

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

3. Auflage

 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/>

ISBN 978-3-540-77431-0

e-ISBN 978-3-540-77432-7

DOI 10.1007/978-3-540-77432-7

ISSN 1614-5216

Bibliografische Information der Deutschen Nationalbibliothek

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

© 2008 Springer-Verlag Berlin Heidelberg

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.

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.

*Einbandgestaltung:* KünkelLopka Werbeagentur, Heidelberg

Gedruckt auf säurefreiem Papier

9 8 7 6 5 4 3 2 1

springer.com

---

# 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 Erlernte selbständig umzusetzen. Die Aufwärmübungen trainieren Rechentechniken und es gibt vollständige Lösungen dazu. Die weiterführenden Aufgaben sollen Sie etwas herausfordern und verlangen auch, selbständig 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 „→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/>

eingerrichtet, 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“.

### **Zur dritten Auflage**

In dieser Auflage sind nun alle *Mathematica*-Teile mit der aktuellen Version 6 kompatibel. Weiters haben wir noch einige kleinere Druckfehler und Unklarheiten beseitigt.

### **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 *T<sub>E</sub>X*, *L<sup>A</sup>T<sub>E</sub>X*, *T<sub>E</sub>XShop* 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!

Wien, im Jänner 2008

Gerald und Susanne Teschl



---

# Inhaltsverzeichnis

---

## Grundlagen

---

<b>1</b>	<b>Logik und Mengen</b> .....	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
<b>2</b>	<b>Zahlenmengen und Zahlensysteme</b> .....	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

---

<b>3</b>	<b>Elementare Begriffe der Zahlentheorie</b> .....	73
3.1	Das kleine Einmaleins auf endlichen Mengen .....	73
3.1.1	Anwendung: Hashfunktionen .....	76
3.2	Gruppen, Ringe und Körper .....	79
3.2.1	Anwendung: Welche Fehler erkennen Prüfciffern? .....	89
3.3	Der Euklid'sche Algorithmus und diophantische Gleichungen .....	92
3.3.1	Anwendung: Der RSA-Verschlüsselungsalgorithmus .....	97
3.4	Der Chinesische Restsatz .....	102

3.4.1	Anwendung: Rechnen mit großen Zahlen .....	103
3.4.2	Anwendung: Verteilte Geheimnisse .....	105
3.5	Mit dem digitalen Rechenmeister .....	106
3.6	Kontrollfragen .....	109
3.7	Übungen .....	111
<b>4</b>	<b>Polynomringe und endliche Körper</b> .....	<b>115</b>
4.1	Der Polynomring $\mathbb{K}[x]$ .....	115
4.2	Der Restklassenring $\mathbb{K}[x]_{m(x)}$ .....	121
4.2.1	Anwendung: Zyklische Codes .....	126
4.3	Endliche Körper .....	127
4.3.1	Anwendung: Der Advanced Encryption Standard .....	130
4.3.2	Anwendung: Reed-Solomon-Codes .....	130
4.4	Mit dem digitalen Rechenmeister .....	131
4.5	Kontrollfragen .....	133
4.6	Übungen .....	136
<b>5</b>	<b>Relationen und Funktionen</b> .....	<b>139</b>
5.1	Relationen .....	139
5.1.1	Anwendung: Relationales Datenmodell .....	148
5.2	Funktionen .....	151
5.3	Kontrollfragen .....	164
5.4	Übungen .....	168
<b>6</b>	<b>Folgen und Reihen</b> .....	<b>173</b>
6.1	Folgen .....	173
6.1.1	Anwendung: Wurzelziehen à la Heron .....	183
6.2	Reihen .....	184
6.3	Mit dem digitalen Rechenmeister .....	190
6.4	Kontrollfragen .....	192
6.5	Übungen .....	195
<b>7</b>	<b>Kombinatorik</b> .....	<b>199</b>
7.1	Grundlegende Abzählverfahren .....	199
7.2	Permutationen und Kombinationen .....	203
7.3	Mit dem digitalen Rechenmeister .....	210
7.4	Kontrollfragen .....	210
7.5	Übungen .....	211
<b>8</b>	<b>Rekursionen und Wachstum von Algorithmen</b> .....	<b>217</b>
8.1	Grundbegriffe .....	217
8.1.1	Ausblick: Iterationsverfahren und Chaos .....	221
8.2	Lineare Rekursionen .....	224
8.2.1	Anwendung: Sparkassenformel .....	233
8.3	Wachstum von Algorithmen .....	234
8.4	Mit dem digitalen Rechenmeister .....	241
8.5	Kontrollfragen .....	243
8.6	Übungen .....	246

