

Jörg R. Mühlbacher  
Günter Pilz  
Marcel Widi

# Mathematik *explorativ*

Ausgewählte Kapitel der  
Algebra, Zahlentheorie und Graphentheorie  
für Anwendungen in der Informatik

Universitätsverlag Rudolf Trauner

<b>Vorwort</b> .....	<b>9</b>
<b>1. Mengen, Zahlen, Relationen und Funktionen</b> .....	<b>11</b>
1.1. Mengen.....	11
1.2. Natürliche Zahlen.....	16
1.3. Ganze Zahlen.....	19
1.4. Rationale Zahlen.....	23
1.5. Reelle Zahlen.....	25
1.6. Komplexe Zahlen.....	27
1.7. Zahlendarstellung in digitalen Rechenanlagen.....	29
1.7.1. Darstellung von ganzen Zahlen.....	29
1.7.2. Darstellung von rationalen und reellen Zahlen.....	31
1.8. Kombinatorik.....	34
1.9. Relationen und Funktionen.....	37
1.10. Übungsaufgaben.....	43
1.11. Applets.....	44
<b>2. Elementare Zahlentheorie</b> .....	<b>45</b>
2.1. Der größte gemeinsame Teiler.....	45
2.2. Primzahlen.....	48
2.3. Lineare diophantische Gleichungen.....	51
2.4. Kongruenzen und Restklassensysteme.....	52
2.4.1. Kongruenzen.....	52
2.4.2. Restklassensysteme.....	54
2.4.3. Simultane Kongruenzen.....	57
2.4.4. Quadratreste.....	58
2.5. Übungsaufgaben.....	61
2.6. Applets.....	62
<b>3. Analytische Geometrie</b> .....	<b>63</b>
3.1. Koordinatensysteme und Vektoren.....	63
3.2. Vektoren.....	64
3.2.1. Addition und Subtraktion.....	66
3.2.2. Skalarprodukt.....	68
3.3. Die Gerade in der Ebene.....	73
3.3.1. Geradengleichungen.....	73
3.3.2. Gerade und Vektoren.....	75
3.3.3. Hesse'sche Normalform.....	80
3.4. Das Vektorprodukt und seine geometrische Deutung im Raum.....	82
3.4.1. Eigenschaften.....	82
3.4.2. Anwendungen.....	83
3.5. Gerade und Ebene im Raum.....	87
3.5.1. Geradengleichungen.....	87
3.5.2. Ebengleichungen.....	87
3.6. Übungsaufgaben.....	89
3.7. Applets.....	90

<b>4.</b>	<b><i>Algebraische Strukturen</i></b> .....	<b>91</b>
4.1.	Vorbemerkungen.....	91
4.2.	Gruppen.....	92
4.2.1.	Definitionen.....	92
4.2.2.	Beispiele.....	94
4.3.	Untergruppen.....	98
4.3.1.	Definitionen.....	98
4.3.2.	Zyklische Gruppen.....	99
4.3.3.	Nebenklassen und Normalteiler.....	102
4.3.4.	Isomorphie von Gruppen.....	105
4.4.	Ringe und Körper.....	107
4.4.1.	Ringe.....	107
4.4.2.	Körper.....	108
4.5.	Polynome.....	110
4.5.1.	Polynome über einem Körper.....	110
4.5.2.	Rechnen mit Polynomen.....	111
4.5.3.	Nullstellen.....	115
4.6.	Endliche Körper.....	119
4.6.1.	Vorbemerkungen.....	119
4.6.2.	Die Konstruktion von endlichen Körpern.....	119
4.6.3.	Eigenschaften endlicher Körper.....	121
4.7.	Übungsaufgaben.....	122
4.8.	Applets.....	123
<b>5.</b>	<b><i>Vektorräume</i></b> .....	<b>125</b>
5.1.	Grundlagen.....	125
5.2.	Unterräume.....	129
5.3.	Lineare Abhängigkeit.....	134
5.4.	Basen.....	137
5.5.	Übungsaufgaben.....	140
<b>6.</b>	<b><i>Matrizen</i></b> .....	<b>143</b>
6.1.	Einführung und Definitionen.....	143
6.2.	Das Matrixprodukt.....	147
6.3.	Matrizen und lineare Gleichungssysteme.....	149
6.4.	Die inverse Matrix.....	151
6.5.	Invertierbarkeit von Matrizen und Lösbarkeit von linearen Gleichungssystemen 153	
6.6.	Das Gauß'sche Eliminationsverfahren.....	155
6.7.	Übungsaufgaben.....	160
6.8.	Applets.....	161
<b>7.</b>	<b><i>Determinanten</i></b> .....	<b>163</b>
7.1.	Einleitung und Definitionen.....	163
7.2.	Die Cramer'sche Regel.....	171
7.3.	Eigenwerte.....	173
7.4.	Übungsaufgaben.....	176
7.5.	Applets.....	177

