Computeralgebra–Rundbrief

Nummer 14 *Fachgruppe Computeralgebra* *28.2.1994*

Liebe Kolleginnen und Kollegen,

die Fachgruppe Computeralgebra hat am 25. Januar im Rahmen der Wissenschaftspressekonferenz e.V. eine Pressekonferenz veranstaltet. Wir haben mit Vorträgen und Computervorführungen den Journalisten ein attraktives Bild unseres Gebietes vermitteln können. Besonders erfreulich war, daß die drei Präsidenten unserer Trägergesellschaften Prof. Dr. R. Vollmar von der GI, Prof. Dr. M. Grötschel von der DMV und Prof. Dr. R. Mennicken von der GAMM bei der Konferenz anwesend waren und der Veranstaltung nach innen und außen Gewicht gaben. Es sei allen Mitwirkenden zum Gelingen dieser wichtigen Veranstaltung herzlich gedankt! Zu Ihrer Information haben wir die Pressetexte und das Programm vollständig in diesem Rundbrief abgedruckt. Erfreuliche Reaktionen waren z.B. Sendungen im Deutschlandfunk, WDR, Saarländischen Rundfunk und Bayrischen Rundfunk. Bei Interesse können wir eine digitalisierte Form der Aufzeichnungen über das CAIS zur Verfügung stellen. Wir möchten auch anregen, daß Sie mit diesen Hintergrundinformationen und Ihren eigenen Computeralgebra-Projekten an Ihre Universitäts-Pressestellen und Lokalzeitungen herantreten.

Da die DMV sich gerade organisatorisch in einer Umbruchsphase befindet, hat uns das Präsidium der DMV um Verständnis gebeten, daß erst ab 1995 der Jahresbeitrag von DM 15,00 zusammen mit dem Jahresbeitrag erbeten werden kann. Die Fachgruppenleitung erbittet deshalb von ***allen Fachgruppenmitgliedern****, die Mitglied* ***der DMV****, aber* ***nicht zusätzlich der GI*** *sind, die Überweisung dieses Betrages mit dem Vermerk*

> *Beitrag Fachgruppe Computeralgebra auf unser Konto bei der GI: Kontonummer 46581, Sparkasse Bonn, Bankleitzahl 380 500 00*

zu veranlassen. Herzlichen Dank für Ihre Bemühung! (Fortsetzung S. 2)

[0]**Impressum** *Computeralgebra–Rundbrief* Herausgegeben von der Fachgruppe Computeralgebra der GI (2.2.1), DMV und GAMM, Redaktionsschluß 28.02 und 31.08. Anschrift: Dr. Ulrich Schwardmann, Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) Am Fassberg, 37077 Göttingen, Telefax: 0551-21119 Internet: uschwar1@gwdg.de, Adreßverwaltung: GI, Godesberger Allee 99, 53175 Bonn, Internet: gibonn@gmd.de ISSN 0933-5994.

Die auf Initiative der Fachgruppe beim Zentrum für interdisziplinäre Forschung beantragte Konferenz zum Thema COMPUTER ALGEBRA IN SCIENCE AND ENGINEERING, from algorithms to applications findet vom 28.08.1994-31.08.1994 in Bielefeld statt. Wir bitten um Beachtung der Konferenzankündigung in diesem Rundbrief, ebenso sei auf die Sektion Computeralgebra bei der Jahreskonferenz der DMV in Duisburg besonders hingewiesen.

Johannes Grabmeier *B. Heinrich Matzat*

Hinweise auf Konferenzen

1. **Algebra and Combinatorics: Interactions and Applications**

   Dresden, 6.–12.3.1994.

   dedicated to the memory of Lev Arkad'evič Kalužnin on occasion of his 80^{th} birthday.

   Topics of the conference: Groups and Permutation Groups, Algebraic Combinatorics, General Algebra, Applications in various fields of science (mathematics, computer science, chemistry, ...). The *organizing committee* consists of Reinhard Pöschel (chairman, Dresden), Adalbert Kerber (co–chairman, Bayreuth) Mikhail H. Klin (co–chairman, Beer–Sheva) and Otto H. Kegel (Freiburg).

   Kontaktadresse: Reinhard Pöschel, e–mail: LAK@nalw01.math.tu–dresden.de, Phone: (+49)(-(0)351) 463 5355, Fax: (+49)(-(0)351) 463 7114.

2. **INTERVAL'94, International Conference on Interval and Computer-Algebraic Methods in Science and Engineering**

   St.Petersburg, Russia, March 7.–10.3.1994.

   The Organizing Committee has accepted more than 120 abstracts authorized by more than 160 scientists from 25 countries. The collection of abstracts is already in printing house, but in case it was not done before, you still can submit your abstract and your talk can be included in the programme. Please, write to the e-mail address nest@nit.spb.su as soon as possible.

   Kontaktadresse: Dr. V. M. Nesterov, Box 52, St. Petersburg, 195256, Russia, e–mail: nest@nit.spb.su J. Wolff von Gudenberg, Co-chairmen of INTERVAL'94 Email: wolff@informatik.uni-wuerzburg.de, Tel. 0931 / 888-5517, Fax. 0931 / 888-4602.

3. **Southeastern International Conference on Combinatorics, Graph Theory, and Computing**

   Boca Raton, Florida, 7.–11.3.1994

   Kontaktadresse: Frederic Hoffmann, hoffmann@fauvax.bitnet.

4. **RIACA**

   Amsterdam, 10.–11.3.1994.

   Kontaktadresse: riaca@can.nl.

5. **DIMACS Workshop on Computational Aspects of Geometric Group Theory**

   Rutgers Univ., New Brunsvic, NJ. 17.–20.3.1994.

   Kontaktadresse: Pat Toci, DIMACS, toci@dimacs.rutgers.edu.

6. **Rhine Workshop on Computer Algebra**

   Karlsruhe, 22.–24.3.1994.

   Kontaktadresse: Prof. Jacques Calmet, Universität Karlsruhe, Am Fasanengarten 5, 76131 Karlsruhe, `calmet@dkauni2.bitnet`.

7. **MEGA 94: Effektive Methoden der algebraischen Geometrie**

   Santander, Spanien, 5.–9.4.1994.

   Kontaktadresse: Prof. Tomas Recio, Prof. L. González–Vega, Stichtag zum Einreichen von Arbeiten ist der 16.09.1993 in TEX in elektronischer Form an mega94@ccucvx.unican.es oder 16 Kopien an Departamento de Matemáticas, Facultad de Ciencias, Universidad de Cantabria, Santander 39071, Spanien, Tel.: 0034–42–201433, Fax: 0034–42–201402, elektr. Adresse: recio@ccucvx.unican.es. Genauere Informationen finden Sie im CAIS.

8. **GAMM-Jahrestagung 1994, Sektion Computeralgebra**

   Braunschweig, Ostern 5.-8.4.1994.

   Für die nächste GAMM-Jahrestagung ist eine neue Sektion *Computeralgebra und -analysis* von Kurzvorträgen eingerichtet worden, deren Organisation Prof. Rump (Hamburg-Harburg) übernommem hat:

   GAMM 1994, Annual meeting April 5-8, 1994, at Braunschweig, Germany,

   The *Gesellschaft für Angewandte Mathematik und Mechanik* (GAMM) will hold its annual meeting 1994 at Braunschweig the week after easter. There is a new section of short lectures on *Computer algebra and computer analysis*. This section is devoted to algorithms producing correct answers on the computer, correct by means of exact results or verified error bounds. In order to establish this section for future GAMM-meetings we would very much appreciate many talks from the field of symbolic and algebraic computation and others working on algorithms in the above sense. Interested people should fill out a registration and a lecture form which can be obtained by e-mail from the address below. The computer algebra and computer analysis section has number 14.

   For more information contact S.M. Rump, TU Hamburg-Harburg, Informatik III, Eissendorfer Str. 38, 21071 Hamburg, Germany, e-mail: rump@tu-harburg.d400.de

9. **Workshop: Algorithms and Computer Applications in Representation Theory of Finite Dimensional Algebras**

   Bielefeld, 18.–21.5.1994

   Kontaktadresse: P. Dräxler, Fakultät für Mathematik, Universität Bielefeld, draexler@mathematik.uni-bielefeld.de.

10. **Kolloquium des DFG Schwerpunkts Algorithmische Zahlentheorie und Algebra**

    Dagstuhl, 10.–16.7.1994

    Kontaktadresse: Prof. B. H. Matzat, IWR, Univ. Heidelberg, matzat@clio.iwr.uni-heidelberg.de.

11. **IMACS'94**

    Atlanta, Georgia, USA, 11.–15.7.1994.

    The IMACS World Congress Secreteriat: School of Mathematics, Georgia Institute of Technology Atlanta, GA 30332-0160, USA, Fax: 404-853-9112, ames@math.gatech.edu

12. **1st International Derive Conference**

    Plymouth (Großbritannien), 11.–15.7.1994.

    Arbeiten sind einzureichen bis zum 31.01.1994. Nähere Informationen durch Prof. John Berry, Centre for Teaching Mathematics, Univ. of Plymouth, Drake Circus, Plymouth, Devon PL4 8AA, GB.

13. **OpenMath workshop**

    Oxford, UK, 20.–21.7.94.

    The next OpenMath workshop has been tentatively scheduled for the two days (July 20,21) preceeding the ISSAC 94 conference, in Oxford, England.

14. **International Symposion on Symbolic and Algebraic Computation, ISSAC'94**

    St. Catherine's College, Oxford, UK, 20. - 22. 7. 1994

    General Chair: Malcolm MacCallum, QMW, London, UK, `mm@maths.qmw.ac.uk` Program Chair: Joachim von zur Gathen, University of Toronto, Canada, `issac@cs.toronto.edu`

15. **Second International Workshop/Conference on Artificial Intelligence and Symbolic Mathematical Computing (AISMC-2)**

    King's College, Cambridge, England, 3.–5.8.1994

    The target date for receipt of papers and submissions is 23 April 1994.

    The address for submissions (in 3 copies) and for expressions of interest in attending the meeting is:
    Prof. J.A. Campbell, Dept. of Computer Science, University College London, Gower Street, London WC1E 6BT, England. Email enquiries can be sent to jac@cs.ucl.ac.uk.

16. **Maple Summer Workshop and Symposium '94**

    Rensseaer Polytechnic Institute, Troy, NY, 9.–13.8.1994.

    Kontaktadresse: Robert J. Lopez, Department of Mathematics, Rose-Hulman Inst. of Techn., 5500 Wabash Avenue, Terre Haute, IN 47803.

17. **Workshop: Computational Methods in Lie Theory**

    Essen, 15.–19.8.1994

18. **NIRFI-Conference: Algorithms in Fundamental Mathematics**

    Nizhny Novgorod, 20.–28.8.1994

    The conference will take place near Nizhny Novgorod from 20.08.1994 to 28.08.1994 (this time may be slightly changed).

    The Nizhny Novgorod State University, Radiophysical Research Institute and the High Technology Incubation Center plan to organize the series of the International Conferences "Algorithms in Fundamental Mathematics".

    The scientific program of these Conferences includes the methods of construction and the investigations of the complexity and efficiency of algorithms in various branches of fundamental mathematics. The First Conference "Algorithms in Algebra, Geometry and Combinatorics" will be held in 1994. Address: M.A.Antonets,Radiophysical Research Institute(NIRFI), Bolshaya Pecherskaya str.,25, Nizhny Novgorod,603600, Russia. FAX: 7-8312369902 E-MAIL:anton@nirfi.sandy.nnov.su

19. **Computeralgebra in Science and Engineering**

    Bielefeld, 28.8.–31.8.1994

    We invite computer scientists, mathematicians, physicists, chemists, biologists, and engineers from academia and industry to participate in our interdisciplinary workshop. We try to bring together a broad spectrum of people involved in theory, systems, and application aspects of computer algebra.

    Invited lectures are given by internationally leading experts. Beyond that we invite for computer demonstrations, short presentations and contributions to poster sessions.

    Speakers include: Brans (New Orleans), Caviness (Newark), Cohen (Amsterdam), Dress (Bielefeld), Fleischer (Bielefeld), Cerdt (Dubna), Gonnet (Zürich), Grabmeier (Heidelberg), Hartley (St. Augustin), Havel (Harvard), Kerber (Bayreuth), Kovács (Berlin), Küchlin (Tübingen), Laskar (Paris), Loos (Tübingen), Melenk (Berlin), Shirkov (Dubna), Stifter (Linz), Veltman (Michigan), Vermaseren (Amsterdam).

    Scientific organization: Jochem Fleischer (U Bielefeld), Johannes Grabmeier (IBM Heidelberg), Friedrich-Wilhelm Hehl (U Cologne and GK "Scientific Computing" Cologne-St.Augustin), Wolgang Küchlin (U Tübingen)

    Kontaktadresse: Marina Hoffmann (conference office), Wellenberg 1, D-33615 Bielefeld, Germany.
    Phone: *49/(0)521/106 2768; Fax: *49/(0)521/106 2782; E-Mail: hoffmann@nov.zif.uni-bielfeld.de

20. **CONPAR 94 / VAPP VI International Conference**

    Linz, Austria, 6.–8.9.1994.

    Bei dieser Tagung gibt es eine spezielle Sektion über paralleles symbolisches Rechnen. Chairman: Prof. Jens Volkert, Program Chairman: Prof. Bruno Buchberger. Weitere Informationen bei Wolfgang Schreiner, RISC-Linz, J. Kepler Univ., A-4040 Linz, Austria, Phone: +43-7236-3231-66, Fax: +43-7236-3231-30, email: conpar94@risc.uni-linz.ac.at

21. **DMV-Jahrestagung 1994, Sektion Computeralgebra**

    Duisburg, 19.–23.9.1994.

    Erfreulicherweise hat die DMV bei ihrer Jahrestagung 1994 in Duisburg nach Berlin 1987 und Regensburg 1988 wieder eine Sektion Computeralgebra eingerichtet. Die Sektionsleitung liegt in den Händen von Prof. B. Fuchssteiner, dem DMV-Vertreter in der Fachgruppenleitung.

    Den folgenden Hauptvortrag gibt es zusätzlich zu der Sektion Computeralgebra auf dieser Tagung:

    Prof. D. Bayer. New York: The impact of computation on algebraic geometry.

    How has a decade of practical machine computation influenced algebraic geometry? While better access to examples has illuminated theoretical investigations, ultimately a more significant effect may be the opening up of algebraic geometry as a resource to other disciplines. This talk will examine influences of computational algebraic geometry within and beyond its home turf, looking at examples including the study of curves, the study of splines, four-colorings of graphs, and applications of toric varieties to fields such as statistics and integer programming.

