

eXamen.press

eXamen.press ist eine Reihe, die Theorie und Praxis aus allen Bereichen der Informatik für die Hochschulausbildung vermittelt.

Gerald Teschl
Susanne Teschl

Mathematik für Informatiker

Band 1: Diskrete Mathematik und Lineare Algebra

2. Auflage
Mit 91 Abbildungen

 Springer

Gerald Teschl

Universität Wien
Fakultät für Mathematik
Nordbergstraße 15
1090 Wien, Österreich
gerald.teschl@univie.ac.at
<http://www.mat.univie.ac.at/~gerald/>

Susanne Teschl

Fachhochschule Technikum Wien
Höchstädtplatz 5
1200 Wien, Österreich
susanne.teschl@technikum-wien.at
<http://www.esi.ac.at/~susanne/>

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISSN 1614-5216

ISBN 978-3-540-70824-7 Springer Berlin Heidelberg New York

ISBN 978-3-540-25782-0 1. Auflage Springer Berlin Heidelberg New York

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Springer ist ein Unternehmen von Springer Science+Business Media
springer.de

© Springer-Verlag Berlin Heidelberg 2006, 2007

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Text und Abbildungen wurden mit größter Sorgfalt erarbeitet. Verlag und Autor können jedoch für eventuell verbliebene fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Satz: Druckfertige \LaTeX -Daten der Autoren
Herstellung: LE- \TeX , Jelonek, Schmidt & Vöckler GbR, Leipzig
Umschlaggestaltung: KünkelLopka Werbeagentur, Heidelberg
Gedruckt auf säurefreiem Papier 33/3100 YL - 5 4 3 2 1 0

Vorwort

Warum Mathematik?

Wenn Sie sich mit Ihrem Webbrowser ein Bild im JPEG-Format ansehen, Ihr Online-Banking über ein verschlüsseltes Formular abwickeln oder ein paar Stichworte der Suchmaschine Ihrer Wahl übergeben, dann haben alle diese Tätigkeiten eines gemeinsam: Immer ist Mathematik im Spiel! Auch wenn das für den Benutzer oft nicht unmittelbar ersichtlich ist.

Wollen Sie also Informatik verstehen und in der Lage sein, existierende Lösungen zu hinterfragen bzw. neue Probleme zu lösen, dann liefert die Mathematik die Grundlage dazu. Natürlich ist uns dabei klar, dass Sie an der Mathematik in erster Linie als „Handwerkszeug“ interessiert sind. Deshalb haben wir auch versucht, wann immer möglich sofort auf Anwendungen einzugehen oder zumindest Ausblicke auf mögliche Anwendungen zu geben. Trotzdem wird aber nicht nur Wert auf reine Rechentechnik, sondern auch auf solides Verständnis gelegt.

Mathematik hat noch einen weiteren wichtigen Aspekt: Sie ist eine der besten Möglichkeiten logisches Denken, Abstraktionsvermögen und kreative Problemlösungskompetenz zu fördern. Sie verlangt präzise Formulierungen und gründliche Berücksichtigung aller möglichen Szenarien. Letzteres wurde gerade in der Programmierpraxis bis vor kurzem noch als nutzlos belächelt: Es sei Zeitverschwendung, Fälle zu berücksichtigen, die bei *normaler* Benutzung nie auftreten. Heute bedeuten diese Fälle aber genau jene Schwachstellen, die einem Hacker den Zugriff auf Ihren Computer ermöglichen.

Gebrauchsanweisung (für Studierende)

Das vorliegende Buch entstand aus einem Skriptum, das von unseren Studentinnen und Studenten bereits seit mehreren Jahren verwendet wird, teilweise auch im Selbststudium (Stichwort *blended learning*). Es wurde laufend dank vieler Rückmeldungen überarbeitet. Insbesondere haben wir uns bemüht, typische Fehler und häufige Missverständnisse zu berücksichtigen. Trotzdem wird es passieren, dass Sie etwas beim ersten Lesen nicht gleich verstehen. Das geht allen so – Mathematik braucht etwas Zeit! Die zahlreichen Musterbeispiele sollen Ihnen aber ein möglichst effizientes Lernen ermöglichen. Am Ende jedes Kapitels finden Sie Kontrollfragen mit Lösungen, mit denen Sie Ihr Verständnis testen können.

Wie es aber für eine gute Kondition nicht reicht, Fitnessvideos aus sicherer Entfernung vom Sofa aus zu betrachten, so genügt es leider auch nicht, dieses Buch passiv zu lesen. Deshalb gibt es am Ende jedes Kapitels eine große Anzahl von Aufwärmübungen und weiterführenden Aufgaben, die Ihnen helfen, das Erlernete selbstständig umzusetzen. Die Aufwärmübungen trainieren Rechentechniken und es gibt vollständige Lösungen dazu. Die weiterführenden Aufgaben sollen Sie etwas herausfordern und verlangen auch, selbstständig mithilfe des Gelernten neue Wege zu gehen. Zu ihnen gibt es, wenn notwendig, kurze Lösungen oder Lösungshinweise.