<b>8.</b>	<b><i>Graphentheorie</i></b>	<b>179</b>
8.1.	Vorbemerkung	179
8.2.	Ungerichtete Graphen	180
8.2.1.	Elementare Definitionen	180
8.2.2.	Zusammenhang und Komponenten	183
8.2.3.	Artikulationen und Brücken	184
8.2.4.	Bäume	187
8.3.	Gerichtete Graphen	189
8.3.1.	Zusammenhang und Komponenten	189
8.3.2.	Arboreszenzen	192
8.4.	Spannende Bäume	194
8.4.1.	Definitionen und Einführung	194
8.4.2.	Minimalgerüst	195
8.4.3.	Kürzeste Wege	197
8.5.	Wichtige Baumklassen	199
8.5.1.	Binäre Bäume	199
8.5.2.	Suchbäume	202
8.5.3.	Fibonacci Bäume	205
8.5.4.	Balanzierte Bäume	209
8.5.5.	B-Bäume	210
8.6.	Weitere Graphenklassen	212
8.7.	Petrinetze	218
8.7.1.	Einführung	218
8.7.2.	Definitionen	219
8.8.	Transportnetze	222
8.9.	Matching	227
8.10.	Übungsaufgaben	230
8.11.	Applets	231
<b>9.</b>	<b><i>Grundkonzepte der Automatentheorie</i></b>	<b>233</b>
9.1.	Alphabete und Sprachen	233
9.2.	Endliche Automaten	235
9.3.	Übungsaufgaben	241
9.4.	Applet	241
<b>10.</b>	<b><i>Codierungstheorie</i></b>	<b>243</b>
10.1.	Allgemeines	243
10.2.	Übungsaufgaben	256
<b>11.</b>	<b><i>Ausgewählte Anwendungen</i></b>	<b>257</b>
11.1.	Vorbemerkungen	257
11.2.	Speicherung von Dreiecksmatrizen	257
11.3.	Erzeugung von Zufallszahlen	258
11.4.	Speichern und Suchen in Tabellen mittels Hashfunktionen	261
11.4.1.	Aufgabenstellung	261
11.4.2.	Kollisionsstrategien	262
11.5.	Berechnung ganzzahliger Potenzen	264

11.6.	Kryptographische Hashfunktionen.....	265
11.6.1.	Fragestellung.....	265
11.6.2.	Beispiele für kryptographische Hashfunktionen.....	266
11.6.3.	Speichern von Passwörtern.....	267
11.7.	Asymmetrische Verschlüsselung.....	269
11.8.	Schlüsselaustausch über unsicheren Kanal.....	271
11.9.	Breitensuche in einem Graphen.....	273
11.10.	Fluten und Link-State Routing in einem Netzwerk.....	275
11.11.	Maximaler Fluss und Matching in paaren Graphen.....	278
11.12.	Huffman Code.....	279
11.13.	Halden.....	281
11.14.	Organisation von großen Datenmengen mit B-Bäumen.....	285
11.15.	CRC Codes in der Praxis.....	288
11.16.	Eigenwerte und Potenzen von Matrizen.....	291
11.17.	Bewertung von Web-Seiten.....	293
11.18.	Anwendung von Matrizen in der Computergrafik.....	297
11.19.	Applets.....	302
<b>12.</b>	<b>Lösungen zu den Übungsaufgaben.....</b>	<b>303</b>
12.1.	Zahlen, Relationen und Funktionen.....	303
12.2.	Elementare Zahlentheorie.....	308
12.3.	Analytische Geometrie.....	311
12.4.	Algebraische Strukturen.....	315
12.5.	Vektorräume.....	319
12.6.	Matrizen.....	322
12.7.	Determinanten.....	324
12.8.	Graphentheorie.....	328
12.9.	Grundkonzepte der Automatentheorie.....	330
12.10.	Codierungstheorie.....	331
<b>13.</b>	<b>Literatur.....</b>	<b>333</b>
	Allgemeine.....	333
	Zahlentheorie.....	333
	Analytische Geometrie.....	333
	Algebra 334	
	Graphentheorie.....	334
	Spezielle Literatur zu den Anwendungen.....	335
<b>14.</b>	<b>Index.....</b>	<b>337</b>

## Vorwort

Die Informatik als Ingenieurwissenschaft basiert letztlich immer auf mathematischen Grundlagen. Neben der Analysis sind für viele Anwendungen insbesondere Algebra, Zahlentheorie und Graphentheorie wichtig. Einer Auswahl von Themen aus diesen drei letztgenannten Fächern ist dieses Buch gewidmet.

