System heißt *entscheidbar*, wenn ein systematisches Verfahren existiert, mit dem für jede Aussage entschieden werden kann, ob sie innerhalb des Kalküls beweisbar ist. Hinter der Eigenschaft der Entscheidbarkeit verbirgt sich nichts Geringeres als der Wunsch nach einer mechanisierten Mathematik. Wäre z. B. die Zahlentheorie vollständig und entscheidbar, so ließe sich für jede wahre zahlentheoretische Aussage auf maschinellem Wege ein Beweis konstruieren. Der Traum eines jeden Mathematikers würde wahr.

Hilbert war überzeugt, dass eine vollständige, widerspruchsfreie und entscheidbare Axiomatisierung der Mathematik möglich sei. Im Jahr 1929 wurden seine Hoffnungen durch die Arbeiten des jungen Mathematikers Kurt Gödel zusätzlich genährt, als dieser in seiner Promotionsschrift die Vollständigkeit der Prädikatenlogik erster Stufe bewies [36]. Es war also möglich, einen Kalkül zu konstruieren, in dem sich jede wahre prädikatenlogische Formel in endlich vielen Schritten aus den Axiomen ableiten lässt. In diesen Tagen schien es nur eine Frage der Zeit zu sein, bis aus Hilberts Vermutungen Gewissheit werden würde.

1930 war das Jahr, in dem die Entwicklung eine abrupte Kehrtwende nehmen sollte. Am 8. September bekräftigte Hilbert vor der Versammlung Deutscher Naturforscher und Ärzte in seiner Heimatstadt Königsberg seine tiefe Überzeugung, dass es in der Wissenschaft keine unlösbaren Probleme gibt. Ein Auszug aus seiner Rede wurde in Form einer Radioansprache ausgestrahlt. Sie schließt mit den berühmten Worten:

> *„Wir dürfen nicht denen glauben, die heute mit philosophischer Miene und überlegenem Tone den Kulturuntergang prophezeien und sich in dem Ignorabimus gefallen. Für uns gibt es kein Ignorabimus, und meiner Meinung nach auch für die Naturwissenschaft überhaupt nicht. Statt des törichten Ignorabimus heiße im Gegenteil unsere Losung: Wir müssen wissen, wir werden wissen.“*

„Ignoramus et ignorabimus.“
(Wir wissen es nicht und wir werden es niemals wissen)



Emil Heinrich Du Bois-Reymond
(1818 – 1896)

„Für uns gibt es kein Ignorabimus“. Mit diesem Satz bekräftigte David Hilbert seine Haltung, dass es in den Naturwissenschaften keine unbeweisbaren Wahrheiten gibt. Der Begriff *Ignorabimus* wurde durch den deutschen Gelehrten Emil Heinrich Du Bois-Reymond geprägt. Durch seine Leipziger Rede vor der Versammlung Deutscher Naturforscher und Ärzte löste er im Jahr 1872 einen Richtungsstreit aus, der auf Jahre hinweg zu kontroversen Diskussionen in der Wissenschaftsgemeinde führen sollte. Er vertrat die Meinung, dass Begriffe wie das Bewusstsein niemals mit naturwissenschaftlichen Methoden erklärbar sein werden. Kurzum: Die Wissenschaft besitzt unüberwindbare Grenzen. *„Ich werde jetzt, wie ich glaube, in sehr zwingender Weise dartun, dass nicht allein bei dem heutigen Stand unserer Kenntnis das Bewusstsein aus seinen materiellen Bedingungen nicht erklärbar ist, was wohl jeder zugibt, sondern dass es auch der Natur der Dinge nach aus diesen Bedingungen nicht erklärbar sein wird.“* [8].