Einige Passagen werden Ihnen wahrscheinlich noch aus der Schule bekannt sein. Falls Sie sich dabei langweilen, überfliegen Sie sie einfach – wir haben sie vor allem für jene, deren aktive Mathematik-Jahre schon etwas länger zurückliegen (berufsbegleitend Studierende), hinzugefügt. (Untersuchungen zeigen, dass auch Studierende mit guten mathematischen Vorkenntnissen von einer kleinen Auffrischung profitieren;-)

Die zahlreichen Beispiele und Übungsmöglichkeiten erklären auch den Umfang dieses Buches: Natürlich wäre es kein Problem gewesen, den gleichen Stoff in einem schmalen Bändchen unterzubringen. Wenn Sie lieber statt zwei Seiten nur eine halbe lesen und dann zwei Stunden darüber grübeln, dann sind Sie im falschen Buch.

Während des Lesens werden Sie immer wieder auf klein gedruckte Absätze stoßen. Diese enthalten weiterführende Bemerkungen, Beweise, Historisches oder einfach nur etwas Aufmunterung.

Gebrauchsanweisung (für Dozentinnen und Dozenten)

Wir haben uns bemüht, den Stoff in möglichst gleich große Teile zu zerlegen, die unserer Erfahrung nach von den Studierenden pro Einheit verdaut werden können. Außerdem haben wir versucht, die Kapitel so weit wie möglich unabhängig voneinander zu gestalten, um Schwerpunktsetzung und Auswahl einzelner Kapitel zu erleichtern.

Einige Kapitel können im Allgemeinen sicher als bekannt vorausgesetzt bzw. im Selbststudium erarbeitet werden. Für uns war es in der Lehre hilfreich, damit einen Grundstein zu legen, den wir für alle Studierenden voraussetzen können.

Die Themenbereiche Kryptographie und Codierungstheorie haben wir bewusst kurz gehalten, da wir davon ausgehen, dass sie in eigenen Vorlesungen behandelt werden.

Der Schwerpunkt liegt im Band 1 auf der diskreten Mathematik. Analysis und Statistik werden in Band 2 behandelt.

Computereinsatz

Obwohl wir den Einsatz des Computers als wichtigen Bestandteil der Mathematikausbildung sehen, haben wir ihn nicht direkt in den Text integriert, sondern am Ende jedes Kapitels positioniert. Erstens haben die Rückmeldungen gezeigt, dass die meisten Studierenden es bevorzugen, wenn Stoff und Computeralgebra getrennt sind, um nicht zwei neue Dinge auf einmal verstehen zu müssen. Zweitens ist es so leicht möglich, das von uns verwendete System, *Mathematica*, durch ein beliebiges anderes Programm zu ersetzen.

Beispiele, bei denen uns der Computereinsatz sinnvoll erscheint, sind mit „ \rightarrow CAS“ gekennzeichnet und im zugehörigen Abschnitt „Mit dem digitalen Rechenmeister“

mit *Mathematica* gelöst. Die Befehle dazu brauchen Sie nicht abzutippen. Die zugehörigen Notebooks sind auf der Website zum Buch (URL siehe unten) zu finden.

Eine Bitte...

Druckfehler sind wie Unkraut. Soviel man auch jätet, es bleiben immer ein paar übrig und so sind auch in diesem Buch trotz aller Sorgfalt sicher noch ein paar unentdeckte Fehler. Wir bitten Sie daher, uns diese mitzuteilen (auch wenn sie noch so klein sind). Die Liste der Korrekturen werden wir im Internet (URL siehe unten) bekannt geben. Natürlich freuen wir uns auch über alle anderen Rückmeldungen und sind für Verbesserungsvorschläge und Kritik offen.

Ergänzungen

Begleitend zu diesem Buch haben wir eine Website

<http://www.mat.univie.ac.at/~gerald/ftp/book-mfi/>

eingrichtet, auf der Sie Ergänzungen finden können. Surfen Sie einfach vorbei.

Zur zweiten Auflage

An dieser Stelle möchten wir uns zunächst für die zahlreichen positiven Rückmeldungen zur ersten Auflage bedanken. Wir freuen uns darüber, dass aufgrund der großen Nachfrage schon nach kurzer Zeit ein (korrigierter) Nachdruck notwendig war. In die nun vorliegende zweite Auflage sind auch Verbesserungsvorschläge und Anregungen unserer Leserinnen und Leser eingeflossen. Neu hinzugekommen ist weiters ein Kapitel über „Polyomringe und endliche Körper“.