22. **2nd European Fluid Mechanics Conference**

    Warschau, Poland, 20.–24.9.1994

    Auf dem Kongreß wird von K.G. Rösner ein Vortrag zum Thema: "The Impact of Computer Algebra on Fluid Dynamics" gehalten werden.

    Weitere Informationen bei: Prof. H. Zorski, Inst. of Fund. Techn. Research, Polish Academy of Science, Swietokrzyska 21, 00-049 Warzaw, Poland, und: Prof. J.S. Ostrowski, Inst. of Aeronautics and Appl. Mech., Warzaw Univ. of Techn., Nowowiejska 22/24, 00665 Warzaw, Poland.

23. **COMPUTER ALGEBRA,**
with emphasis on discrete algebra and geometry

Eindhoven, The Netherlands September 26.–30.9.1994.

Organized by: Euler Institute of Discrete Mathematics and its Applications , EIDMA , P.O. Box 513, , 5600 MB Eindhoven , The Netherlands

The goal of the course is to make the participants familiar with methods and techniques used in computer algebra, as well as to introduce them in the (new) research area of Algorithms in Algebra.

24. **Algorithms and Number Theory**

Dagstuhl, 10.–14.10.1994

Im Internationalen Begegnungs- und Fortbildungszentrum fuer Informatik in Schloss Dagstuhl findet vom 10.10.1994 bis zum 14.10.1994 ein Seminar mit dem Thema "Algorithmen und Zahlentheorie" statt. Leiter sind: Prof. Dr. Johannes Buchmann, Saarbruecken, Prof. Dr. Harald Niederreiter, Wien, Prof. Dr. Andrew Odlyzko, Murray Hill, USA, Prof. Dr. Horst Guenter Zimmer, Saarbruecken.

"Algorithms and Number Theory"

is aimed at presenting and discussing problems, methods and results in algorithmic elementary, analytic and algebraic number theory as well as algorithmic geometry of numbers and arithmetic algebraic geometry. Of particular interest will be applications to complexity, coding theory and cryptography and presentations of implementations and computer algebra systems.

25. **Computeralgebra-Software**

Dagstuhl, 6.–10.2.1995.

Tagungsleiter: J. Buchmann, R. Loos, R. Mäder.

26. **Symbolische Reduktionstechniken - Vervollständigungen und ihre Anwendungen**

Monte Verità, Ascona (Schweiz), 1.–6.5.1995.

Diese Tagung wird im Centro Stefano Franscini der ETH Zürich von Prof. Dr. E. Engeler (ETH Zürich), Prof. Dr. M. Bronstein (ETH Zürich), Prof. Dr. V. Weispfenning (U Passau) und Dr. J. Grabmeier (IBM Heidelberg) organisiert.

Symbolische Reduktionstechniken spielen eine zentrale Rolle in der Computeralgebra. Themenbereiche sind Knuth-Bendix-Methode für Gruppen, Monoide und allgemeine Termersetzungssysteme, die Gröbnerbasis-Methode und ihre Verallgemeinerungen in der kommutativen Algebra und nichtkommutativen Ringtheorie, die Methode der charakteristischen Mengen für gewöhnliche Differentialgleichungen, die Riquier-Janet-Methode für partielle Differentialgleichungen. Im weiteren Sinne ferner die Todd-Coxeter-Methode zum Auffinden von Permutationsdarstellungen endlich präsentierter Gruppen, sowie ähnliche Methoden zur Matrixdarstellung von endlich präsentierten nichtkommutativen Algebren.

Weitere Informationen: Phone: +41-1-632-7474, Fax: +41-1-632-3973, email: bronstein@inf.ethz.ch

27. **ICIAM 95**

Hamburg 3.–7.7.1995

Kontaktadresse: GAMM-Office, Univ. Regensburg, NWF I - Mathematik, D-93053 Regensburg, Germany

Berichte von Konferenzen

1. **OpenMath Workshop**

ETH Zürich, 17.-18.12.1993

INVITED PARTICIPANTS: John Abbot, Bruno Buchberger, David Clark, Arjeh Cohen, Stephane Dalmas, James Davenport, Richard Fateman, John Fitch, Benno Fuchsteiner, Marc Gaetano, A. Galligo, Keith Geddes, Morven Gentleman, Gaston Gonnet, Dominik Gruntz, Tony Hearn, Chris Howlett, Richard Jenks, Norbert Kajler, George Labahn, Helmut Lenzig, Roman Mäder, Niklaus Mannhart, Michael Monagan, Ron Neumann, Bruno Salvy, Alain Sausse, Mika Seppala, Carlo Traverso, Jos Vermaseren, Stefan Vorkoetter, Paul Wang, Stephen Watt, Wolfgang Weck

ATTENDEES: Heikki Apiola, Stephane Dalmas, Marc Gaetano, A. Galligo, Gaston Gonnet, Dominik Gruntz, Chris Howlett, Norbert Kajler, Niklaus Mannhart, Michael Monagan, Mika Seppala, Carlo Traverso, Jos Vermaseren, Stefan Vorkoetter, Wolfgang Weck, Clifton Williamson

PURPOSE: A workshop to formulate a character based standard for the exchange of mathematical formulas and other mathematical objects between programs.

PROCEEDINGS: For any presentations accompanied by paper(s), we omit detail here and refer the reader to the paper(s).

Gaston Gonnet gave an introduction to OpenMath, and outlined some of the requirements that such a protocol must have in order to function in arbitrary environments. Some of these requirements are: text (character) based, can be sent by electronic mail, a limit on line length, extensible.

Chris Howlett outlined Waterloo Maple Software's plans for OpenMath: committed to implementing a client/server math architecture for Maple during 1994, and need an agreed upon standard such as OpenMath to ensure utility and acceptance; input from and agreement of a large group is essential.

Stefan Vorkoetter described the current OpenMath proposal, as put forward by Waterloo Maple Software. During the ensuing discussion, some weaknesses and Maple-specific aspects were discovered: choice of data structures too Maple-biased, and how to decide which operators/functions to include.

Heikki Apiola described ESC, an Environment for Scientific Computation, which combines various mathematical tools.

Wolfgang Weck described the concept of an extensible OO class hierarchy for representation of mathematical Expressions.

Marc Gaetano described the ASAP protocol: "Designing a protocol for exchanging mathematical objects" S. Dalmas, M. Gaetano, A. Sausse; "The ASAP Protocol: a description" S. Dalmas, M. Gaetano, A. Sausse; "A C library for ASAP" S. Dalmas, A. Sausse.

Carlo Traverso described POSSO: "The POSSO External Data Representation"

Norbert Kajler spoke on building a computer algebra environment and described the SAFIR project and CAS/&pi: "Building a Computer Algebra Environment by Composition of Collaborative Tools", Norbert Kajler

Mika Seppala gave a brief historical review of EuroMath.

Stefan M. Vorkoetter

2. Dreitägiger Crashkurs über Computeralgebra

Köln–St.Augustin,20.–22.12.1993.

Das **Graduiertenkolleg** (GK) **'Scientific Computing' Köln–St.Augustin** hatte vom 20.–22.Dezember 1993 einen Crashkurs über Computeralgebra (CA) veranstaltet. Ziel und Zweck der Veranstaltung war es, den Stipendiaten des GK einerseits und Studenten und wissenschaftlichen Mitarbeitern verschiedener Universitäten andererseits exemplarisch in die Anwendung moderner Computeralgebra–Systeme einzuführen und gleichzeitig – sozusagen ein Blick hinter die Kulissen werfend – die Datenstrukturen und Algorithmen, die ein Computeralgebra–System konstituieren, kennenzulernen.

Anthony C. Hearn (RAND, Santa Monica, Kalifornien) erläuterte in einführenden Vorlesungen 'Fundamental Algorithms and Data Structures' von CA–Systemen, während Willi-Hans Steeb (Rand Afrikaans University, Johannesburg) eine elementare Einführung (mit Übungen) in das CA-System REDUCE gab.

Mike Dewar (University of Bath, England) berichtete über die bemerkenswerten Fortschritte, die mit 'Symbolic Numeric Interfaces' letzthin gemacht wurden, während James H. Davenport die 'Cylindrical Decomposition', ein Verfahren der reellen algebraischen Geometrie, besprach. Herbert Melenk (Konrad Zuse–Zentrum Berlin) beschrieb Algorithmen zum 'Lösen algebraischer Gleichungssysteme' und Thomas Wolf (Queen Mary and Westfield College, London) stellte Computer–Verfahren zum 'Lösen von Differentialgleichungen' zusammen. W. Küchlin (Univ. Tübingen) erläuterte die Fortschritte, die beim Parallelisieren von CA erzielt wurden.

Abschließend präsentierte Johannes Grabmeier (IBM Heidelberg) das CA–System AXIOM in einer Vorlesung. Übungen in AXIOM, betreut durch die Herren Grabmeier, Davenport und Dewar rundeten den Crashkurs ab, in dessen Verlauf es zu guten Kontakten zwischen Stipendiaten und Dozenten kam.

Den etwa 50 Teilnehmern erläuterte Thomas Lengauer für das gastgebende 'Institut für Methodische Grundlagen' der GMD in St.Augustin (bei Bonn) die wissenschaftliche Arbeit in diesem Institut. Herr Schrüfer gab eine allgemeine Einführung in die Computeralgebra sowohl aus der Sicht des Anwenders, als auch der des Forschungsgebietes.

Friedrich W. Hehl (Univ. zu Köln), Eberhard Schrüfer (GMD, St.Augustin)

3. Workshop on Computational Aspects of Geometric Group Theory I

Geometry Center an der Universität von Minnesota in Minneapolis, 3.-14.01.1994.

Vom 3. bis 14. Januar dieses Jahres fand im Geometry Center an der Universität von Minnesota in Minneapolis ein Workshop über Computer Aspekte der geometrischen Gruppentheorie statt. Jeder der 24 Teilnehmer hatte im Verlauf der zwei Wochen die Möglichkeit sich, und gegebenfalls seine Programme, in einem kurzen Vortrag vorzustellen. Außerdem gab es eine längere Diskussion zum Thema mathematischer Programme und deren Benutzerschnittstellen. Darüberhinaus fanden sich die Teilnehmer in wechselnden Gruppen zusammen, um gemeinsame Interessen zu diskutieren. Dazu gehörten unter anderem Methoden für endlich präsentierte Gruppen mit unlösbarem Wortproblem und Fragen zur Implementation von mathematischen Programmen.

Martin Schönert (Aachen)

4. **Gröbner bases and related topics**

Dagstuhl, 10.–14.2.1994.

The conference was part of the programme of the DFG Schwerpunkt "Algorithmische Zahlentheorie und Algebra". Its purpose was to give an overview on new developments and applications of Gröbner basis methods in different fields of mathematics.

In particular, members of the Schwerpunkt had the opportunity to discuss and exchange ideas, together with specialists from outside the Schwerpunkt, on

- different applications of Gröbner basis techniques (ranging from Galois theory, group rings and differential algebra to singularities and real algebraic geometry);
- new strategies for speeding up the classical algorithm (using Hilbert–Poincaré series, HighCornerMethod, ecart-Method);
- extension of the classical algorithm to more general structures (arbitrary semigroup–orderings, special non–commutative structures);
- complexity problems, change of ordering by linear algebra, possible applications to cryptography, parallelization of integer arithmetic for Gröbner basis computations and further topics;
- existing implementations in different computer algebra systems.

Several demonstrations of software (CALI, CoCoA, POSSO, SINGULAR) contributed to a relaxed but stimulating atmosphere during the conference.

J. Apel (Leipzig), E. Becker (Dortmund), D. Besseghini (Pisa), A. Capani (Genua), O. Caprotti (RISC), W. Decker (Saarbrücken), A. Dolzmann (Passau), C. Fieker (Berlin), J. Grabmeier (Heidelberg), H.-G. Graebe (Leipzig), G.-M. Greuel (Kaiserslautern), T. Jebelean (RISC), G. Kemper (Heidelberg), K. Lux (Aachen), K. Madlener (Kaiserslautern), A.M. Mandache (RISC), B. Martin (Cottbus), B.H. Matzat (Heidelberg), H. Melenk (Berlin), M. Meßollen (Saarbrücken), M. Moeller (Hagen), T. Mora (Genua), J. Müller (Aachen), V. Müller (Saarbrücken), R. Nauheim (Heidelberg), M. Niermann (Dortmund), G. Niesi (Genua), T. Nüßler (Kaiserslautern), M. Pesch (Passau),G. Pfister (Kaiserslautern), W. Pohl (Kaiserslautern), B. Reinert (Kaiserslautern), L. Robbiano (Genua), J. Schmid (Dortmund), H. Schönemann (Kaiserslautern), F.-O. Schreyer (Bayreuth), T. Siebert (Berlin), R. Stobbe (Kaiserslautern), C. Traverso (Pisa), V. Weispfenning (Passau), W. Windsteiger (RISC).

G.-M. Greuel

Wissenschaftspressekonferenz zum Thema Computeralgebra Bonn, 25. 1. 1994

Referenten: **Dr. Johannes Grabmeier**
Sprecher der Fachgruppe Computeralgebra, Institut für Supercomputing und Angewandte Mathematik, Wissenschaftliches Zentrum Heidelberg (ISAM), IBM Deutschland Informationssysteme GmbH
Prof. Dr. Benno Fuchssteiner
Fachbereich Mathematik-Informatik, Universität-Gesamthochschule Paderborn
Prof. Dr. Johannes Buchmann
Fachbereich Informatik, Universität des Saarlandes, Saarbrücken
Prof. Dr. Thomas Beth
Fakultät für Informatik, Universität Karlsruhe

Podium: **Prof. Dr. Martin Grötschel**
Vorsitzender der Deutsche Mathematiker-Vereinigung (DMV), Konrad-Zuse-Zentrum für Informationstechnik, Berlin
Prof. Dr. B. Heinrich Matzat
Stellvertretender Sprecher der Fachgruppe Computeralgebra, Interdisziplinäres Zentrum für Wissenschaftliches Rechnen, Universität Heidelberg
Prof. Dr. Reinhard Mennicken
Präsident der Gesellschaft für angewandte Mathematik und Mechanik (GAMM), Fachbereich Mathematik, Universität Regensburg
Prof. Dr. Roland Vollmar
Präsident der Gesellschaft für Informatik (GI), Fakultät für Informatik, Universität Karlsruhe

Programm: Dr. Johannes Grabmeier: Begrüßung und Einführung

Prof. Dr. Benno Fuchssteiner: **„Computeralgebra: Spielerei im Elfenbeinturm oder neuer Durchbruch zur Beherrschung mathematisch-technischer Sachverhalte?"**

Ausgewählte **Anwendungen aus Kryptographie, Signalverarbeitung und Robotik**, vorgestellt durch Prof. Dr. Johannes Buchmann und Prof. Dr. Thomas Beth

Vor, während und nach der Konferenz werden **Anwendungen der Computeralgebra am Computer** vorgeführt.