---

**Lineare Algebra**


---

<b>9</b>	<b>Vektorräume</b>	249
9.1	Vektoren	249
9.2	Lineare Unabhängigkeit und Basis	257
9.3	Teilräume	262
9.4	Mit dem digitalen Rechenmeister	267
9.5	Kontrollfragen	268
9.6	Übungen	270
<b>10</b>	<b>Matrizen und Lineare Abbildungen</b>	275
10.1	Matrizen	275
10.2	Multiplikation von Matrizen	280
10.3	Lineare Abbildungen	287
10.3.1	Anwendung: Lineare Codes	295
10.4	Mit dem digitalen Rechenmeister	298
10.5	Kontrollfragen	300
10.6	Übungen	303
<b>11</b>	<b>Lineare Gleichungen</b>	309
11.1	Der Gauß-Algorithmus	309
11.1.1	Anwendung: Elektrische Netzwerke	317
11.1.2	Anwendung: Input-Output-Analyse nach Leontjef	319
11.2	Rang, Kern, Bild	320
11.3	Determinante	325
11.4	Mit dem digitalen Rechenmeister	330
11.5	Kontrollfragen	331
11.6	Übungen	333
<b>12</b>	<b>Lineare Optimierung</b>	337
12.1	Lineare Ungleichungen	337
12.2	Lineare Optimierung	340
12.3	Der Simplex-Algorithmus	341
12.4	Mit dem digitalen Rechenmeister	347
12.5	Kontrollfragen	349
12.6	Übungen	350
<b>13</b>	<b>Skalarprodukt und Orthogonalität</b>	355
13.1	Skalarprodukt und orthogonale Projektion	355
13.1.1	Anwendung: Matched-Filter	365
13.1.2	Anwendung: Lineare Klassifikation	366
13.1.3	Anwendung: Ray-Tracing	366
13.2	Orthogonalentwicklungen	368
13.3	Orthogonale Transformationen	374
13.3.1	Anwendung: QR-Zerlegung	378
13.4	Mit dem digitalen Rechenmeister	379
13.5	Kontrollfragen	380

13.6	Übungen	382
<b>14</b>	<b>Eigenwerte und Eigenvektoren</b>	385
14.1	Koordinatentransformationen	385
14.2	Eigenwerte und Eigenvektoren	388
14.2.1	Anwendung: Bewertung von Webseiten mit <i>PageRank</i>	397
14.3	Eigenwerte symmetrischer Matrizen	400
14.3.1	Anwendung: Die diskrete Kosinustransformation	403
14.4	Mit dem digitalen Rechenmeister	406
14.5	Kontrollfragen	406
14.6	Übungen	408

## Graphentheorie

<b>15</b>	<b>Grundlagen der Graphentheorie</b>	411
15.1	Grundbegriffe	411
15.2	Darstellung von Graphen am Computer	417
15.3	Wege und Kreise	419
15.4	Mit dem digitalen Rechenmeister	427
15.5	Kontrollfragen	428
15.6	Übungen	431
<b>16</b>	<b>Bäume und kürzeste Wege</b>	437
16.1	Bäume	437
16.2	Das Problem des Handlungsreisenden	443
16.2.1	Ausblick: Die Komplexitätsklassen $P$ und $NP$	445
16.3	Minimale aufspannende Bäume	445
16.4	Kürzeste Wege	448
16.4.1	Anwendung: Routing im Internet	451
16.5	Mit dem digitalen Rechenmeister	452
16.6	Kontrollfragen	453
16.7	Übungen	457
<b>17</b>	<b>Flüsse in Netzwerken und Matchings</b>	463
17.1	Netzwerke	463
17.2	Matchings	471
17.3	Mit dem digitalen Rechenmeister	477
17.4	Kontrollfragen	479
17.5	Übungen	481

## Anhang

<b>A</b>	<b>Einführung in Mathematica</b> .....	487
	A.1 Erste Schritte .....	487
	A.2 Funktionen .....	489
	A.3 Gleichungen .....	491
	A.4 Programme .....	492
<b>B</b>	<b>Lösungen zu den weiterführenden Aufgaben</b> .....	495
	B.1 Logik und Mengen .....	495
	B.2 Zahlenmengen und Zahlensysteme .....	495
	B.3 Elementare Begriffe der Zahlentheorie .....	496
	B.4 Polynomringe und endliche Körper .....	496
	B.5 Relationen und Funktionen .....	496
	B.6 Folgen und Reihen .....	497
	B.7 Kombinatorik .....	497
	B.8 Rekursionen und Wachstum von Algorithmen .....	497
	B.9 Vektorräume .....	498
	B.10 Matrizen und Lineare Abbildungen .....	498
	B.11 Lineare Gleichungen .....	498
	B.12 Lineare Optimierung .....	499
	B.13 Skalarprodukt und Orthogonalität .....	499
	B.14 Eigenwerte und Eigenvektoren .....	499
	B.15 Grundlagen der Graphentheorie .....	500
	B.16 Bäume und kürzeste Wege .....	500
	B.17 Flüsse in Netzwerken und Matchings .....	501
	<b>Literatur</b> .....	503
	<b>Verzeichnis der Symbole</b> .....	505
	<b>Index</b> .....	507