Jörg R. Mühlbacher
Günter Pilz
Marcel Widi

Mathematik *exploriativ*

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

Universitätsverlag Rudolf Trauner

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 Bedienungsoberfläche geschaffen wird. Zur Spezifikation und Implementierung der Applets haben neben Jörg R.Mühlbacher noch Bernhard Niedermayer, Markus Pfleger, 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. Vetters: 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, 2nd 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
4th 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

F

G

H

I

T

U

V

W

X

Y

Z