Computervorführungen:

Prof. Dr. Thomas Beth
Fakultät für Informatik, Universität Karlsruhe
Beispiele aus der Kryptographie, der Signal- und Bildverarbeitung

Prof. Dr. Johannes Buchmann
Fachbereich Informatik, Universität des Saarlandes, Saarbrücken
Sicherheit elektronischer Kommunikation – Faktorisierung großer Zahlen

Prof. Dr. Andreas Dress, Olaf Delagado und Dr. Daniel Huson
FSP Mathematisierung - Strukturbildungsprozesse, Universität Biefeld
Periodische Muster und Graphik-Design, RepTiles – ein Computerprogramm zur Erzeugung von Pflasterungen

Prof. Dr. Benno Fuchssteiner, Klaus Gottheil
Fachbereich Mathematik-Informatik, Universität-Gesamthochschule Paderborn
Computeralgebra: Das MuPAD-System

Prof. Dr. A. Kerber, Prof. Dr. R. Laue und R. Hohberger
Lehrstuhl II für Mathematik, Universität Bayreuth
MOLGEN+, molekulare Strukturaufklärung in der Chemie

Dr. Peter Kovàcs
Technische Universität Berlin
Robotersteuerung

Prof. Dr. Wolfgang Küchlin, Dr. Beatrice Amrhein, Georg Hagel
Wilhelm Schickard Institut für Informatik, Universität Tübingen
Computeralgebra im Mathematikunterricht

Dr. habil. Fritz Schwarz
Gesellschaft für Mathematik und Datenverarbeitung (GMD), Institut Fa1, St. Augustin
Lösen von Differentialgleichungen mit Computeralgebra

Fachgruppe Computeralgebra in Deutschland

Johannes Grabmeier

Seit 1987 ist in Deutschland die Fachgruppe Computeralgebra der GI, DMV und GAMM aktiv und gibt der stürmischen Entwicklung dieses Gebietes im Übergangsbereich von Informatik, Mathematik und Anwendungsgebieten in den Natur-, Ingenieur- und Wirtschaftswissenschaften eine gemeinsame Plattform. Die Fachgruppe gibt den Computeralgebra-Rundbrief heraus, der zweimal im Jahr erscheint und an die mehr als 1100 Mitglieder versandt wird. Die Fachgruppe betreibt ein elektronisches Informationssystem CAIS.

In Deutschland gibt es Computeralgebra-Arbeitsgruppen an Universitäten, Forschungsinstituten und in der Industrie. Es werden Computeralgebra-Systeme – wie z.B. das weit verbreitete System GAP und MuPAD, das erste System für parallele Rechnerarchitekturen – entwickelt. Weiter sind sie an der Mitentwicklung von großen Systemen wie z.B. REDUCE und AXIOM beteiligt. Bei vielen Arbeitsgruppen steht die Entwicklung neuer Algorithmen im Mittelpunkt, in anderen Arbeitsgruppen steht die Umsetzung und die Anwendung der symbolische Methoden im Vordergrund.

Der Industriestandort Deutschland ist in großem Maße von Methoden und Werkzeugen, wie sie auch die Computeralgebra anbietet, abhängig. Durch die damit gegebenen Optimierungsmöglichkeiten werden die notwendigen neuen Qualitätssprünge und das schnelle Reagieren auf neue Marktsituationen möglich.

Die Fachgruppe hat in den vergangenen zwei Jahren einen **Report** zur Computeralgebra in Deutschland zusammengestellt. Auf 320 Seiten haben dazu 99 Autoren mit Grundsätzlichem, mit Übersichtsartikeln, Anwendungsbeschreibungen, Berichten zu den Systemen und sonstigen Informationen beigetragen. Damit ist zum ersten Mal ein umfassender Überblick über dieses Gebiet gegeben. Diesen Report dürfen wir Ihnen heute präsentieren.

Computeralgebra: Spielerei im Elfenbeinturm oder neuer Durchbruch zur Beherrschung mathematisch-technischer Sachverhalte?

Benno Fuchssteiner

Charles Eugène Delaunay arbeitete mehr als zwanzig Jahre an den Formeln seiner zweibändigen unvollendeten Theorie der Mondbewegung. Die Überprüfung alleine nahm die letzten 10 Jahre im Leben dieses kreativen Geistes in Anspruch. 1970 wurden die Ergebnisse – wohlgemerkt die Formeln, nicht das Rechnen mit Zahlen – erneut überprüft: mit einem Computeralgebrasystem innerhalb von 20 Stunden. Heute würde diese Prüfung, bei der auf Seite 234 ein Fehler gefunden wurde, weniger als zwei Stunden dauern. Was hätte Delauny mit den geschenkten 10 Jahren nicht alles anfangen können?

Dieses Beispiel zeigt das Potential einer neuen Disziplin – zumindest das Potential für Autoren tausendseitiger Bücher voller komplizierter Formeln – aber nicht nur für diese, denn Computeralgebra wird den Umgang unserer Kinder und Enkel mit Mathematik wesentlich prägen und ihr Verständnis von Wissenschaft und Technik entscheidend beeinflussen: Gigantische Formeln werden ihre Schrecken verlieren und den Umgang mit scheinbar komplizierter Mathematik da zum Kinderspiel machen, wo bisher der routinemäßige syntaktische Umgang mit der strengen und abweisenden Sprache der Mathematik den Blick auf die eigentlichen Inhalte verstellte.

Was ist Computeralgebra ? Stellen Sie sich vor, Sie hätten alle Formeln Ihrer Schulzeit, Ihres Studiums und Ihres Berufes sofort zur Verfügung, Sie würden diese anreichern mit dem algorithmischen Wissen einer großen Zahl professioneller Mathematiker, Ingenieure und Naturwissenschaftler, und hätten dann noch jemand, der Ihnen den Umgang mit diesem Wust von Information intelligent erledigt, der Ihnen Schreibarbeit abnimmt, die Formeln fehlerfrei ineinander einsetzt, Ableitungen bestimmt, Gleichungen löst, Graphiken zeichnet, Geometrie verdeutlicht, und benötigte Resultate zur Not in Windeseile tausendstellig ausrechnet. Wenn Sie sich das alles vorstellen, dann haben Sie einen kleinen Ausschnitt dessen, was Computeralgebra heute schon ist und einen noch kleineren dessen, was sie morgen leisten kann und wird.

Nur soviel in Kurzform: Computeralgebra nutzt den Rechner nicht, oder zumindest nicht in erster Linie, zum Berechnen von Zahlen, sondern zum intelligenten Umgang mit Formeln. Das Ausrechnen von Zahlen erledigt Computeralgebra natürlich auch, aber eher *en passant.* Wenn Sie mehr wissen wollen, dann schauen Sie sich die folgenden Demos an, wo Abituraufgaben und Differentialgleichungen gelöst werden, Chemische Formeln behandelt werden, Anwendungen auf Kryptographie und Robotik zu sehen sind.

Nur etwa 56% der Anfänger der Studiengänge unserer Universitäten absolvieren ihr Examen im gewählten Studiengang, eine Durchschnittszahl, welche von den geringen Erfolgsquoten unserer Studenten in den Ingenieur- und Naturwissenschaften geprägt wird. Bundesweit brechen sicher mehr als 60% der studentischen Anfänger der ingenieur- und naturwissenschaftlichen Fächer ihr Studium entweder ergebnislos ab oder wechseln zu anderen Fächern. Der Grund für diese volkswirtschaftlich kaum tragbare Abbruchquote ist unter anderem in einem Mangel an Routine beim effizienten Umgang mit mathematischen Sachverhalten und Formeln zu sehen. Die Abbruchquoten dieser Studentengruppe haben ihre Ursachen also in einem Fach, welches zwar zur Formulierung der eigenen Interessen notwendig ist, aber trotzdem von den Inhalten dieser Interessen recht weit entfernt liegt. Die Verfügbarkeit von Hilfsmitteln moderner Technologie für den formalen und algorithmischen Umgang mit Mathematik kann einen kleinen Beitrag leisten, diesen bedauerlichen Umstand zu ändern. Die Schaffung solcher Hilfsmittel ist deshalb eine volkswirtschaftliche Notwendigkeit, und die freie Verfügbarkeit solcher Hilfsmittel muß ein ernstes Anliegen aller wissenschaftspolitischen Planung sein.

Computeralgebra wird bei der Lösung von Problemen in Forschung und Lehre einen gewichtigen Beitrag leisten, zum Teil wird er schon heute geleistet: Unbemerkt von der Öffentlichkeit hat die Entwicklung solcher Systeme, und das Vorantreiben der dazu notwendigen Grundlagenforschung heute bereits eine beachtliche Bandbreite erreicht und zu Resultaten und Werkzeugen geführt, die zum Teil weltweit verwendet werden. Computeralgebra wird an vielen deutschen Hochschulen mit immer mehr wachsendem Erfolg entwickelt und eingesetzt. Eine Vielzahl von Studentenlizenzen populärer Computeralgebrasysteme tragen zu einer breitgefächerten modernen Ausbildung bei.

Dies ist nur der Anfang, morgen werden sich solche Systeme auf dem Notebook jedes Schülers und Studenten befinden, und den Schulalltag Ihrer Kinder bestimmen und prägen. Eine rasante Neuorientierung der mathematischen Ausbildung wird die Folge sein.

Neben diesen Auswirkungen der Verbreitung von Werkzeugen der Computeralgebra, die in unserem täglichen Umfeld zu beobachten sein werden, wird eine ganz neue Dimension mathematischer Forschung und deren Anwendung auf Technik und Naturwissenschaft möglich sein. In einem amerikanischen Report an die National Science Foundation heißt es deshalb:
Mathematik ist die Basis des technologischen Fortschritts und dieser ein Schlüssel zur internationalen Wettbewerbsfähigkeit. Die Automatisierung eines beträchtlichen Teils mathematischer Problemlösungen ist für eine Nation, die den technischen Fortschritt beschleuinigen will, eine Schlüsseltechnologie und ein wirksamer Hebel, die menschliche Produktivität zu vervielfachen.

Sicherheit elektronischer Kommunikation – Faktorisierung großer Zahlen

Kurzreferat und Computervorführung

Johannes Buchmann

Kurzfassung

Bei der elektronischen Kommunikation z.B. via Fax oder Electronic Mail treten Sicherheitsprobleme auf. Manche Nachrichten müssen unterschrieben oder sogar geheimgehalten werden. Die Sicherheit einiger wichtiger Techniken zur Unterschrift oder Geheimhaltung beruhen auf der Schwierigkeit des Faktorisierungsproblems. Die *Primfaktorzerlegung* oder *Faktorisierung* $6 = 2 \times 3$ zu finden ist leicht. Die Faktorisierung von 2145907 zu finden ist schwerer. Sie lautet $2145907 = 1523 * 1409$. Um die Faktorisierung einer Zahl mit einhundert Dezimalstellen und zwei etwa gleich großen Primfaktoren zu finden, muß man mit den heute bekannten Verfahren auf sehr schnellen Computern monatelang rechnen. Das Faktorisierungsproblem zu erforschen ist aber nicht nur wichtig, um die Sicherheit von elektronischen Verschlüsselungsverfahren zu untersuchen, sondern Zahlen zu Faktorisieren ist Voraussetzung für die Lösung vieler anderer Probleme der Computeralgebra

Elektronische Kommunikation ist schon heute sehr verbreitet und wird immer wichtiger. Einige Beispiele:

- In Deutschland gibt es Millionen von Fax-Geräten und drahtlosen Telefonen.
- Weltweit sind Millionen von Computern miteinander verbunden. Sie können untereinander Nachrichten austauschen, die Daten der anderen verwenden und sich gegenseitig bei Berechnungsproblemen helfen.
- Viele Banken bieten ihren Kunden für wenig Geld Zusatzgeräte an, die "electronic banking" erlauben, also die Abwicklung von Finanzgeschäften von zu Hause.

Elektronische Kommunikation birgt viele Gefahren.

- Fax-Briefe sind rechtsverbindlich. Es ist aber ganz leicht, die Unterschrift von einem auf ein anderes Schreiben zu kopieren.
- Rechtsradikale bauen elektronische Kommunikationsnetze auf, die von außen schwer kontrollierbar sind.
- Elektronische Geldgeschäfte können belauscht und manipuliert werden.

Diese Gefahren sind vielen nicht bewußt. Trotzdem müssen Lösungen gefunden werden; besonders für folgende Probleme:

- Die Kommunikationspartner müssen ihre Gespräche vor anderen *geheimhalten* können. Eventuell sollen aber Gerichte geheime Nachrichten lesen können.
- Elektronische Dokumente müssen *unterschrieben* werden können und zwar so, daß die Unterschrift die Authentizität des Dokumentes beweist.
- Rechner in Netzen müssen *vor unberechtigtem Zugang geschützt* werden.

Die Lösungen der genannten kryptographischen Probleme sollen so sicher wie möglich sein.

Eine Möglichkeit ist, kryptographische Verfahren zu benutzen, die sehr kompliziert aussehen. Diese unterzieht man allen möglichen Tests. Ein Verfahren gilt dann als sicher, wenn es alle Tests erfolgreich besteht.

Ein solches Vorgehen ist aber problematisch. Man könnte den richtigen Test, der die Schwäche des Systems aufdeckt, übersehen haben. Besser wäre es, beweisbar sichere Systeme zu konstruieren. Das ist aber bis heute nicht gelungen. Vor etwa fünfzehn Jahren begann man Verfahren zu konstruieren, deren Sicherheit auf der Schwierigkeit der Lösung berühmter mathematischer Probleme beruht.

Ein solches System ist RSA. Es beruht auf der Schwierigkeit des *Faktorisierungsproblems*. Angenommen jemand sucht sich zwei Primzahlen aus (das ist leicht), multipliziert sie und veröffentlicht das Produkt. Das Problem besteht darin, die gewählten Faktoren zu finden. Wenn jemand z.B. 35 veröffentlicht, weiß jeder, daß die beiden Faktoren 7 und 5 waren. Wenn die veröffentlichte Zahl 6725569 ist, wird die Auffindung der Faktoren schon erheblich schwieriger. Haben die Faktoren je 100 Dezimalstellen, so kann heute niemand in der Welt die Faktoren finden.