Zur Motivation, sich zu Beginn eines Studiums der Informatik mit der abstrakten mathematischen Welt auseinanderzusetzen, ist ein umfangreiches Kapitel mit ausgewählten Beispielen enthalten, denen Studierende im Laufe ihres Studiums in Fächern wie z. B. Algorithmen- und Datenstrukturen, Computergraphik, Kryptographie, Modellierung, Codierungstheorie und Computernetzwerke in nahezu jedem informatiknahen Curriculum begegnen. Naturgemäß kann eine solche Auswahl aber nur unvollständig bleiben.

Der Text ist aus didaktischer Sicht gleichsam untrennbar mit einer Sammlung von JAVA-Applets auf der beigefügten CD-ROM verbunden. Mit dieser soll selbstgesteuertes exploratives Lernen gefördert werden, wobei – soweit es in Zahlentheorie und abstrakter Algebra möglich ist – auf die Kraft der Visualisierung und der Interaktion gesetzt wird.

Das Buch ist nicht nur als Begleitmaterial zu herkömmlichen Lehrveranstaltungen, sondern insbesondere für ein Studium im Rahmen von E-Learning gedacht, wobei in diesem Fall für die Gestaltung des Unterrichtes „Blended Learning“ als pädagogisches Modell empfohlen wird.

Aus technischer Sicht ist das Lernmaterial entsprechend der IMS Content Packaging Specification als CPS-Paket ausgelegt, sodass es auch online angeboten werden kann: Moderne E-Learning Plattformen wie WeLearn unterstützen dieses Format.

Angesprochen sind Studierende der Informatik (Bakkalaureat, Universitäten und Fachhochschulen), die im Rahmen der zugehörigen Mathematikausbildung je nach fachlichem Schwerpunkt ihres Studiums jedenfalls mit einem Großteil des vorgestellten Stoffes vertraut werden sollten.

Da die Eingangsvoraussetzungen der Studierenden im Allgemeinen unterschiedlich sind und nicht immer eine Mathematikvorbildung im Umfang einer Matura (Abitur) vorausgesetzt werden kann, sind zur Erleichterung des Einstieges ein Kapitel über Mengen, Zahlen, Relationen und Funktionen sowie ein Kapitel über Analytische Geometrie vorgesehen.

Das Manuskript stammt aus einer Zusammenarbeit zwischen dem Institut für Algebra (Prof. Dr. Günter Pilz, Dipl. Ing. Marcel Widi) und dem Institut FIM unter Leitung von Prof. Dr. Jörg R. Mühlbacher.

Herr M.Sc. Alexandros Paramythis (FIM) entwickelte das Framework, in das die Applets eingebettet sind, sodass eine gemeinsame Bedienungsfläche geschaffen wird. Zur Spezifikation und Implementierung der Applets haben neben Jörg R. Mühlbacher noch Bernhard Niedermayer, Markus Pflieger, Christian Praher und Peter Zehetner im Rahmen von Bakkalaureatsarbeiten mitgearbeitet.

Ein besonderer Dank gilt Frau Dr. Gisela Razen, die Teile des Manuskriptes kritisch gelesen und viele Anregungen eingebracht hat, Herrn Dipl.Ing. Andreas Putzinger (FIM) für die Unterstützung beim Erstellen der CD-ROM, sowie Frau Ingeborg Ritzinger für die Niederschrift des Manuskriptes.

Ferner sei der Johannes Kepler Universität Linz (JKU) gedankt, von deren E-Learning Initiative das Projekt seinen Ausgang nahm und unterstützt wurde.