Danksagungen

Unsere Studentinnen und Studenten haben uns durch die Jahre des Entstehens dieses Buches laufend mit Hinweisen auf Druckfehler und Verbesserungsvorschlägen versorgt. Hervorheben möchten wir dabei Markus Horehled, Rudolf Kunschek, Alexander-Philipp Lintenhofer, Markus Steindl und Gerhard Sztasek, die sich durch besonders lange Listen ausgezeichnet haben. Unsere Kollegen Oliver Fasching, Wolfgang Kugler, Wolfgang Timischl, Florian Wisser und insbesondere Karl Unterkofler haben immer wieder Abschnitte kritisch gelesen und mit vielen Tipps geholfen. Ihnen allen möchten wir herzlich danken!

Die Erstellung dieser Seiten wäre nicht ohne eine Reihe von Open-Source-Projekten (vor allem $\text{T}_{\text{E}}\text{X}$, $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$, $\text{T}_{\text{E}}\text{X}$ Shop und Vim) möglich gewesen.

Last but not least danken wir dem Springer-Verlag für die freundliche und engagierte Unterstützung.

Viel Freude und Erfolg mit diesem Buch!

Inhaltsverzeichnis

Grundlagen

1	Logik und Mengen	1
1.1	Elementare Logik	1
1.2	Elementare Mengenlehre	10
1.3	Schaltalgebra	15
1.3.1	Anwendung: Entwurf von Schaltkreisen	21
1.4	Mit dem digitalen Rechenmeister	23
1.5	Kontrollfragen	24
1.6	Übungen	28
2	Zahlenmengen und Zahlensysteme	33
2.1	Die Zahlenmengen \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} und \mathbb{C}	33
2.2	Summen und Produkte	44
2.3	Vollständige Induktion	46
2.4	Stellenwertsysteme	48
2.5	Maschinenzahlen	51
2.6	Teilbarkeit und Primzahlen	55
2.7	Mit dem digitalen Rechenmeister	58
2.8	Kontrollfragen	61
2.9	Übungen	65

Diskrete Mathematik

3	Elementare Begriffe der Zahlentheorie	71
3.1	Das kleine Einmaleins auf endlichen Mengen	71
3.1.1	Anwendung: Hashfunktionen	74
3.2	Gruppen, Ringe und Körper	77
3.2.1	Anwendung: Welche Fehler erkennen Prüffziffern?	87
3.3	Der Euklid'sche Algorithmus und diophantische Gleichungen	90
3.3.1	Anwendung: Der RSA-Verschlüsselungsalgorithmus	95
3.4	Der Chinesische Restsatz	100

3.4.1	Anwendung: Rechnen mit großen Zahlen	101
3.4.2	Anwendung: Verteilte Geheimnisse	103
3.5	Mit dem digitalen Rechenmeister	104
3.6	Kontrollfragen	107
3.7	Übungen	109
4	Polynomringe und endliche Körper	113
4.1	Der Polynomring $\mathbb{K}[x]$	113
4.2	Der Restklassenring $\mathbb{K}[x]_{m(x)}$	119
4.2.1	Anwendung: Zyklische Codes	124
4.3	Endliche Körper	125
4.3.1	Anwendung: Der Advanced Encryption Standard	128
4.3.2	Anwendung: Reed-Solomon-Codes	128
4.4	Mit dem digitalen Rechenmeister	129
4.5	Kontrollfragen	131
4.6	Übungen	134
5	Relationen und Funktionen	137
5.1	Relationen	137
5.1.1	Anwendung: Relationales Datenmodell	146
5.2	Funktionen	149
5.3	Kontrollfragen	162
5.4	Übungen	166
6	Folgen und Reihen	171
6.1	Folgen	171
6.1.1	Anwendung: Wurzelziehen à la Heron	181
6.2	Reihen	182
6.3	Mit dem digitalen Rechenmeister	188
6.4	Kontrollfragen	190
6.5	Übungen	193
7	Kombinatorik	197
7.1	Grundlegende Abzählverfahren	197
7.2	Permutationen und Kombinationen	201
7.3	Mit dem digitalen Rechenmeister	208
7.4	Kontrollfragen	208
7.5	Übungen	209
8	Rekursionen und Wachstum von Algorithmen	215
8.1	Grundbegriffe	215
8.1.1	Ausblick: Iterationsverfahren und Chaos	219
8.2	Lineare Rekursionen	222
8.2.1	Anwendung: Sparkassenformel	231
8.3	Wachstum von Algorithmen	232
8.4	Mit dem digitalen Rechenmeister	239
8.5	Kontrollfragen	242
8.6	Übungen	244