Leider kann ich das RSA-Verfahren hier nicht erklären. Ich kann nur soviel sagen. Wer verschlüsselte Nachrichten erhalten will, der erzeugt das Produkt von Primzahlen, macht daraus die Schlüssel und veröffentlicht sie. Jeder kann diese Schlüssel zum Verschlüsseln benutzen. Aber nur wer die Faktoren kennt, kann auch entschlüsseln.

Wie gesagt, sicher ist das RSA-Verfahren nur, wenn Faktorisieren schwer ist. Es ist darum nötig, zu untersuchen, wie schwer das Problem wirklich ist. Dazu muß man versuchen, die existierenden Berechnungsverfahren zu Verbessern und neue zu finden. Auf diesem Gebiet hat es in den letzten 15 Jahren große Fortschritte gegeben. Die besten Verfahren, die 1970 bekannt waren konnten mit den damals verfügbaren Computern Zahlen mit 40 Dezimalstellen zerlegen. Heute kann man schon weit über 100-stellige Zahlen faktorisieren. Die dabei verwendeten Algorithmen verwenden neue komplizierte Techniken der Computeralgebra. Die Anwendung des Faktorisierungsproblems in der Kryptographie hat also zu einem großen Fortschritt in der Computeralgebra geführt.

Die amerikanische Kryptofirma RSA veranstaltet einen internationalen Wettbewerb, wer am besten faktorisieren kann. Sie veröffentlicht schwer zu faktorisierende Zahlen und setzt Preise für ihre Zerlegung aus. Gemeinsam mit zwei amerikanischen Gruppen hält unsere Arbeitsgruppe in Saarbrücken zur Zeit den Weltrekord in diesem Wettbewerb. Die gesamte Weltrekordrechnung hätte auf einem PC 1000 Jahre gedauert, unser Beitrag immerhin 250 Jahre. Um so aufwendige Rechnungen durchzuführen, haben wir eigens das System LiPS entwickelt, das in einem Netz von Arbeitsplatzrechnern nicht genutzte Rechenzeit automatisch einer schweren Berechnungsaufgabe zur Verfügung stellt. Das System wird inzwischen in vielen anderen Anwendungen eingesetzt.

Man sieht also – und das ist typisch für viele Bereiche der Computeralgebra – , daß das scheinbar so abstrakte Problem der Zerlegung von Zahlen in ihre Primfaktorem nicht nur mathematisch hoch interessant ist, sondern auch eine große praktische Bedeutung hat und zwar sowohl im Bereich der Datensicherheit als auch im Gebiet des High Performance Computing.

Anwendungen und Erfolge der Computeralgebra in Signalverarbeitung, Bildverarbeitung, Robotik, Kryptologie und Kommunikationstechnik.

Kurzreferat und Computervorführung

Thomas Beth

Kurzfassung

Der Entwurf von komplexen Hardware- bzw. Software-Systemen stellt eine große Herausforderung dar. Durch eine Algorithmenentwicklungsumgebung, in der ein VLSI-System und Computeralgebra-Systeme integriert sind, konnten bei der automatischen Generierung der Beschreibung solcher Systeme große Fortschritte erzielt werden.

Die Anwendbarkeit eines solchen Systems beruht auf algebraischen Spezifikationen der Probleme, das heißt auf einer Problembeschreibung durch Angabe von mathematischen Formeln.

Durch Methoden der Computeralgebra, insbesondere durch Struktur-Zerlegungen, lassen sich effiziente Algorithmen mit automatischem Algorithmenengineering erzeugen. Diese Methoden werden an Beispielen aus der Kryptographie, der Signal- und Bildverarbeitung demonstriert.

Der enge Zusammenhang zwischen der Computeralgebra und der anwendbaren Algebra wird auf diversen Gebieten industrieller und wissenschaftlicher Praxis sichtbar. Algorithmen der Signalverarbeitung, die etwa in der Consumer-Elektronik in CD-Spielern, Phototechnik, Mobiltelefonen, aber auch in der Satellitentechnik täglich eingesetzt werden, sind Ergebnisse der Anwendung der Computeralgebra.

Eine in der Forschung der letzten 5 Jahre entwickelte neue Perspektive ergibt sich aus der Verwendung der Methoden der Computeralgebra in Verbindung mit der Algebraischen Geometrie. Hierbei werden für weitgehend autonome Roboter die Bahnplanungsaufgaben für die Vorausberechnung der gezielten und kollisionsfreien Bewegung der Gehäuse, Arme und Finger in der Fertigung erfolgreich eingesetzt.

Der simultane Einsatz von optischen, taktilen und akusto-chemischen Sensoren in den Robotern und die daraus entstandene Modellierung von evtl. mehrdimensionalen Bewegungsfreiräumen zur Problemlösung ist erst durch Methoden der Computeralgebra realisierbar geworden. Diese Techniken wurden in der Forschung so weit verfeinert, daß inzwischen Einsätze außerhalb des Labors und industrieller Fertigungsstraßen auch im Bergbau, in der Reparatur von Kanalisationssystemen oder in der Chirurgie, insbesondere durch Mikrosystemkomponenten, angestrebt werden.

Diese sind nur möglich durch den gezielten Systementwurf in Planung, Hardware und Software, deren komplexe Entwurfsproblematik erst durch den Einsatz neuartiger CAD-Systeme lösbar wurde.

So ist es gelungen, eine integrierte Algorithmen-Entwurfsumgebung durch Kombination eines VLSI-CAD-Systems mit Computeralgebra-Systemen derart aufzubauen, daß damit algebraisch spezifizierte, das heißt durch reine Formelangabe spezifizierte Algorithmen der o.g. Anwendungsgebiete automatisch unter Einsatz computeralgebraischer Methoden in Hardware-Komponenten umgesetzt werden können. Erst die durch diesen Entwurfsprozeß entwickelten Komponenten ermöglichen neben ihrer hohen Integrationsdichten und Leistung den Einsatz im jeweiligen Anwendungsfall (Videokontrolle, Steuerungs- und Identifikationsmodule).

Die Verarbeitung einer solchen Aufgabenstellung setzt immer eine algebraische Spezifikation der gesuchten algorithmischen Lösung in mathematischer Form voraus. Darauf aufbauend kann diese Spezifikation dann in mehreren Transformationsschritten in das gewünschte Implementierungsmedium (z.B. Hardware oder konventionelle Programmiersprachen) umgewandelt und dabei auf jeder Stufe optimiert werden.

Bei der praktischen Umsetzung dieser Methoden konzentrierte man sich in Karlsruhe zunächst auf Problemfelder aus der Kryptographie, Codierungstheorie und Signalverarbeitung.

In der Kryptographie möchte man zum schnellen Ver- und Entschlüsseln, aber auch für elektronische Unterschriften, bestimmte arithmetische Operationen besonders effizient ausführen. Hierbei spielt die Arithmetik auf endlichen Körpern und auf elliptischen Kurven eine besondere Rolle. Für beides ist eine exakte Spezifikation im

Rahmen der Sprachen von Computeralgebra-Systemen problemlos möglich und für die jeweiligen industriellen Anwendungen jederzeit wiederholbar.

Schon auf dieser abstrakten Ebene erbringen Methoden der Computeralgebra eine deutliche Beschleunigung bzw. wesentlich vereinfachte Algorithmen. Die algebraische Spezifikation ermöglicht darüber hinaus eine automatische Transformation auf hardwarenahe Strukturen, die zu einer vollständigen Beschreibung eines ASIC (application specific integrated circuit) führen.

Ein zweites hier vorgestelltes Beispiel für diesen Algorithmen-Synthese Prozeß ist die zur Zeit wichtige Cosinus-Transformation, die für den Einsatz in der Signal- bzw. Bildverarbeitung, z.B. zur Datenkompression nach JPEG-Standard, besonders effizient implementiert werden muß. Durch Anwendung der Computeralgebra wird es möglich, solche Algorithmen in effiziente Teilalgorithmen zu zerlegen, ohne dabei ein exaktes Rechnen aufgeben zu müssen. Ähnliche Anwendung für Wavelet-Transformationen sind Gegenstand der aktuellen Forschung.

Periodische Muster und Graphik-Design, RepTiles – ein Computerprogramm zur Erzeugung von Pflasterungen

Computervorführung

Olaf Delgado, Andreas Dress und Daniel Huson

Kurzfassung

Regelmäßige Muster, Parkette und Mosaike werden seit Jahrtausenden benutzt, um Fußböden, Wände und Textilien zu schmücken. Auch die Frage nach der mathematischen Klassifizierung solcher Muster — in der Ebene, aber auch z.B. auf der Oberfläche einer Kugel — beschäftigte seit den Zeiten Platons immer wieder die Gelehrten. In den Augen heutiger Mathematiker sind die berühmten Platonischen Körper (Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder) schließlich nichts anderes als besonders regelmäßige Aufteilungen der Kugeloberfläche.

Unter einer periodischen Pflasterung verstehen wir eine lückenlose Überdeckung der Ebene durch ein sich immer wiederholendes Muster von Pflastersteinen. Solche Pflasterungen liegen also schon sehr lange buchstäblich auf der Straße. Trotzdem gelang es erst in den letzten Jahren an der Universität Bielefeld, einen mathematischen Formalismus zu entwickeln, mit dem die verschiedensten Fragestellungen auf diesem Gebiet systematisch behandelt und gelöst werden können. Weil die dazu notwendigen Berechnungen aber schnell mühselig werden, hat man die reine Rechenarbeit bald dem Computer übertragen. Im Laufe der Jahre entstand so eine Vielzahl von Programmen für die verschiedensten Zwecke.

Daniel Huson und Olaf Delgado haben diese Programme zusammengefaßt und mit einer leicht verständlichen Bedienungsoberfläche versehen, so daß jetzt auch interessierte Laien die Welt der Pflasterungen auf dem Computer erkunden können. Das so entstandene Computeralgebra-System heißt RepTiles und läuft auf allen Macintosh-Rechnern. Man kann damit systematisch Pflasterungen mit vorgegebenen Eigenschaften ausrechnen lassen, in Datenbanken suchen und grafisch gestalten.

Periodische Muster werden schon seit grauer Vorzeit benutzt, um zum Beispiel Fußböden, Wände, Vasen und Textilien zu schmücken. Auch im Werk des niederländischen Graphikers M.C. Escher (1889-1972) spielen lückenlose “Flächenaufteilungen”, deren Bau-Elemente meist Menschen, Tiere oder Fabelwesen sind, eine große Rolle. Fast jede seiner Flächenaufteilungen ist regelmäßig; sie entsteht wie ein Tapetenmuster durch periodisches Wiederholen eines möglichst einfachen Grundmusters, eines sogenannten “Fundamentalbereiches” der Aufteilung. Solche Flächenaufteilungen lassen sich in alle Richtungen beliebig weit fortsetzen.

Eine solche lückenlose Überdeckung einer Ebene, oder z.B. auch einer Kugeloberfläche, wird in der Mathematik “Pflasterung” genannt. Obwohl die periodischen Pflasterungen schon lange buchstäblich auf der Straße lagen, ist es erstaunlich, daß das Problem der mathematischen Behandlung von solchen Pflasterungen sich als sehr schwierig erwiesen hat und erst in den letzten 10 Jahren, durch intensive Forschung an der Universität Bielefeld, vollständig gelöst werden konnte.

Mathematisch geht es darum, einen vollständigen Überblick über die möglichen Typen von solchen Pflasterungen zu bekommen. Dabei muß zunächst geklärt werden, wann zwei Pflasterungen “vom selben Typ” sind. Mathematisch ist es sinnvoll, zwei Pflasterungen als äquivalent oder vom selben Typ anzusehen, wenn sie bruchlos ineinander umgeformt werden können. Vereinfacht läßt sich das so beschreiben: Eine der beiden Pflasterungen wird auf eine Gummihaut aufgemalt; läßt sich dann die Gummihaut so zurechtziehen, daß die beiden Pflasterungen zur Deckung gebracht werden können, so sind sie äquivalent, andernfalls gelten sie als nicht äquivalent. Oft wird dann noch gefordert, daß beide Pflasterungen die gleichen Symmetrien haben. Wie Beispiele zeigen, können zwei äquivalente Pflasterungen sehr verschieden aussehen. Es ist darum im allgemeinen gar nicht so einfach, zu entscheiden, ob zwei vorgegebene Pflasterungen äquivalent sind oder nicht.

Wie kann man nun die wesentlichen Eigenschaften einer periodischen Pflasterung mathematisch am einfachsten ausdrücken? Intuitiv leuchtet ein, daß es möglich sein müßte, periodische Muster in sehr kompakter Form zu beschreiben, denn schließlich muß man ja nur einen kleinen Teil einer Tapete sehen, um sich das endlose Muster vorstellen zu können. Der Versuch, diese Intuition in eine handfeste Theorie umzusetzen, führte zu einem Verfahren, welches jeder periodischen Pflasterung ein kurzes, auch von Computern handhabbares "Symbol" zuordnet. Diese Zuordnung hat die sehr nützliche Eigenschaft, daß zwei Pflasterungen genau dann äquivalent sind, wenn ihre Symbole übereinstimmen. Ist eine Pflasterung gegeben, so ist es relativ leicht, das zugehörige Symbol zu konstruieren. Umgekehrt kann man fragen: Wenn ein beliebiges Symbol gegeben ist, woran läßt sich erkennen, ob dazu wirklich eine periodische Pflasterung gehört? Andreas Dress (Bielefeld) konnte beweisen, daß ein Symbol genau dann zu einer periodischen Pflasterung der Ebene gehört, wenn dessen sogenannte "Krümmung" gleich 0 ist.

Um die periodischen Pflasterungen der Ebene mittels solcher Symbole zu klassifizieren, kann man wie folgt vorgehen: Zunächst werden per Computer alle in Frage kommenden Symbole mit Krümmung 0 erzeugt und danach wird zu jedem Symbol die zugehöriger Pflasterung konstruiert. Da es unendlich viele verschiedene Typen solcher Pflasterungen gibt, ist es dabei zweckmäßig, zuerst nur diejenigen zu berechnen, die *nur eine* Sorte von Pflastersteinen benutzen. In diesem Fall gibt es, wie schon lange bekannt ist, genau 93 verschiedene Typen. Sind dagegen 2 verschiedene Sorten von Pflastersteinen erlaubt, so gibt es genau 1270 verschiedene Typen, bei 3 Sorten sind es schon 48231, ...