Laufende Updates zum Buch und zu den Applets sowie Errata können unter folgender URL eingesehen werden: <http://www.fim.at/mathe-explorativ>

Linz, im August 2006

Jörg R. Mühlbacher  
Günter Pilz  
Marcel Widi

## 13. Literatur

### *Allgemeine*

- W. Dörfler, W. Peschek: Einführung in die Mathematik für Informatiker  
C. Hanser-Verlag, 1988  
ISBN: 34 46 15 11 25
- P. Hartmann: Mathematik für Informatiker  
Vieweg-Verlag, 2006, 4. Auflage  
ISBN: 38 34 80 09 61
- E. Zeidler (Hrsg.): Teubner-Taschenbuch der Mathematik  
B. G. Teubner-Verlag, 2003, 2. Auflage  
ISBN: 35 19 20 01 20

### *Zahlentheorie*

- H. Hasse: Vorlesungen über Zahlentheorie  
Grundlehren der Mathematischen Wissenschaften Bd. 59  
Springer-Verlag, 1964  
ISBN: B 0000 BJ 4K9
- G.H. Hardy, E.M. Wright: An Introduction to the Theory of Numbers  
Clarendon Press Oxford, 1980, 5. Auflage  
deutsche Übersetzung: Oldenbourg-Verlag, 1958  
ISBN: 01 98 53 17 10
- R. Remmert, P. Ullrich: Elementare Zahlentheorie  
Birkhäuser-Verlag, 1995, 2. Auflage  
ISBN: 37 64 35 19 77

### *Analytische Geometrie*

- E. Barth, F. Barth, G. Krumbacher: Anschauliche Analytische Geometrie  
Oldenbourg, 2000, 4. Auflage  
ISBN: 34 86 03 02 3X
- M. Koecher: Lineare Algebra und Geometrie  
Springer-Verlag, 1997, 4. Auflage  
ISBN: 35 40 62 90 33



**Algebra**

- A. Fischer, W. Schirotzek, K. Veters: Lineare Algebra. Eine Einführung für Ingenieure und Naturwissenschaftler  
Teubner-Verlag, 2003  
ISBN: 35 19 00 37 08
- G. Pilz: Endliche Strukturen  
Trauner-Verlag, 1988  
ISBN: 38 53 20 42 87
- K.H. Spindler: Abstract Algebra with Applications (2 Bände)  
Marcel Dekker, New York, 1994  
ISBN: 0-8247-9144-4  
ISBN: 0-8247-9159-2
- B. Huppert: Lineare Algebra  
Teubner, 2006  
ISBN: 38 35 10 08 90
- R. Lidl, G. Pilz: Applied Abstract Algebra  
Springer, New York, 2<sup>nd</sup> Edition, 1998  
ISBN: 0-387-98290-6
- A. V. Mikhalev, G. Pilz: The Concise Handbook of Algebra  
Kluwer, Dordrecht, 2002  
ISBN: 0-7923-7072-4

**Graphentheorie**

- M. Aigner: Diskrete Mathematik  
Vieweg-Verlag, 2004, 5. Auflage  
ISBN: 35 28 47 26 85
- R. Diestel: Graphentheorie  
Springer-Verlag, 2006, 3. Auflage  
ISBN: 35 40 21 39 10
- W. Dörfler, J. Mühlbacher: Graphentheorie für Informatiker  
Walter de Gruyter, Göschen Band 6016, 1973  
ISBN: 3 11 003946 X
- G. Pilz: Endliche Strukturen  
Trauner-Verlag, 1988  
ISBN: 38 53 20 42 87

## *Spezielle Literatur zu den Anwendungen*

- D.E. Knuth: The Art of Computer Programming  
Vol 2: Seminumerical Algorithms, 3rd Edition, Addison Wesley, Reading, MA, 1997  
ISBN: 0-201-89684-2.
- T.Ottmann, P.Widmayer: Algorithmen und Datenstrukturen  
4. Auflage, Spektrum Verlag, 2002  
ISBN: 3-8274-1029-0
- J.R. Mühlbacher:  
Full Hash Table Search using Primitive Roots of the Prime Residue Group  $Z/p$ ;  
Journal of Universal Computer Science, Vol.10 (2004), Issue 9, pp. 1239-1249
- D. R.Stinson: Cryptography, Theorie and Praxis  
CRC Press LLC, 1995  
ISBN: 0-8493-8531-0
- W.Diffie, M.E. Hellman: Multiuser Cryptographic Techniques  
Proc. of AFIPS National Computer Conference, 1976, 109-112
- B.Schneier: Angewandte Kryptographie  
Addison Wesley, 1996  
ISBN: 3-89319-854-7 bzw.  
Applied Cryptography, 1996  
ISBN: 0-471-11709-9
- R. R. Jueneman, S. M. Matyas, C. H. Meyer: Message Authentication with Manipulation  
Detection Codes  
Proc. IEEE Symposium on Research in Security and Privacy, 733-754, 1983
- R-L.Rivest, A.Shamir, L.M.Adleman: A Method for Obtaining Digital Signatures and Public-  
Key Cryptosystems  
CAMCM, Vol 21, Nr 2, 1978, 120-128
- R.Sedgewick: Algorithms  
Addison Wesley, 1988  
ISBN: 0-201-06673-4 bzw.  
Algorithmen, Pearson Studium  
ISBN: 3-8273-7032-9
- J.F.Kurose, K.W.Ross: Computer Networking: A top down Approach featuring the Internet  
Addison Wesley Longman, 2001, bzw.  
Computernetze, ein Top Down Ansatz mit Schwerpunkt Internet  
Pearson Studium 2002  
ISBN: 3-8273-7017-5