Lineare Algebra

9	Vektorräume	247
9.1	Vektoren	247
9.2	Lineare Unabhängigkeit und Basis	255
9.3	Teilräume	260
9.4	Mit dem digitalen Rechenmeister	265
9.5	Kontrollfragen	266
9.6	Übungen	268
10	Matrizen und Lineare Abbildungen	273
10.1	Matrizen	273
10.2	Multiplikation von Matrizen	278
10.3	Lineare Abbildungen	285
10.3.1	Anwendung: Lineare Codes	293
10.4	Mit dem digitalen Rechenmeister	296
10.5	Kontrollfragen	298
10.6	Übungen	301
11	Lineare Gleichungen	307
11.1	Der Gauß-Algorithmus	307
11.1.1	Anwendung: Elektrische Netzwerke	315
11.1.2	Anwendung: Input-Output-Analyse nach Leontjef	317
11.2	Rang, Kern, Bild	318
11.3	Determinante	323
11.4	Mit dem digitalen Rechenmeister	328
11.5	Kontrollfragen	329
11.6	Übungen	331
12	Lineare Optimierung	335
12.1	Lineare Ungleichungen	335
12.2	Lineare Optimierung	338
12.3	Der Simplex-Algorithmus	339
12.4	Mit dem digitalen Rechenmeister	345
12.5	Kontrollfragen	347
12.6	Übungen	348
13	Skalarprodukt und Orthogonalität	353
13.1	Skalarprodukt und orthogonale Projektion	353
13.1.1	Anwendung: Matched-Filter	363
13.1.2	Anwendung: Lineare Klassifikation	364
13.1.3	Anwendung: Ray-Tracing	364
13.2	Orthogonalentwicklungen	366
13.3	Orthogonale Transformationen	372
13.3.1	Anwendung: QR-Zerlegung	376
13.4	Mit dem digitalen Rechenmeister	377
13.5	Kontrollfragen	378

13.6	Übungen	380
14	Eigenwerte und Eigenvektoren	383
14.1	Koordinatentransformationen	383
14.2	Eigenwerte und Eigenvektoren	386
14.2.1	Anwendung: Bewertung von Webseiten mit <i>PageRank</i>	395
14.3	Eigenwerte symmetrischer Matrizen	398
14.3.1	Anwendung: Die diskrete Kosinustransformation	401
14.4	Mit dem digitalen Rechenmeister	404
14.5	Kontrollfragen	404
14.6	Übungen	406

Graphentheorie

15	Grundlagen der Graphentheorie	409
15.1	Grundbegriffe	409
15.2	Darstellung von Graphen am Computer	415
15.3	Wege und Kreise	417
15.4	Mit dem digitalen Rechenmeister	425
15.5	Kontrollfragen	426
15.6	Übungen	429
16	Bäume und kürzeste Wege	435
16.1	Bäume	435
16.2	Das Problem des Handlungsreisenden	441
16.2.1	Ausblick: Die Komplexitätsklassen P und NP	443
16.3	Minimale aufspannende Bäume	443
16.4	Kürzeste Wege	446
16.4.1	Anwendung: Routing im Internet	449
16.5	Mit dem digitalen Rechenmeister	450
16.6	Kontrollfragen	451
16.7	Übungen	454
17	Flüsse in Netzwerken und Matchings	459
17.1	Netzwerke	459
17.2	Matchings	467
17.3	Mit dem digitalen Rechenmeister	473
17.4	Kontrollfragen	475
17.5	Übungen	477

Anhang

A	Einführung in Mathematica	483
	A.1 Erste Schritte	483
	A.2 Funktionen	485
	A.3 Gleichungen	487
	A.4 Programme	488
B	Lösungen zu den weiterführenden Aufgaben	491
	B.1 Logik und Mengen	491
	B.2 Zahlenmengen und Zahlensysteme	491
	B.3 Elementare Begriffe der Zahlentheorie	492
	B.4 Polynomringe und endliche Körper	492
	B.5 Relationen und Funktionen	492
	B.6 Folgen und Reihen	493
	B.7 Kombinatorik	493
	B.8 Rekursionen und Wachstum von Algorithmen	493
	B.9 Vektorräume	494
	B.10 Matrizen und Lineare Abbildungen	494
	B.11 Lineare Gleichungen	494
	B.12 Lineare Optimierung	495
	B.13 Skalarprodukt und Orthogonalität	495
	B.14 Eigenwerte und Eigenvektoren	495
	B.15 Grundlagen der Graphentheorie	496
	B.16 Bäume und kürzeste Wege	496
	B.17 Flüsse in Netzwerken und Matchings	497
	Literatur	499
	Verzeichnis der Symbole	501
	Index	503