Der Unvollständigkeitsbeweis ist nicht nur aufgrund seiner inhaltlichen Tragweite von Bedeutung. Auch die trickreiche Beweisführung, mit der Gödel sein Resultat erzielte, zeugt von der Tiefgründigkeit des Ergebnisses. Gödel konnte zeigen, dass mathematische Schlussregeln, die Aussagen *über* Zahlen machen, selbst als Zahl verstanden werden konnten. Damit war es möglich, die Ebene der Zahlentheorie mit ihren Metaebenen zu vermischen. Aussagen sind nichts anderes als Zahlen, die selbst Aussagen über Zahlen tätigen. Auf diese Weise gelang es Gödel, Metaaussagen wie *„Aussage XYZ ist beweisbar“* innerhalb des Systems zu codieren.
Um die Unvollständigkeit zu beweisen, wandte Gödel einen Trick an. Er konstruierte Aussagen, die auf sich selbst Bezug nehmen und so eine Metaaussage über sich selbst beinhalten. Auf diese Weise gelang es ihm, eine Formel zu konstruieren, die der Metaaussage *„Diese Formel ist nicht beweisbar“* entspricht. Ist die Formel wahr, so lässt sie sich nicht beweisen und das zugrunde liegende Axiomensystem ist unvollständig. Ist sie falsch, so würde ein Beweis für eine falsche Aussage existieren und das Axiomensystem wäre nicht widerspruchsfrei. Mit anderen Worten: Erfüllt ein Axiomensystem die Eigenschaft der Widerspruchsfreiheit, so ist es zwangsläufig unvollständig.
Der Unvollständigkeitssatz zeigte zudem, dass die Widerspruchsfreiheit eines hinreichend aussagekräftigen formalen Systems nicht *innerhalb* des Systems selbst bewiesen werden kann. Gödel nutzte aus, dass in einem widersprüchlichen System alle Aussagen wahr sind, d. h., ein Kalkül ist genau dann widerspruchsfrei, wenn es eine einzige Aussage gibt, die nicht bewiesen werden kann. Gödel konnte jedoch zeigen, dass eine Aussage der Form *„es existiert eine unbeweisbare Aussage“* ebenfalls nicht innerhalb des Systems bewiesen werden kann.

Die Rede ist im Originalton erhalten und ein unschätzbares Dokument der Zeitgeschichte. Sie zeigt nachdrücklich, wie überzeugt Hilbert von der Durchführbarkeit seines ehrgeizigen Programms wirklich war.

Zum Zeitpunkt seiner Rede wusste Hilbert noch nichts von den Ereignissen, die sich am Vortag an anderer Stelle in Königsberg abspielten. Es war die große Stunde eines vierundzwanzigjährigen Mathematikers, der mit der Präsentation seines Unvollständigkeitssatzes die Mathematik aus den Angeln hob. Derselbe Kurt Gödel, der kurze Zeit zuvor die Vollständigkeit der Prädikatenlogik bewies, konnte zeigen, dass die Arithmetik aus fundamentalen Überlegungen heraus unvollständig sein musste. Sein Ergebnis war so allgemein, dass es auf jedes axiomatische System angewendet werden konnte, das ausdrucksstark genug ist, um die Zahlentheorie zu formalisieren. Damit war nicht nur gezeigt, dass der logische Apparat der Principia Mathematica unvollständig war, sondern auch, dass jeder Versuch, die Principia oder ein ähnliches System zu vervollständigen, von Grund auf zum Scheitern verurteilt ist. Gödel versetzte dem Hilbert'schen Programm einen schweren Schlag, von dem es sich nie erholen sollte.

Gödels Arbeit verwies die Mathematik zweifelsohne in ihre Grenzen, ließ jedoch Hilberts dritte Vermutung außen vor. Auch wenn wir nicht in der Lage sind, einen widerspruchsfreien und zugleich vollständigen Kalkül für die Theorie der Zahlen zu konstruieren, so könnte die Frage nach der Entscheidbarkeit eines Kalküls dennoch positiv beantwortet werden. Der Unvollständigkeitsbeweis schließt nicht aus, dass ein systematisches Verfahren existiert, das für jede Aussage bestimmt, ob es innerhalb des Systems beweisbar ist oder nicht.

Die Hoffnung, dass zumindest diese letzte Frage positiv beantwortet werden könnte, wurde im Jahr 1936 vollends zerstört, als der britische Mathematiker Alan Turing seine grundlegende Arbeit *On computable numbers, with an application to the Entscheidungsproblem* der Öffentlichkeit präsentierte (Abbildung 1.8). Turings Arbeit ist für die theoretische Informatik aus zweierlei Gründen von Bedeutung. Zum einen gelang es ihm als einem der Ersten, die Grenzen der Berechenbarkeit formal zu erfassen und das Entscheidungsproblem negativ zu beantworten; die Jagd nach dem mathematischen Perpetuum Mobile war zu Ende. Zum anderen konstruierte Turing für seinen Beweis ein abstraktes Maschinenmodell, das dem Funktionsprinzip moderner Computer bereits sehr nahe kam. Aus heutiger Sicht bildet das gedankliche Gebilde der *Turing-Maschine* die Nahtstelle zwischen der abstrakten Mathematik des frühen zwanzigsten Jahrhunderts und der Welt der realen Rechenmaschinen. In gewissem Sinne ersann Turing den *missing link*, der die Mathematik in Form des Computers zum Leben erweckte.

Sachwortverzeichnis

Symbole

A

B

C

D

E

F

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z