- A.S. Tanenbaum: Computer Networks  
4<sup>th</sup> Ed., Pearson Education Inc, 2003  
ISBN: 0-13-038488-7, bzw.  
Computernetzwerke, Pearson Studium, 2003  
ISBN: 3-8273-7011-6
- Z.Galil: Efficient Algorithms for finding Maximum Matching in Graphs  
ACM Computing Surveya, Vol 18, Nr. 1, 1986
- D.A.Huffman: A method for the construction of minimum – redundancy codes  
Proceedings of the IERE, 40,1098-1101, 1952
- R.W. Floyd: Treesort  
CACM Vol 7, Nr.12, pg 701, 1964
- R.Bayer, E. McCreight: Organization and Maintenance of Large Ordered Indexes  
Acta Informatica, 1, 1972, 173-189
- S. Brin, L.Page: The Anatomy of a Large-Scale Hypertextual Web Search Engine  
Computer Networks and ISDN Systems, 30, 107-11, 1998
- J. Encarnação, W. Straßer , R. Klein: Graphische Datenverarbeitung I  
R. Oldenbourg Verlag, 1996  
ISBN: 3-486-23223-1

## 14. Index

A	C		
Abszisse.....	63	Carl Adam Petri .....	218
Additionsregeln .....	19	Carl Friedrich Gauß .....	57, 155
adjazent.....	180	charakteristische Gleichung.....	173
Adjazenzmatrix .....	257	charakteristisches Polynom .....	173
Algebraische Strukturen.....	91	Chinesischer Restsatz .....	57
allgemeine Geradengleichung .....	74	Cliquenproblem .....	213
Alphabet .....	233	Code.....	243
alternierender Weg .....	228	Codewörter .....	247
Analytische Geometrie .....	63	Codierungs-Algorithmus .....	251
antisymmetrisch .....	37	Codierungstheorie.....	243
Arboreszenzen .....	192	Cosinus-Satz .....	69
array.....	257	Cramer'schen Regel.....	165
Artikulation .....	184	Cramer'schen Regel.....	171
assoziativ .....	92	CRC Codes in der Praxis .....	288
Assoziativgesetz.....	13, 66	cut .....	225
Asymmetrische Verschlüsselung .....	269	Cyclic Redundancy Check.....	251
Austauschsatz von Steinitz.....	138	Cyclic Redundancy Code .....	112
Automatentheorie .....	233		
azyklischer Graph.....	192	D	
B		David A. Huffman .....	279
b-adische Darstellung.....	29	DEA .....	236
Balance .....	193	Decodierung.....	247
Balanzierte Bäume .....	209	Definitionsbereich.....	38
Basen .....	137	Determinante.....	75, 163
Bäume.....	187	deterministischer endlicher Automat....	236
B-Bäume.....	210	Diagonalisierbarkeit.....	291
Bertrand Russel .....	15	Diagonalmatrix .....	145
bewerteten Graphen.....	195	Differenz .....	12
Bewertung von Web-Seiten .....	293	Diffie-Hellman-Verfahren .....	271
bijektiv.....	40	Diophantos von Alexandria .....	51
Bildbereich .....	38	Diskrete Fourier-Transformation.....	255
binäre Arboreszenz.....	192	diskreter Logarithmus.....	271
Binäre Bäume .....	199	Distributivgesetz.....	13
binäre Codes.....	247	dominanter Eigenwert.....	173
binäre Relation .....	92	Doppelfehler .....	244
Binet'schen Formel .....	208	Dreiecksmatrizen .....	145, 257
Binomialkoeffizient.....	34	Dreipunktform .....	87
Binomialverteilung.....	35	Durchschnitt.....	12
bipartiter Graph .....	218		
Blatt .....	199	E	
Block .....	185	Ebene .....	63
Breitensuche (BSF) .....	273	Ebengleichungen.....	87
Brücke .....	186	EBNF .....	234
BSF-Verfahren .....	273	Eigenvektor.....	173
		Eigenwerte .....	173
		Einfachfehler.....	244
		Einheitsmatrix.....	145