An der Fakultät für Mathematik der Universität Bielefeld haben Olaf Delgado und Daniel Huson ein Computerprogramm mit dem Namen "RepTiles" entwickelt, das auf diesen Symbolen als Grunddatentyp aufbaut. Der Name des Programms kommt von *repeated tiles* (wiederholte Pflastersteine) und spielt zugleich auf die Reptilien an, die M.C. Escher gern in seinen Graphiken verwandte. Das interaktive Macintosh-Programm erlaubt es dem Benutzer, mit Hilfe von zwei einfachen geometrischen Operationen, "Spalten" und "Kleben", aus 46, wohlbekannten, bereits von H. Heesch klassifizierten Grundtypen jede mögliche periodische Pflasterung der Ebene zu erzeugen. Naheliegend ist deshalb die Anwendung von RepTiles auch im Graphik-Design-Bereich, ebenso aber auch bei der Analyse von Kristall-Oberflächen.

Weitaus interessanter als die zweidimensionalen sind die dreidimensionalen Pflasterungen. Hier geht es um die Frage, wie der *Raum* durch eine regelmäßige Anordnung von Körpern gefüllt werden kann. Diese Frage ist sehr eng mit Fragen aus der Kristallographie und der Chemie verbunden. Chemiker sind immer auf der Suche nach neuen Kristallstrukturen. Es fehlte ihnen bisher jedoch eine Methode, die mathematisch möglichen Strukturen systematisch aufzulisten.

Am neu eingerichtem "Forschungsschwerpunkt Mathematisierung - Strukturbildungsprozesse" der Universität Bielefeld werden nun einerseits Verfahren entwickelt, um Kristallstrukturen, die aus der Chemie kommen, mathematisch durch periodische Pflasterungen und deren Symbole zu beschreiben. Andererseits wird an der systematischen Klassifikation dreidimensionaler Pflasterungen gearbeitet, in der Hoffnung, daß diese Arbeit zu der Entdeckung neuer Kristallstrukturen führen wird.

Ein erstes Ergebnis ist kürzlich von Andreas Dress, Daniel Huson und Emil Molnár (Budapest) erzielt worden: Es wurde bewiesen, daß es genau 88 Typen von Pflasterungen des Raumes gibt, die die Eigenschaft haben, daß alle *zweidimensionalen Seiten* der Pflastersteine zueinander äquivalent sind.

Computeralgebra: Das MuPAD-System

Computervorführung

Benno Fuchssteiner und Klaus Gottheil

Kurzfassung

MuPAD ist ein Computeralgebrasystem, im Unterschied zur numerischen Behandlung mathematischer Sachverhalte manipuliert Computeralgebra auch Zeichen und Symbole. Der Name ist eine Abkürzung für: **Mu**lti **P**rocessing **A**lgebra **D**ata **T**ool. MuPAD ist eine Entwicklung der Mathematikgruppe im *Institut für Automatisierung und Instrumentelle Mathematik* der Universität-Gesamthochschule Paderborn. Forschungsinstitutionen und Ausbildungseinrichtungen steht MuPAD kostenlos zur Verfügung.

MuPAD ist ein Softwareprodukt, das den Umgang mit Formeln erlaubt und diesen mit intelligentem mathematischen Expertenwissen erleichtert. Neben numerischem Rechnen erlaubt MuPAD nicht nur den interaktiven, formelmäßigen Umgang mit mathematischen Objekten, sondern ermöglicht auch die problemlose Handhabung von Formeln - und damit von technischen Sachverhalten - die bisher wegen ihrer Kompliziertheit dem Anwender unzugänglich waren.

MuPAD hat eine außerordentlich komfortable Bedieneroberfläche, die selbst mathematischen Laien mit geringer Rechnererfahrung das spielerische Erlernen der Beherrschung des Systems ermöglicht. Ein interaktives digitales Handbuch, eine Systemkomponente zur interaktiven Fehlersuche, sowie ein leistungsfähiges menügesteuertes Graphikmodul runden das System ab. Ein ca. 400-seitiges Handbuch wird vom Birkhäuser Verlag in Basel publiziert.

Über Spezialaufgaben hinaus hat MuPAD die effiziente Erledigung allgemeiner mathematischer Aufgaben zum Ziel. Um Aufgaben und Probleme von ganz neuer Dimension lösen zu können, bietet MuPAD neben der Möglichkeit des sequentiellen Arbeitens, Versionen, die auf parallelen Rechnerarchitekturen aufbauen. Das zugrunde liegende Rechnermodell ist ein Netzwerk von Shared-Memory-Maschinen.

Gegenwärtig steht MuPAD für UNIX Arbeitsplatzrechner und Rechner der Familie APPLE-Macintosh zur Verfügung; eine Portierung auf andere Rechnerplattformen wird durchgeführt.

MOLGEN+, molekulare Strukturaufklärung in der Chemie

Computervorführung

A. Kerber, R. Laue, R. Hohberger

Kurzfassung

Molekulare Strukturaufklärung identifiziert chemische Substanzen anhand von spektroskopischen Daten. Das massenhafte Auftreten solcher Probleme, beispielsweise auch im Umweltschutz, läßt den Wunsch nach Automatisierung entstehen, wenn möglich durch Computerprogramme, die die anfallenden Daten wie Reaktionsverhalten, Spektren und ähnliche Informationen analysieren können und dem Chemiker dann Kandidaten vorlegen – möglichst wenige, aber unbedingt *alle,* die in Frage kommen.

Das von der Arbeitsgruppe A. Kerber und R. Laue an der Universität in Bayreuth entwickelte Computeralgebra-System MOLGEN$^+$ stellt den hierfür zentralen mathematischen Teil dar, der zu vorgegebener chemischer Summenformel samt Nebenbedingungen – vorgeschriebene und/oder verbotene Substrukturen – alle chemischen Strukturformeln ermittelt, die zu den eingegebenen Daten passen. Aus diesen Strukturformeln wird dann die zu identifizierende Substanz, genauer deren Strukturformel, ausgelesen.

Dieses System wurde mit dem Deutsch-Österreichischen Hochschul-Software-Preis 1993 ausgezeichnet.

MOLGEN$^+$ ist ein Computeralgebrasystem für Forschung und Lehre in der Chemie, das in mehrjähriger Arbeit im Rahmen von Forschungsprojekten — finanziell unterstätzt von der VW-Stiftung und von der Deutschen Forschungsgemeinschaft — am Lehrstuhl II für Mathematik der Universität Bayreuth entwickelt worden ist. Es wurde mit dem Deutsch-Österreichischen Hochschul-Software-Preis 1993 für herausragende Lehrsoftware im Fachbereich Chemie ausgezeichnet.

Dieses Computeralgebrasystem dient der *molekularen Strukturaufklärung,* deren Aufgabe die Identifizierung chemischer Substanzen anhand von spektroskopischen Daten ist. Es stellt den hierfür zentralen mathematischen Teil dar, der zu vorgegebener chemischer Summenformel samt Nebenbedingungen (vorgeschriebene und/oder verbotene Substrukturen) alle chemischen Strukturformeln ermittelt, die zu den eingegebenen Daten passen. Aus diesen Strukturformeln wird dann die zu identifizierende Substanz, genauer: deren Strukturformel, ausgelesen.

Diese Identifizierung chemischer Substanzen anhand von experimentellen Daten ist heute ein zentrales Thema in den Labors der Analytischen Chemie. Das massenhafte Auftreten solcher Probleme, beispielsweise auch im Umweltschutz, läßt den Wunsch nach Automatisierung entstehen, wenn möglich durch Computerprogramme, die die anfallenden Daten, wie Reaktionsverhalten, Spektren und ähnliche Informationen, analysieren können und dem Chemiker dann Kandidaten vorlegen — möglichst wenige, aber unbedingt *alle,* die in Frage kommen. Im Zentrum solcher Systeme steckt also notwendigerweise ein *Generator,* der in der Lage sein muß, alle mathematisch möglichen Strukturformeln zu produzieren — effizient und redundanzfrei, dies leistet MOLGEN$^+$, das bereits im industriellen Einsatz erprobt worden ist.

Innerhalb der Lehre — an Schulen, Universitäten und in der Ausbildung der chemischen Industrie — eröffnet MOLGEN$^+$ die Möglichkeit, dem Auszubildenden schnell und effektiv die Fülle der chemischen Strukturen zu demonstrieren, die vorgegebenen Daten genügen.

MOLGEN$^+$ läuft unter DOS auf dem PC, wird vom Umschau-Verlag vertrieben und ist insbesondere auch für die Lehre an Schulen und Hochschulen gedacht. Eine Industrieversion MOLGEN$^+$ ist ebenfalls erhältlich (von den Autoren), sie erfordert allerdings, je nach Ausbaustufe, erheblich mehr Speicherplatz auf der Festplatte.

Robotersteuerung

Computervorführung

Peter Kovàcs

Kurzfassung

Zur Steuerung der heute in der Industrie eingesetzten Roboter muß für jeden Robotertyp ein spezielles, kompliziertes Gleichungssystem gelöst werden. Um die Roboterhand schnell in eine gewünschte Stellung zu positionieren bzw. um die Hand schnell entlang einer vorgegebenen Bahnkurve zu bewegen muß die Lösung des jeweiligen Gleichungssystems innerhalb weniger Millisekunden erfolgen. Diese Bedingungen haben es bislang nur gestattet, sehr eingeschränkte Typen von Robotern zu realisieren.

An der TU-Berlin wurde das Expertensystem Rocky-X konstruiert, welches unter verschiedenen möglichen Varianten die jeweils optimale symbolische Lösung des obigen Gleichungssystems findet. Rocky-X gelingt dies unter anderem durch den Einsatz eines mächtigen Hilfsmittels der Computeralgebra, dem sogenannten *Buchberger-Algorithmus* sowie mittels der sogenannten *bivariaten homogenen Zerlegung.* Letztere reduziert die Lösung einer komplizierten einzelnen Gleichungen auf die sukzessive Lösung von zwei zugehörigen einfacheren Gleichungen.

Die Verwendung dieser innovativen Ergebnisse in Rocky-X ermöglicht nun die Lösung und somit die Realisierung von leistungsfähigen neuen Robotergenerationen.

Beim Einsatz von Robotern erwartet der Anwender, daß er zur Positionierung der Roboterhand in einer gewünschten Zielstellung nicht etwa Gelenkeinstellungen angeben muß, sondern daß er die gewünschte Zielstellung in einem geeigneten Koordinatensystem spezifizieren kann. Die Berechnung aller passenden Gelenkeinstellungen aus den Koordinaten der gewünschten Handstellung wird dann von der Robotersteuerung übernommen. Diese Berechnung wird als *Rückwärtsrechnung* bezeichnet.

Die Rückwärtsrechnung erfordert die Auflösung komplizierter nichtlinearer Gleichungssysteme, der sogenannten *kinematischen Gleichungssysteme*. Während der Entwicklung des Robotertyps, also vor dessen praktischem Einsatz, wird das jeweilige kinematische Gleichungssystem mittels aufwendiger, langwieriger Berechnungen auf eine Familie einzelner *(Gelenk-)Bestimmungsgleichungen* reduziert, die sich mit herkömmlichen Methoden lösen lassen. Eine solche Familie von symbolischen Bestimmungsgleichungen wird als *Triangulation* bezeichnet. Die Ermittlung einfacher Triangulationen ist das wesentliche Ziel der Rückwärtsrechnung.

Zu jedem Robotertyp existiert stets eine Vielzahl verschiedener Triangulationen, deren Qualität in bezug auf ihre praktische Einsetzbarkeit stark unterschiedlich sein kann. Die Herleitung optimaler Triangulationen war mit bisherigen Mitteln nicht möglich, da schon bei mäßig komplexen Robotern die Ermittlung einer einzigen Triangulation ein großes Problem darstellt.

Für industrielle Anwendungen müssen die Lösungen des kinematischen Gleichungssystems innerhalb weniger Millisekunden berechnet werden können. Das gelingt nur dann, wenn während der Entwicklung des Roboters eine einfache Triangulation gefunden wurde. Die Ermittlung einer einfachen Triangulation ist also eine Vorbedingung für die praktische Einsetzbarkeit eines Robotertyps. Diese Rückwärtsrechnung spielt derzeit in der Robotik eine herausragende Rolle, da sie das primäre Entwurfskriterium für Roboterkonstrukteure ist. Alle anderen Kriterien, wie zum Beispiel die Gestalt des Arbeitsraums, dynamische Eigenschaften und konstruktiv-mechanische Kriterien, wie die Anordnung der Motoren, müssen der (leichten) Lösbarkeit des kinematischen Gleichungssystems untergeordnet werden. Hierdurch wurden bislang wesentliche Entwicklungen in der Robotik behindert.

An der TU-Berlin wurde von Kovàcs und Hommel das Expertensystem Rocky-X für die Rückwärtsrechnung für umfangreiche Roboterklassen entwickelt. Rocky-X ist in der Lage, optimale Triangulationen für extrem große, bislang nicht beherrschbare Roboterklassen bereitzustellen. Unter anderem benutzt Rocky-X hierfür die folgenden Strategien, die bislang nicht in der Roboterkinematik eingesetzt wurden.

(1) Durch die Verwendung eines mächtigen Hilfsmittels der Computeralgebra, dem sogenannten *Buchberger-Algorithmus*, gelingt es, einen vollständigen Überblick über die Gesamtheit aller Triangulationen zu erhalten und einfachste Triangulationen sicher zu identifizieren. Alle wesentlichen Informationen über das kinematische Gleichungssystem können vor Beginn des eigentlichen Auflösungsprozesses ermittelt werden. Dadurch werden alle Anstrengungen gezielt auf die besten Lösungsalternativen konzentriert. Intuitive Vorgehensweisen und Fehlschläge bei der Rückwärtsrechnung können weitgehend vermieden werden.

(2) Bei vielen Robotertypen kann es sein, daß die Bestimmungsgleichungen der optimalen Triangulation immer noch zu kompliziert für den praktischen Einsatz sind, weil ihr Grad zu groß ist. Nach einem Vorschlag von Kovács läßt sich die Lösung mancher Bestimmungsgleichungen höheren Grades aber hinlänglich vereinfachen. Hierbei wird die Lösung der Gleichung großen Grades reduziert auf die sukzessive Lösung von zwei einfachen Gleichungen kleinen Grades. Die spezielle Art, wie dies geschieht, wird als *bivariate homogene Zerlegung* bezeichnet. Mit Hilfe des Computeralgebra-Systems Maple wurden von von zur Gathen für kleine Grade der Polynome sämtliche solche Zerlegungen allgemein bestimmt. Die Methode hat gegenüber der älteren funktionalen Zerlegung den entscheidenden Vorteil, daß sie auf alle Polynome anwendbar ist.