Einwegfunktion .....	265
Elementare Zahlentheorie .....	45
Endknoten.....	181
Endliche Automaten.....	235
endliche Gruppen .....	94
Endliche Körper .....	119
Ergiebigkeit.....	222
erweiternder Weg.....	228
erweiterte Koeffizientenmatrix .....	149
erzeugendes Element.....	100
Erzeugung von Zufallszahlen.....	258
Euklid's erstes Theorem.....	48
Euklid'sche Algorithmus.....	46
Euler'sche Kriterium.....	60
Euler'sche Polyederformel.....	217
Euler-Graph.....	214
Eulersche $\varphi$ -Funktion.....	56
Eulertour.....	214
Euler-Venn-Diagramme .....	12
Evariste Galois .....	109
Exponentiation .....	266

## F

Faktorgruppe .....	104
Faktorraum .....	131
Fakultät.....	34
Fano-Bedingung.....	279
Fehler-Burst.....	244
fehlererkennende Codes .....	245
fehlerkorrigierende Codes .....	245
Fehlstelle .....	169
Fermat'sche Primzahlen.....	50
Fibonacci Bäume.....	205
Flooding .....	275
Fluten.....	275
Ford - Fulkerson.....	225
freies Monoid .....	243
Fundamentallemma der Zahlentheorie.....	47
Fundamentalsatz der Algebra.....	118
Funktionen.....	37

## G

G. Fano .....	279
Gabriel Cramer.....	171
Galois-Feld.....	109
Galoisfeld der Ordnung $p^n$ .....	119
Ganze Zahlen.....	19
Ganzzahlige Potenzen .....	264
ganzzahliger Fluss $\Phi$ .....	222
Gauß'sches Eliminationsverfahren .....	155
gemeinsamer Teiler.....	45
gemeinsames Vielfaches .....	46

Generator .....	100
geordnetes Paar.....	14
Georg Cantor .....	11
Gerade im Raum.....	87
Gerade in der Ebene.....	73
Gerade und Vektoren.....	75
Geradengleichungen .....	73, 87
Gerichtete Graphen.....	189
gerichtete Wurzelbäume .....	192
Gerüst.....	188, 194
gesättigter Teilgraph.....	185
Gleichungssystem Lösbarkeit .....	153
Graphentheorie .....	179
größter gemeinsame Teiler .....	45
Gruppen .....	92
Gruppenhomomorphismus .....	106
Gruppenisomorphismus.....	106
Gruppentafel .....	94

## H

Halbgruppe .....	92
halboffenes Intervall.....	11
Halde.....	281
Hamilton, William Rowan.....	215
Hamilton'sche Linien .....	215
Hamming-Code.....	249
Hamming-Distanz.....	247
Hamming-Gewicht .....	249
Hashfunktionen.....	261, 265
Hauptdiagonale.....	143
Hauptsatz der elementaren Zahlentheorie .....	48
Hauptsatz über den ggT .....	47
Hauptsatz über simultane Kongruenzen .....	57
Hausadresse .....	261
Heap.....	281
Heap-Sort.....	284
Hesse'sche Abstandsformel.....	80
Hesse'sche Normalform .....	80
Hintereinanderausführung .....	42
Höhe eines Baumes.....	201
homogen .....	149
homogene Koordinaten.....	299
Homomorphismus.....	106
Hop .....	275
Huffman Code .....	279

## I

Idempotenzgesetze.....	13
Imaginärteil.....	27
Index .....	104

Induktion .....	17	Korrekturrate.....	251
Informationsrate .....	251	Kosten einer Kante .....	197
inhomogen .....	149	Kreis.....	182
injektiv.....	40	Kriterium von Euler.....	60
Inneres Produkt .....	68	Kronecker-Symbol.....	146
Integritätsbereich.....	108	Kryptographische Hashfunktionen.....	265
inverse Matrix .....	151	Kürzeste Wege.....	197
inverse Relation.....	37		
invertierbar .....	153	<b>L</b>	
Invertierbarkeit von Matrizen.....	153	Lagrange .....	99, 104
inzident.....	180	Länge einer Kante.....	197
irrationale Zahl .....	25	Laplace'scher Entwicklungssatz... 164, 169	
irreduzibel.....	113	laufender Punkt.....	73
isolierter Knoten.....	181	least significant.....	29
isomorph.....	180	Leonhard Euler .....	214
Isomorphie von Gruppen.....	105	Leopold Kronecker .....	146
<b>J</b>		linear .....	110
Joseph-Luis Lagrange .....	99	lineare Abhängigkeit.....	79, 134
<b>K</b>		lineare diophantische Gleichungen.....	51
kanonische Zerlegung .....	49	lineare Gleichungssysteme .....	149
Kanten .....	180	lineare Hülle.....	134
Kantenfolge.....	190	lineare Kollisionsstrategie .....	262
Kantenzug.....	181	lineare Kongruenz.....	58
Kapazität.....	225	lineare Kongruenzmethode.....	259
kartesisches Koordinatensystem .....	63	lineare Mannigfaltigkeit.....	132
kartesisches Produkt.....	14	lineare Unabhängigkeit.....	79
k-Clique.....	213	linearer Code.....	247
Kleinsche Vierergruppe.....	98	linearer Raum.....	125
kleinstes gemeinsame Vielfache .....	46	Link-Matrix.....	295
Knotenüberdeckung .....	213	Linksnebenklasse.....	103
Koeffizientenmatrix .....	149	Link-State Routing.....	275
Kollisionsstrategie.....	261	Link-State-Verfahren.....	277
Kollisionsstrategien.....	262	Lösbarkeit von linearen	
Kombinatorik .....	34	Gleichungssystemen .....	153
kommutativer Ring.....	108	<b>M</b>	
Kommutativgesetz.....	13, 67	m Fakultät .....	97
Komplement.....	12	Marin Mersenne.....	50
komplementärer Graph.....	212	Markierung .....	218
komplementärer Teiler .....	22	Matching .....	227
Komplexe Zahlen .....	27	Matching in paaren Graphen .....	278
Komponente .....	183	Matrixprodukt.....	147
Kongruenzen .....	52	Matrizen.....	143
Königsberger Brückenproblem .....	214	Matrizen in der Computergrafik.....	297
konjugiert komplexe Zahl .....	27	Max- Flow-Min-Cut Theorem.....	225
Konkatenation .....	93	Maximaler Fluss in paaren Graphen.....	278
Konstruktion von endlichen Körpern... 119		maximales Matching.....	228
Kontrollmatrix.....	247	Mehrfachkante .....	189
Koordinatenachsen .....	63	Menge .....	11
Koordinatensysteme .....	63	Mersenne'schen Primzahlen.....	50
Körper.....	108	Metrik .....	247
		Minimaldistanz .....	248

Minimalgerüst .....	195
Monoid .....	93
Multiplikation von Permutationen .....	96
Multiplikationsregeln .....	19
<b>N</b>	
Nächste-Nachbar-Decodierung .....	248
Natürliche Zahlen .....	16
Nebenklassen .....	102
neutrales Element .....	92
neutrales Element in der Gruppe .....	127
n-fach Fehler .....	244
nicht-regulär .....	151
Niveau .....	193
Norm .....	69
Normalform der Geradengleichung .....	74
Normalteiler .....	102, 103
Normalvektorform .....	87
Normierung .....	157
n-ter Potenzrest modulo m .....	58
n-Tupel .....	14
Nullmatrix .....	20, 145
Nullpolynom .....	110
Nullraum .....	153
Nullstellen .....	115
Nullteiler .....	20
Nullvektor .....	67, 126
<b>O</b>	
offenes Hashcoding .....	261
offenes Intervall .....	11
Ordinate .....	63
Ordnung der Gruppe .....	94
Ordnungsrelation .....	38
<b>P</b>	
paarer Graph .....	329
PageRank Algorithmus .....	293
PageRanks .....	295
parallel .....	75
Parameterform .....	87
Peano'sche Axiome .....	16
Permutation .....	96
Petrinetze .....	218
Pierre de Fermat .....	50
Pierre F. Sarrus .....	164
planarer Graph .....	216
plättbarer Graph .....	216
Polar(koordinaten)darstellung .....	28
Polynome .....	110
Polynome über einem Körper .....	110
Polynomfunktionen .....	110
Potenzen von Matrizen .....	291
Potenzmenge .....	15
Präfixeigenschaft .....	279
prime Restklassen mod m .....	55
primitives Element mod m .....	260
Primitivwurzel .....	101, 260
Primzahlen .....	48
Priority Queue .....	282
Projektion eines Vektors .....	72
Protokoll .....	275
Pseudozufallszahlen .....	258
Punktrichtungsform .....	75, 87
Punktrichtungsgleichung .....	73
<b>Q</b>	
quadratisch .....	110
quadratische Matrix .....	143
Quadratrest .....	58, 262
Quelle .....	222
<b>R</b>	
Rationale Zahlen .....	23
Rechenregeln für Teiler .....	22
Rechnen mit Polynomen .....	111
Rechtsnebenklasse .....	103
reduzibel .....	113
Reed-Solomon Code .....	254
Reelle Zahlen .....	25
reflexiv .....	37
Regeln für die Ordnung .....	20
Regeln von Sarrus .....	164
regulär .....	151
Relationen .....	37
Restklassensysteme .....	54
Ringe .....	107
Rotation .....	299
Routing-Tabelle .....	277
RSA Verfahren .....	50, 269
Rückwärtselimination .....	156
Rundreiseproblem .....	216
<b>S</b>	
Satz von Pythagoras .....	25
schalten im Petrinetz .....	218
schlichter Graph .....	257
Schlingen .....	189, 257
Schlüsselaustausch .....	271
Schnitt (cut) .....	225
schwach kollisionsresistent .....	265
Sekundärkollisionen .....	261
Senke .....	222
separabel .....	184