Die Verwendung dieser innovativen Ergebnisse in Rocky-X ermöglicht nun die Lösung und somit die Realisierung von leistungsfähigen neuen Robotergenerationen. Rocky-X wurde zweimal auf der Hannover-Messe als offizielles Exponat der TU-Berlin ausgestellt.

Computeralgebra im Mathematikunterricht

Computervorführungen

Wolfgang Küchlin, Beatrice Amrhein und Georg Hagel

Kurzfassung

Mit den folgenden zwei Demonstrationen wollen wir exemplarisch zeigen, welch fundamentale Auswirkungen moderne Computeralgebra-Systeme auf den Mathematikunterricht von der Oberstufe Gymnasium bis zum Vordiplom an den Universitäten und Fachhochschulen haben werden. Es wird sich zum ersten eine *Verschiebung der Lernziele* ergeben und zweitens ein *Wechsel in den Lehrmethoden*.

Es ist dabei keine Frage mehr, daß Computeralgebra die Mathematikausbildung beeinflussen wird. Durch kleine und preiswerte, aber gleichzeitig schnelle Rechner sind Computeralgebra-Systeme heute jedem Schüler zugänglich. Die Frage ist lediglich, wie offizielle Lernziele und Lehrmethoden diese Entwicklung reflektieren werden.

Mathematik ist ein unverzichtbarer Bestandteil im Problemlösungsprozeß *Problem* $\rightarrow$ *Formel* $\rightarrow$ *Resultat*. Computeralgebra hat zum Ziel, den Weg von der mathematischen Formulierung zum berechneten Resultat möglichst weitgehend zu automatisieren. Wie weit dies im Bereich des Unterrichts heute schon gelungen ist, zeigen wir am Beispiel der Lösung einiger Abituraufgaben mit dem System *Maple*.

Computeralgebra-Systeme mit anspruchsvoller Graphik eröffnen dem Lehrer qualitativ neue Möglichkeiten der Darstellung mathematischer Objekte. Der Einsatz von Computern ermöglicht zusätzlich eine maßgeschneiderte Einbindung in den Unterricht, da Darstellungen jederzeit verändert werden können und nicht starr im Lehrbuch fixiert sein müssen. Außerdem kann nun der Schüler selbst mit den Lernbeispielen experimentieren. Wie weit dies heute schon Realität ist, zeigen wir an der Visualisierung einiger Objekte mit dem System *Mathematica*.

Computeralgebra-Systeme lösen Abituraufgaben (Georg Hagel)

So wie die allgemeine Verbreitung des Taschenrechners das *von-Hand-Rechnen* im Mathematik-Unterricht ersetzt hat, so werden mit der Zeit Computeralgebra-Pakete auf Kleincomputern im Unterricht das Manipulieren von Formeln übernehmen. Das wird auch zur Folge haben, daß das Schwergewicht des Mathematik-Unterrichts verlagert wird. Im heutigen Unterricht steht oft noch das technische Handwerk im Mittelpunkt, also wie man aus der Formel das fertige Resultat erhält (Formel → Resultat).

Je mehr dieser Teil automatisiert werden kann, desto mehr Raum kann im Unterricht dem ersten Teil des Weges (Problem → Formel) gewidmet werden. Nur der Mensch kann das ursprüngliche Problem erfassen und die erste formale Modellierung erstellen. Diese Aufgabe ist sehr schwierig, da für ein Problem im allgemeinen sehr viele Modelle möglich sind. Nur durch eine genaue Kenntnis der verschiedenen Lösungsmethoden, die es je nach Modell gibt, kann das für die Lösung günstigste Modell gewählt werden. Durch den Einfluß der Computeralgebra in der Schule wird dieser Teil des Lösungswegs, und damit die konkrete Anwendung, mehr ins Zentrum verlagert.

Wie einfach sich Formelmanipulationen, wie sie heute noch in Abituraufgaben gestellt werden, durch Computeralgebra-Systeme erledigen lassen, wird an einigen Beispielen aus der Analysis mit Hilfe von *Maple* gezeigt.

Visualisierungen für den Mathematikunterricht (Beatrice Amrhein)

Visualisierung kann das Verstehen abstrakter Strukturen der Mathematik wie Funktionen, Raumkurven, Flächen, Integralen, Differentialen, Trigonometrischen Funktionen, Folgen, Reihen, usw. sehr erleichtern. Das ist besonders wichtig für Studierende, deren Stärke nicht in den mathematischen Fächern liegt.

Visualisierung fand im Mathematikunterricht bisher vor allem an der Wandtafel oder mit Hilfe eines Hellraumprojektors statt. Mit Hilfe des Computeralgebra-Systems *Mathematica* ist es nun aber möglich, schnell und einfach gute Visualisierungen abstrakter mathematischer Objekte herzustellen.

Der Computer erlaubt aber nicht nur, fertige Bilder herzustellen. Oft möchte man Bilder aus verschiedenen Ansichten betrachten oder allgemein in erstellten Bildern Parameter ändern können. Durch die Möglichkeit, Bilder zu einer Animation zusammenzusetzen, lassen sich auch kleine Filme herstellen. Damit bekommt die Visualisierung eine weitere Dimension, die Zeit. Mit den Methoden der Computeralgebra lassen sich Prozeduren herstellen, welche diese Flexibilität ermöglichen.

Ein gemeinsames Projekt (in Zusammenarbeit mit O. Gloor und Prof. R. E. Mäder, ETH Zürich) hat das Ziel, in *Mathematica* solche Prozeduren zu schreiben. Es soll damit einerseits eine Bibliothek von Visualisierungen aufgebaut werden, die direkt im Klassenzimmer eingesetzt werden können. Anderseits werden diese Prozeduren dem Lehrer zur Verfügung gestellt, so daß er auf einfachste Weise diese Bilder selber herstellen oder ändern kann.

Der Lehrer kann also aus dieser Bibliothek diejenigen Visualisierungen auswählen, welche er im Unterricht einsetzen will. Gleichzeitig kann er Änderungen an diesen Bildern leicht auch noch während des Unterrichts vornehmen und damit direkt auf Fragen von Schülern eingehen.

Auch kann dadurch im Unterricht viel mehr als bisher mit mathematischen Objekten experimentiert werden. Falls die Schüler entsprechend ausgestattet sind, können sie auch selber diese Experimente durchführen, was das Lernverhalten sicherlich verändern wird.

Lösen von Differentialgleichungen mit Computeralgebra

Computervorführung

Fritz Schwarz

Kurzfassung

Das Lösen von Differentialgleichungen ist in fast allen Gebieten der Naturwissenschaften von grundlegender Bedeutung. Die Kenntnis von *analytischen Lösungen in geschlossener Form* ist dabei von ganz besonderem Interesse, da sie *Einsichten in die Struktur* des zugrunde liegenden Problems erlauben, die durch eine numerische Lösung nicht möglich sind. Oft entscheidet sie über den weiteren Fortschritt in dem jeweiligen Gebiet. In aller Regel ist die Bestimmung solcher analytischen Lösungen mit großem Rechenaufwand verbunden. Ähnlich wie beim Integrieren verwendet man Tabellen von gelösten Beispielen und versucht, sein eigenes Problem auf eines dieser Beispiele zurückzuführen. Durch die gezeigte Software wird das Arbeiten mit Differentialgleichungen vollständig revolutioniert. Das langwierige Arbeiten mit Nachschlagewerken wird dann vollständig durch die Arbeit mit dem Computer abgelöst. Die Zeitersparnis, die Korrektheit und die Qualität der Ergebnisse sind ein enormer Gewinn und verschaffen dem Wissenschaftler Zeit für kreative Arbeit.

Das Lösen von Differentialgleichungen ist in fast allen Gebieten der Naturwissenschaften von grundlegender Bedeutung. Die Kenntnis von *analytischen Lösungen in geschlossener Form* ist dabei von ganz besonderem Interesse, da sie *Einsichten in die Struktur* des zugrunde liegenden Problems erlauben, die durch eine numerische Lösung nicht möglich sind. Oft entscheidet sie über den weiteren Fortschritt in dem jeweiligen Gebiet.

In aller Regel ist die Bestimmung solcher analytischen Lösungen mit großem Rechenaufwand verbunden. Außerdem sind die verwendeten Lösungsverfahren meist nur heuristisch, da der Rechenaufwand für systematische Verfahren noch erheblich größer ist. Ähnlich wie beim Integrieren verwendet man Tabellen von gelösten Beispielen - ein Standardwerk ist die Sammlung von Kamke - und versucht, sein eigenes Problem auf eines dieser Beispiele zurückzuführen. Falls man für eine bestimmte Differentialgleichung eine Lösung nicht findet, kann man jedoch nicht sicher sein, ob sie vielleicht doch existiert.

Die Computeralgebra ermöglicht einen fundamental neuen Ansatz. Der Rechenaufwand an analytischen Rechnungen spielt nur noch eine untergeordnete Rolle, er wird *fehlerfrei* auf dem Computer ausgeführt. Deshalb sind die verwendeten Verfahren *algorithmisch*, sie arbeiten für *ganze Klassen* von Gleichungen und erlauben *definitive Aussagen* über die Lösungen des untersuchten Problems.

In dieser Vorführung wird Software gezeigt, mit der die Lösungen linearer Gleichungen, deren Koeffizienten rationale Funktionen sind, bestimmt werden können. Als Benchmarktest wird das Kapitel 2 aus der Sammlung von Kamke verwendet. Zum Beispiel erhält man für die Gleichung

$$x^3y'' + x(2x-1)y' + y = 0$$

die beiden Lösungen

$$y_1 = \frac{1}{x}e^{-\frac{1}{x}}, \qquad y_2 = \frac{1}{x}e^{-\frac{1}{x}}\int e^{\frac{1}{x}}dx$$

oder für

$$x^2(x-2)^2y'' + 2x(x^2-1)y' - 2(x^2-x-1)y = 0$$

entsprechend

$$y_1 = \frac{x^2}{x-1}, \qquad y_2 = \frac{x^2}{x-1}\left(\frac{1}{x} + \frac{1}{x-1} + 2log\frac{x-1}{x}\right).$$

Durch diese Software wird das Arbeiten mit Differentialgleichungen vollständig revolutioniert. In wenigen Jahren werden ähnliche Algorithmen für fast alle Klassen von Gleichungen, die von praktischem Interesse sind, entwickelt und implementiert werden. Das langwierige Arbeiten mit Nachschlagewerken wird dann vollständig durch die Arbeit mit dem Computer abgelöst. Die Zeitersparnis, die Korrektheit und die Qualität der Ergebnisse sind ein enormer Gewinn und verschaffen dem Wissenschaftler Zeit für kreative Arbeit.

Die Akzeptanz dieser neuen Möglichkeiten wird durch eine benutzerfreundliche Oberfläche sehr erleichtert. Für die Eingabe bedeutet das die Möglichkeit, handgeschriebene Gleichungen in der üblichen mathematischen Schreibweise an das System zu übergeben. Das hier in Verbindung mit unserer Software gezeigte Graphiktablett, das am Lehrstuhl von Professor Hotz an der Universität Saarbrücken entwickelt wurde, löst dieses Problem auf ideale Weise. Ein jahrhunderte alter Traum der Mathematiker, ein *intelligentes Blatt Papier*, das umfangreiche und eintönige Rechnungen automatisch ausführt, ist damit in greifbare Nähe gerückt.

Neues über Systeme und Hardware

Mathcad 4.0

Bestandteil von Mathcad 4.0 ist neben den numerischen Fähigkeiten inzwischen der Kern von Maple. Mit einem Klick auf einen Menüpunkt kann Mathcad z. B. eine Formel vereinfachen oder nach einer Variable auflösen. Die symbolische Antwort steht für numerische Berechnungen oder eine weitere symbolische Umformung zur Verfügung.

Mathcad 4.0 ist erhältlich über: MathSoft, Kingswich House, Sunninghill, Berkshire SL5 7BH, Great Britain.

Berichte über Arbeitsgruppen

Computeralgebra am Interdisziplinären Zentrum für Wissenschaftliches Rechnen der Universität Heidelberg

Mitglieder der Arbeitsgruppe

- Leitung: Prof. Dr. B. H. Matzat, PD Dr. G. Hiß, PD Dr. G. Malle.
- Weitere Mitglieder: K. Brodowsky, Dr. R. Dentzer, J. Gruber, G. Kemper, Dr. F. Lübeck, R. Nauheim, U. Porsch, B. Przywara, S. Reiter.
- E-Mail: *name*`@kalliope.iwr.uni-heidelberg.de`, wobei *name* der Nachname in Kleinbuchstaben ist, also etwa

  `matzat@kalliope.iwr.uni-heidelberg.de`.

Ausnahmen: `bro` statt `brodowsky`, `hiss` statt `hisz`, `prz` statt `przywara`, `luebeck` statt `lubeck`

Arbeitsgebiete

- Mitwirkung bei Entwicklung und Pflege des Programmsystems MOC zur Berechnung von modularen Charaktertafeln und Zerlegungszahlen von endlichen Gruppen (siehe auch die Beschreibung in Abschnitt 4.4.7 des Reports „Computeralgebra in Deutschland").

  Erhältlich über K. Lux, e-mail: `Klaus.Lux@Math.RWTH-Aachen.de`

  Literatur: G. Hiß, C. Jansen, K. Lux and R. Parker: Computational Modular Character Theory. Preprint, Aachen 1993.

- Berechnung modularer Charaktere unter Verwendung von MOC als Beiträge zu einem modularen Gruppenatlas.
  Literatur: G. Hiß and K. Lux: Brauer Trees of Sporadic Groups. Oxford University Press 1989.

- Entwicklung und Pflege des Programmsystems CHEVIE für Rechnungen in der Charakter- und Darstellungstheorie von endlichen Gruppen vom Lie-Typ, von Hecke-Algebren und Weyl-Gruppen (siehe auch die Beschreibung in Abschnitt 4.4.3 des Reports „Computeralgebra in Deutschland" sowie die Ankündigung im CA-Rundbrief Nr. 13).

  Erhältlich via: `ftp.iwr.uni-heidelberg.de`

  Literatur: M. Geck, G. Pfeiffer, G. Hiß, F. Lübeck and G. Malle: CHEVIE — Generic Character Tables. IWR Preprint 93–62.

- Berechnung generischer Charaktertafeln unter Verwendung von CHEVIE als Beiträge zu einer Datenbank für generische Charaktertafeln.

- Konstruktive inverse Galoistheorie als Beitrag zur Lösung des Umkehrproblems der Galoistheorie über diversen Grundkörpern sowie der Vermutung von Shafarevich.
  Literatur: B. H. Matzat: Konstruktive Galoistheorie. LNM 1284, Springer Verlag, Berlin 1987.
  G. Malle and B. H. Matzat: Inverse Galois Theory I, II, III. IWR Preprints 92–21, 92–36, 93–46.

- Lösung geometrischer Einbettungsprobleme und Berechnung von Einbettungshindernissen im Hinblick auf geometrische Versionen des Satzes von Shafarevich über auflösbare Gruppen und der Vermutung von Shafarevich.

- Konstruktive Invariantentheorie mit Anwendungen auf das Noethersche Problem
  (INVAR-Package für MAPLE/MACAULAY).
  Literatur: G. Kemper: The INVAR-Package for Calculating Rings of Invariants. IWR Preprint 93–34

- Konstruktive Idealtheorie und nichtlineare Gleichungssysteme.

- Berechnung von Polynomen mit vorgegebener Galoisgruppe und Erstellung einer Datenbank für generische und parameterabhängige Polynome mit interessanter Galoisgruppe.

- Untersuchung von Kongruenzfunktionenkörpern und geometrischen Goppa-Codes.

Vorhandene Systeme und Software-Pakete

- Entwicklung der Systeme MOC und CHEVIE.
- Nutzung der Systeme MAPLE, GAP, MAGMA, MACAULAY, KANT, SIMATH, PARI, MUPAD.

B. H. Matzat (Heidelberg)

Publikationen über Computeralgebra

- F. Brackx: *Computer Algebra with LISP and REDUCE*, 1991, ISBN 0-7923-1441-7, Kluwer Academic Publisher, 300 S.

- W. Burckhardt: *Erste Schritte mit Mathematica*, 1993, ISBN 3-540-56650-3, Springer Verlag, Etwa 125 S.

- H. Cohen: *A Course in Computational Algebraic Number Theory*, 1993, ISBN 3-540-55640-0, Grad. Texts in Math., Springer-Verlag, Berlin-Heidelberg-New York, DM 88.–.

  Die Pioniere der "Computational Algebraic Number Theory" wie Hans Zassenhaus haben schon immer verlangt, die theoretischen Resultate der Algebraischen Zahlentheorie durch Berechnungen der behandelten Größen konstruktiv zu ergänzen, und in dem Buch von M. Pohst und H. Zassenhaus über "Algorithmic Algebraic Number Theory" ist diese Forderung bereits in die Tat umgesetzt worden. In den letzten Jahren

hat die Algebraische Zahlentheorie als arithmetische Theorie der algebraischen Zahlkörper aber zusätzliche Bedeutung in der Informatik, nämlich beim Faktorisieren großer Zahlen und bei Primzahltests, gewonnen. Dabei spielt die Arithmetik der elliptischen Kurven eine ebenso große Rolle, und man kann diese einerseits in die algebraische Zahlentheorie im weitesten Sinne und andererseits in die Arithmetische Algebraische Geometrie einordnen. Abstrakte Theorien, in effiziente Algorithmen umgesetzt, zeitigen plötzlich konkrete Anwendungen in der Informatik. Ein Lehrbuch, das dieser faszinierenden, durch Computeranwendungen gekennzeichneten Entwicklung der Zahlentheorie und Arithmetischen Geometrie gerecht wird, hat Henri Cohen nunmehr vorgelegt, und der reißende Absatz, den es offenbar findet, zeigt, wie groß der Bedarf nach einem solchen Werk ist.
Der Reichtum des behandelten Stoffes ist schier unermeßlich, und das Buch stellt eine Fundgrube sowohl für den konstruktiven Zahlentheoretiker als auch für den etwa an Faktorisierung oder kryptographischen Anwendungen interessierten Informatiker dar, um nur einige der potentiellen Benutzer zu nennen.
In den ersten drei Kapiteln werden vorbereitende Algorithmen zur Algebraischen Zahlentheorie erörtert, und zwar aus der Elementaren Zahlentheorie (z.B. der Euklidische Algorithmus, der Chinesische Restsatz, Kettenbrüche, quadratische Restsymbole und Polynomgleichungen modulo p) im ersten Kapitel, aus der Linearen Algebra und Gittertheorie (z.B. der Gaußsche Algorithmus, Determinantenberechnung und Berechung des charakteristischen Polynoms, Normalformen von Matrizen, Gitterreduktion, diverse Versionen des LLL-Algorithmus und Bestimmung der kürzesten Vektoren) im zweiten Kapitel und aus der Polynomarithmetik (z.B. Darstellung von Polynomen, Euklidischer Algorithmus, Resultantenverfahren, Faktorisierun über Z, Q und Zahlkörpern, Hensel's Lemma) im dritten.
Im vierten bis sechsten Kapitel kommt dann die Algorithmische Algebraische Zahlentheorie zum Zuge, und zwar werden im vierten theoretische Grundlagen gelegt (das Teilkörperproblem, Zerlegungsgesetz, Einheiten- und Klassengruppe, Regulator, Zetafunktion und Klassenzahlformel), im fünften Algorithmen zunächst nur für quadratische Zahlkörper erörtert (Klassenzahlberechnung mit Hilfe quadratischer Formen, Shanks'Baby Step - Giant Step-Methode zur Klassengruppenberechnung sowie Shanks' Infrastruktur-Methode zur Berechnung von Regulator und Einheitengruppe, McCurley's subexponentieller Algorithmus zur Klassengruppenberechnung, analytische Klassenzahlberechnung und Cohen-Lenstra Heuristik, wobei immer zwischen reell- und imaginärquadratischen Zahlkörpern zu unterscheiden ist) und im sechsten Kapitel schließlich Algorithmen für beliebige Zahlkörper behandelt (Ganzheitsbasenberechnung nach dem Zassenhausschen "Round 2"-Verfahren, Primzerlegung, Berechnung von Galoisgruppen für Zahlkörper vom Grade 3-7 über Q, Einheiten- und Klassengruppenberechnung, Bestimmung des Regulators, Hauptidealentscheidung, wobei kubischen Zahlkörpern ausführlichere Betrachtungen gewidmet sind). Diese Kapitel kommen dem eingangs erwähnten Buch von Pohst und Zassenhaus am nächsten, obwohl sie weniger theoretisch als praktisch orientiert sind.
In Kapitel sieben schließlich wendet sich der Autor den elliptischen Kurven zu (Elliptische Integrale, Mordell-Weil-Gruppe, komplexe Multiplikation, L-Funktion, Shimura–Taniyama–Weil–Vermutung, Vermutung von Birch und Swinnerton-Dyer, elliptische Kurven über F_q, Q und C, Hilbertsche und Webersche Klassenpolynome).
Den Anwendungen gelten die letzten drei Kapitel, und zwar Kapitel 8 der Faktorisierung von Zahlen und den Primzahltests in "the dark ages" (Pocklington-Lehmerscher $(N-1)$-Test, Pollard's ρ-Methode, Verfahren von Shanks und die $(p-1)$-Methode), Kapitel 9 den Primzahltests (mittels Jacobisummen oder elliptischer Kuven, Goldwasser-Kilian-Atkin) und Kapitel 10 der Faktorisierung (Kettenbruchmethode, Klassengruppenverfahren, Methode der elliptischen Kurven nach Lenstra, quadratisches Sieb, zahlentheoretisches Sieb) jeweils in "modern times".
Anhang A liefert eine (unvollständige) Auswahl zahlentheoretisch ausgerichteter Computeralgebra-Systeme, hauptsächlich natürlich Cohen's eigenes System PARI, und Anhang B einige Klassenzahl- und Einheitentabellen quadratischer und kubischer Zahlkörper sowie Führer, Rang (stets $= 0$) und Torsionsgruppen elliptischer Kurven.
Eine beeindruckende Materialsammlung also. Die Vorgehensweise ist nun so, daß stets zuerst die benötigte Theorie meistens kurz dargestellt wird und sich daran die entsprechenden Algorithmen anschließen. Dabei liefert der Autor gelegentlich durchaus Beweise für die benötigten Sätze, zeigt, daß die Algorithmen zum Ziel führen und erörtert ausgiebig ihre Effizienz. Wenn auf verschiedene Fälle aus Effizienzgründen verschiedene Algorithmen anzuwenden sind, so geschieht das auch und wird entsprechend kommentiert. Viele Vor- und Rückverweise erleichtern das Verständnis, Querverbindungen werden aufgezeigt und Zusammenhänge zwischen den verschiedenen Gebieten hergestellt. Am Ende eines jeden Kapitels finden sich Übungsaufgaben, die das Bild durch Beweise von Sätzen und Algorithmen, Verallgemeinerungen von Algorithmen oder Beispiele zur Theorie und zu den Verfahren abrunden.
Der Stoff erstreckt sich durchaus auf Teile der Zahlentheorie und Algebra, die *nicht* in jedem Standard-

lehrbuch behandelt werden, z.B. der Sturmsche Satz zur Bestimmung der Anzahl der reellen Nullstellen eines Polynoms und der Signatur eines Zahlkörpers nebst Algorithmus, die Newton-Formeln und Berechnung des charakteristischen Polynoms mittels Resultantenbildung, Polynomreduktion zur Erzeugung von Zahlkörpern durch "einfache" Polynome, das Newton-Polygon nebst Anwendung auf das Zerlegungsgesetz, die Cohen-Lenstra-Heuristik nebst Anwendung auf die p-Teilbarkeit der Klassenzahl und die Transformation einer kubischen Gleichung auf Weierstraß-Normalform.
Bei einem so inhaltsreichen Opus bleibt es nicht aus, daß dem Autor Auslassungen unterlaufen. Die spektakulärste ist vielleich die des zahlentheoretischen Computeralgebra-Systems SIMATH im Anhang A über "Packages for Number Theory", zumal in SIMATH eine Vielzahl der behandelten Algorithmen implementiert und verfügbar ist. Dann fehlen aber auch Hinweise auf den Ganzheitsbasenalgorithmus "Round 4" nach Zassenhaus und seine effiziente Implementierung durch Böffgen sowie auf den daraus resultierenden Algorithmus von Böffgen und Reichert zum Zerlegungsgesetz. Die ausführliche Behandlung kubischer Körper kommt offenbar ohne den Verweis auf die klassischen Arbeiten von Dedekind und Hasse aus. Und im relativ kurzen Kapitel 7 über elliptische Kurven, wo wichtige Algorithmen behandelt werden, finden sich leider keine Beweise, und es fehlen auch jegliche Literaturhinweise. Die Kapitel 9 und 10 über Primzahltests und Faktorisierung werden sich zudem bei der rasanten Entwicklung des Gebiets wahrscheinlich ziemlich bald als überarbeitungsbedürftig erweisen, indem aus den "modern times" wieder die "dark ages" werden, aber das ist unvermeidlich. Erwähnt sei noch, daß inzwischen eine lange Liste von Korrekturen vorliegt, die auf megrez.ceremab.u-bordeaux.fr via ftp verfügbar ist.
Wünschenswert wäre bei einer zweiten Auflage die Aufnahme neuerer Algorithmen zur Berechnung der Mordell-Weil-Gruppe und zur Bestimmung aller ganzen Punkte elliptischer Kurven über Q in Kapitel 7.
Insgesamt das eindruckvolle, fundamentale Werk eines kenntnisreichen Autors. Sowohl der theoretisch Interessierte als auch der praktische Anwender lernt hier eine ganze Menge. Und zum Lösen zahlentheoretischer Probleme sucht man sich einfach den passenden Algorithmus aus dem Buch heraus und implementiert ihn auf dem Rechner. Der Graduate Text vermittelt dem Leser die ganze Faszination, die von der Algorithmischen Algebraischen Zahlentheorie ausgeht.

H. G. Zimmer (Saarbrücken)

- D. V. Chudnovsky, R. D. Jenks: *Computer Algebra*, ISBN 0-8247-8038-8, 1993, Springer LNPAMS, 256 pp., $99.75.

- W. Gander, J. Hrebicek:*Solving Problems in Scientific Computing using Maple and Matlab*, 1994, ISBN 3-540-57329-1, Springer Verlag, Etwa 300 S.

- J.S. Devitt, *Calculus with Maple V*,1993, ISBN 0-534-16362-9, Symbolic Computation Series, Brooks/Cole Publishing Company, Pacific Grove, California, 502 S.

  Das Buch von J.S. Devitt eignet sich für den Einsatz in den Klassen 11 bis 13 von Gymnasien und Gesamtschulen sowie an Fachhochschulen. Es werden die Themenkreise: Gleichungen, Ungleichungen, Grenzwerte, Differentiation, rationale Funktionen, Integration, Parameterdarstellung von Funktionen und Reihen behandelt.

  Maple wird hierbei nicht in erster Linie zur Bearbeitung der gestellten Aufgaben verwandt, sondern es werden zunächst mit Hilfe von Maple die Grundlagen der Begriffe erarbeitet, ehe dann der Begriff selbst eingeführt wird. Es folgt damit dem Vorgehen, wie es auch jetzt bei der Einführung von Begriffen in der Schule üblich ist. Durch den Einsatz von Maple ist es aber möglich, die Begriffe selbst besser vorzubereiten als es bisher der Fall ist, da durch den hohen Arbeitsaufwand z.B. zum Zeichnen eines punktweise zu berechnenden Graphen die Anzahl der Beispiele sehr beschränkt ist.

  Es ist sicherlich allen Schulen zu empfehlen, die Maple zur Verfügung haben, da es ohne große Änderungen des methodischen Vorgehens eingesetzt werden kann, die einzuführenden Begriffe aber durch viele Beispiele und graphische Veranschaulichungen besser vorbereitet und verdeutlicht werden können.

U. Klein (Aachen)

- E. Johnson, *Linear Algebra with Maple V*, 1993, ISBN 0-534-13069-0, Symbolic Computation Series, Brooks/Cole Publishing Company, Pacific Grove, California, 142 S.

  Geeignet ist dieses Buch für einen Leistungskurs zum Thema Lineare Algebra an Schulen oder zur Unterstützung einer Vorlesung zur Linearen Algebra. Es wird davon ausgegangen, daß der Leser die vorgeführten Beispiele am Rechner nachvollzieht.

Es werden die Themenkreise: Matrizen, Vektoren, Eigenwerte und Eigenvektoren von Matrizen und Lineare Transformationen behandelt. Zum Abschluß eines jeden Kapitels werden Anwendungsbeispiele aus verschiedenen Bereichen vorgestellt.