Sieb des Eratosthenes von Kyrene .....	49
Signatur .....	169
Simultane Kongruenzen .....	57
Single-Parity-Check .....	244
singulär .....	151
Skalar .....	68
Skalarprodukt .....	68
Skalierung .....	298
Spaltenvektoren .....	126
spannender Baum .....	188, 194
Speicherabbildungsfunktion .....	261
Speichern mit Hashfunktionen .....	261
Speichern von Passwörtern .....	267
Speicherung von Dreiecksmatrizen .....	257
Sprache .....	233
Square – and – Multiply-Methode .....	264
stark kollisionsresistent .....	265
stark zusammenhängend .....	190
starke Komponente .....	190
State Diagram .....	237
Suchbaum .....	202
Suchen mit Hashfunktionen .....	261
Summenformel .....	17
surjektiv .....	40
symmetrisch .....	37
symmetrische Differenz .....	12
symmetrische Verschlüsselung .....	269
<b>T</b>	
Teiler des Polynoms $p$ .....	113
Teilmenge .....	12
Token .....	218
Transitionen .....	218
transitiv .....	37
Transitivitätsgesetz .....	20
Translationsvektor .....	297
transponierte Matrix .....	144
Transportnetze .....	222
Travelling Salesman Problem .....	216
Tripel .....	14
<b>U</b>	
Übergangsfunktion .....	236
Übergangsrelation .....	236
unendliche Gruppen .....	94
Ungerichtete Graphen .....	180
Untergruppen .....	98
Untergruppenkriterium .....	98
Unterräume .....	129
Ursprung .....	63
<b>V</b>	
Variation .....	36
Vektoren .....	64
vektorielles Produkt .....	69, 82
Vektorräume .....	125
Vereinigung .....	12
Verschlüsselung .....	266, 269
Verschmelzungsgesetze .....	13
Vielfachheit der Nullstelle .....	116
Vollständige Induktion .....	17
vollständige symmetrische Gruppe .....	97
vollständiges Restsystem mod $m$ .....	54
Vorrangwarteschlange .....	282
Vorwärtselimination .....	156
<b>W</b>	
Wald .....	187
Weg .....	181
Wort .....	233
Wortmonoid .....	93, 243
Wurzel .....	199
<b>X</b>	
x-Achse .....	63
<b>Y</b>	
y-Achse .....	63
<b>Z</b>	
Zahlendarstellung in digitalen Rechenanlagen .....	29
Zeilenvektoren .....	126
Zentrum .....	98
Zerfallungsknoten .....	184
Zufallszahlen .....	258
Zufallszahlengenerator .....	258
zusammenhängend .....	183, 189
Zustandsdiagramm .....	189
Zustandsgraph .....	235
Zustandsgraphen .....	237
Zustandstrajektorie .....	239
Zweierkomplement .....	30
Zweipunktform .....	76, 87
Zyklische Gruppe .....	99
zyklischer Code .....	251