Der Aufbau ähnelt dem von der Maple–Gruppe herausgegebenen Buch *First Leaves: A Tutorial Introduction*. Es werden die verwandten Maple–Kommandos angegeben und jeweils in einer links davon stehenden Spalte kurz erläutert, was mit dem entsprechenden Befehl erreicht werden soll. Daß auch die Behandlung der Themenkreise an den von Maple zur Verfügung gestellten Kommandos orientiert ist, wird in verschiedenen Abschnitten dadurch deutlich, daß zunächst alle zugehörigen Befehle mit ihrer Wirkungsweise aufgelistet werden. Die Bearbeitung der behandelten Beispiele beschränkt sich nicht auf die bloße Anwendung einzelner Kommandos, sondern es werden auch einige kleinerer Prozeduren eingesetzt.

U. Klein (Aachen)

- W. Ellis, E. Johnson, E. Lodi, D. Schwalbe, *Maple V Flight Manual*, 1992, ISBN 0-534-21235-2, Symbolic Computation Series, Brooks/Cole Publishing Company, Pacific Grove, California, 185 S.

Das Buch mit dem Untertitel *Tutorial for Calculus, Linear Algebra, and Differential Equations* ist als Einführung in Maple und zum Gebrauch an Schulen der von Brooks/Cole vertriebenen Student Edition von Maple beigefügt. Es wird die Benutzung von Maple auf einem DOS–Rechner bzw. einem Macintosh erläutert, wobei davon ausgegangen wird, daß dem Schüler ein Rechner beim Arbeiten mit dem Buch zur Verfügung steht. In einem einführenden Kapitel, das sich an den Lehrer richtet, werden die Einsatzmöglichkeiten des Buches im Unterricht erläutert.

Auch hier ist im Aufbau eine Anlehnung an das Buch *First Leaves: A Tutorial Introduction* zu erkennen. Die Kurzkommentare zu den einzelnen Maple–Kommandos sind jeweils links in einer besonderen Spalte angegeben.

Da es für die Schule gedacht ist, wird in kleinen Schritten vorgegangen und es wird z.B. der Graph einer Funktion für verschiedene Intervalle der x–Achse gezeichnet, um deutlich zu machen, an welchen Stellen die zu diskutierende Funktion näher untersucht werden soll. Insgesamt werden Kurvendiskussionen von Funktionen in einer und mehreren Variablen, Grenzwerte, Differentiation, Integration, eine Einführung in die Lineare Algebra und das Lösen von Differentialgleichungen behandelt. Maple wird hierbei als Rechenhilfsmittel benutzt und nicht zur Einführung dieser Begriffe im Unterricht.

U. Klein (Aachen)

- A. Fattahi, *Maple V Calculus Labs*, 1992, ISBN 0-534-19272-6, Brooks/Cole Publishing Company, Pacific Grove, California, 95 S.

Dieses Buch ist in 25 Abschnitte gegliedert, die jeweils während einer Sitzung am Rechner bearbeitet werden sollen. Alle Seiten sind perforiert, so daß man sie einzeln zur Bearbeitung verwenden kann. Zu Ende eines jeden Abschnitts sind Beispielaufgaben angegeben, die selbständig gelöst werden sollen. Zum Eintrag der Ergebnisse sind Zeilen im Buch vorgesehen. Die hierbei verwandten Themen kommen aus unterschiedlichen Gebieten der Mathematik. So wird z.B. die Berechnung von Grenzwerten, die Differentiation, rationale Funktionen, Integration, Differentialgleichungen, Reihen und Vektoren, aber auch das Newton–Verfahren und die Simpson–Regel jeweils an bis zu drei kurzen Beispielen behandelt. Maple wird hierbei als Werkzeug benutzt, um die gestellte Aufgabe zu bearbeiten. Auf die mathematischen Inhalte, z.B. die Wirkungsweise des Simpson–Verfahrens, wird nicht eingegangen. Als ich das Stichwortverzeichnis gesucht habe, hat mich sehr erstaunt, daß am Ende eines so dünnen Buches noch 19 leere Seiten eingelegt sind. Zur Behandlung dieser Themenkreise würde ich eines der oben vorgestellten Bücher vorziehen.

U. Klein (Aachen)

- K. G. Fischer, P. Loustaunau, J. Shapiro, E. L. Green, D. Farkas (Editors): *Computational Algebra*, ISBN 0-8247-9070-7, 1993, Springer LNPAMS, 272 pp., $125.00.

- P. Kovács: *Rechnergestützte symbolische Kinematik* , Reihe: Fortschritte der Robotik, ISBN 3-528-06544-3, 1993, Vieweg Verlag, Braunschweig, Wiesbaden, DM 112,00.

Dieses Buch ist die Veröffentlichung der Doktorarbeit des Autors in der Reihe *Fortschritte der Robotik* und ist dort der zweite von 18 Bänden, der sich mit symbolischen Aspekten bei Roboterproblemen beschäftigt. Die Parameter eines Roboters bzw. einer Roboterklasse wie Länge der Gelenke, Drehwinkel, Teleskopauszüge und Winkelstellung der Gelenke zueinander bestimmen die Position und die Orientierung der Roboterhand durch i.w. polynomiale Gleichungen. Wichtig zur konkreten Realisierung von Robotern ist es nun, die Drehwinkel etc. in Abhängigkeit von der vorgebenen Handposition zu bestimmen. Schon für einfachere Roboterklassen ist es nach dem heutigen Stand der Gröbnerbasen und der Computerleistungen nicht möglich, Gröbnerbasen zur Lösung dieses Problems durch *Triangulation* zu finden, da die Anzahl der Unbestimmten sehr hoch ist. Trotzdem ist es aus Sicht der Computeralgebra nicht hoffnungslos, diese Problematik der *inversen Roboterkinematik* zu studieren. Dem Autor kommt der Verdienst zu, Gröbnerbasis-Berechungen als Werkzeug einzusetzen, das den konventionellen Auflösungsprozeß steuert und unterstützt. Er hat dazu ein Expertensystem *ROCKY-X* implementiert, das die Gröbnerbasis-Implementierung von REDUCE benutzt. Damit konnten bislang nicht behandelbare Roboterklassen erfolgreich gelöst werden.

Im einzelnen werden nach einer Einführung in die Grundlagen der Kinematik folgende Themen behandelt: Standard-Beschreibungsmethoden von Gelenken, die klassischen Techniken der Rückwärtsrechung, die explizite Lösung von SC-Gleichungen (Polynome in Sinus/Cosinus der Winkel), Ermittlung von Triangulationen (und zwar verschiedene um möglichst einfache zu finden), Beschreibung des Kernverfahrens mit intensivem Einsatz von Gröbnerbasis-Berechungen für spezialisierte (für die geometrischen Parameter und die Handposition werden nach gewissen Regeln rationale Zahlen eingesetzt) Gleichungssysteme und Heuristiken zur Gewinnung von allgemeinen Gleichungen im Ideal etc. sowie schließlich eine Beschreibung des Expertensystems.

Am Rande sei vermerkt, daß die mathematische Präsentation mir an einigen Stellen etwas verwirrend erscheint, da z.B. die Symbole (meiner Meinung nach) unnötigerweise Indizes links oben und rechts unten besitzen. Auch könnte ich mir vorstellen, daß bei manch deskriptivem Teil des Kernverfahrens eine etwas genauere mathematische Beschreibung möglich gewesen wäre.

Ich halte das Buch für eine Bereicherung für den Computeralgebraiker und empfehle es Allen, die sich über dieses interessante Anwendungsgebiet der Gröbnerbasen-Theorie informieren und in dieses Gebiet einarbeiten wollen. Genügend zu tun in Hinblick auf Verbesserungen des Gröbnerbasis-Algorithmus in der Situation von Gleichungssystemen mit zusätzlichen Strukturen ist ja sicher noch!

Johannes Grabmeier (Heidelberg)

- Michael E. Pohst: *Computational Algebraic Number Theory*, DMV Seminar, Bd. 21, Birkhäuser Verlag Basel, Boston, Berlin 1993, 88 pp.

Dieses aus im Rahmen eines DMV-Seminars über "Konstruktive Zahlentheorie" gehaltenen Vorlesungen hervorgegangene Heft stellt im wesentlichen eine Kurzversion des Buches von M. Pohst und H. Zassenhaus über "Algorithmic Algebraic Number Theory" (Cambridge University Press, Cambridge 1989, XIV + 465 pp.) dar. Während das letztgenannte Werk aber für an direkten Anwendungen Interessierte wegen seines Allgemeinheitsanspruchs eher ungeeignet sein dürfte (vgl. das Referat von R. Schoof, Bull. AMS **29** (1993), 111 - 113), liefert die erstgenannte Monographie für direkte Anwender genau das richtige Rüstzeug. Das Hauptverdienst des vorliegenden Bändchens ist allerdings darin zu sehen, daß dem Leser ein direkter Einstieg in die "Konstruktive Algebraische Zahlentheorie" ermöglicht wird und er zudem auf kurzem Wege einen vollständigen Überblick über dieses relativ neue Gebiet der Zahlentheorie erhält. Darüber hinaus ist diese Kurzversion von Pohst-Zassenhaus in einigen Teilen, z. B. bei der Einheitenberechnung, up to date gebracht worden - ein angesichts der rasanten Entwicklung der Konstruktiven Zahlentheorie wichtiger Gesichtspunkt.

Nach H. Zassenhaus besteht die Hauptaufgabe der "Computational Algebraic Number Theory" in der Bestimmung der Galoisgruppe eines Polynoms sowie in der Berechnung von Ganzheitsbasis, Einheitengruppe und Klassengruppe algebraischer Zahlkörper. Bis auf die Bestimmung der Galoisgruppe macht die Lösung dieser Hauptaufgabe, also die Berechnung der Invarianten algebraischer Zahlkörper, den wesentlichen Inhalt der Monographie aus. Zur Vorbereitung werden in den ersten Kapiteln die benötigten Hilfsmittel aus der Theorie der endlichen Körper (Polynomfaktorisierung), der Geometrie der Zahlen (Gitter, LLL- und MLLL-Reduktion), der Linearen Algebra (Normalformen von Matrizen) und der Arithmetik der algebraischen Zahlkörper (Grundbegriffe) bereitgestellt. In einem Anhang geht der Autor noch ganz kurz auf das number field sieve nach A. K. Lenstra, H. W. Lenstra, M. S. Manasse und J. M. Pollard ein und gibt einen Abriß seines Algorithmenpakets KANT, in dem die meisten der vorher behandelten Algorithmen implementiert sind.

Die Monographie ist kurz und knapp gehalten. Einige Sätze und Propositionen werden bewiesen, für die meisten Beweise wird jedoch auf das ausführlichere Buch von Pohst und Zassenhaus verwiesen. Mit dem Computer erstellte Beispiele illustrieren die behandelten Algorithmen, und Übungsaufgaben ergänzen die präsentierte Theorie. Während die behandelten Algorithmen für direkte Anwender als Rezepte ohne weiteres verwendbar sind, muß der theoretisch Interessierte zu ihrem Verständnis an einigen Stellen wohl doch die Originalliteratur heranziehen (z. B. bei Dirichlets Methode zur Einheitenberechnung, beim Algorithmus über die Äquivalenz zweier Ideale oder beim number field sieve). Vielleicht wäre daher bei einer Neuauflage an eine etwas ausführlichere Darstellung zu denken, die möglichst "self-contained" sein sollte, ohne die Übersichtlichkeit zu beeinträchtigen.

Insgesamt stellt die Monographie eine echte Bereicherung der Literatur über Konstruktive Zahlentheorie dar und wird ihren Platz neben dem Buch von Pohst und Zassenhaus ohne weiteres behaupten können.

P.S.: Ergänzend zur Round-Four-Methode von Ford/Zassenhaus zur Berechnung einer Ganzheitsbasis sollte vielleicht erwähnt werden, daß eine frühere, sehr effiziente Implementierung des entsprechenden Algorithmus von R. Böffgen stammt (Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren. Annales Univ. Saraviensis, Ser. Math., Vol. 1, No. 3 (1987), 60 - 129) und im Computeralgebra-System SIMATH verfügbar ist.

H. G. Zimmer (Saarbrücken)

- C.C. Sims, *Computation with finitely presented groups*, ISBN 0-521-43213-8, 1994, Cambridge University Press, xiii + 604 pp., $ 99.00.
- B. Sturmfels: *Algorithms in Invariant Theory*, 1993, ISBN 3-211-82445-6, Springer Verlag, 197 S.

  Dies ist der erste Band der Reihe:

  > Hrsg.: B. Buchberger, G. E. Collins: *Texts and Monographs in Symbolic Computation*, Johannes Kepler University, Linz, Austria

- M. C. Tangora, *Computers in Algebra*, ISBN 0-8247-7975-4 1993, Springer LNPAMS, 176 pp., $99.75.
- Wen-tsün Wu: *Mechanical Theorem Proving in Geometries*, 1994, ISBN 3-211-82506-1, Springer Verlag, Etwa 250 S.
- R. Zippel: *Effective Polynomial Computation*, 1993, ISBN 0-7923-9375-9, Kluwer Academic Publisher, approx. 376 pp.

Lehrveranstaltungen über Computeralgebra im SS 1994

- **RWTH Aachen**
  Algebra II (Mathematische Methoden der CA), Neubüser, V4, Ü2.
  Einführungspraktikum Maple, Neubüser, Klein, Dietrich, Ü2.
  Praktikum: Programmieren in Maple, Neubüser, Klein, Ü2.
- **FU Berlin**
  Invariantentheorie und Computer Algebra, K. Gatermann, S.
  Problemlösen mit Mathematica, Köpf, S2.
- **Universität Bonn**
  Primalitätstests und Faktorisierungsalgorithmen, A. Shokrollahi: , V2.
- **Universität Erlangen**
  Methoden der Computeralgebra: Arithmetik endlicher Körper, H. Meyn, M. Becker-Wenneker, V3, Ü1.
- **Universität Heidelberg**
  Angewandte Computeralgebra ,W. Böge,v4, Ü2.
  Computeralgebra (Algorithmen der Gruppentheorie), G. Hiß, V2, Ü2.
- **Universität Karlsruhe**
  Computeralgebra in der Robotik, J. Calmet, V.
  Computeralgebra und Künstliche Intelligenz, Calmet, J., Homann, K., Zenger, C., S.
  Computeralgebrapraktikum, Calmet, J., Homann, K., Zenger, C., P.
- **Universität Kaiserslautern**
  Algebra II (Computeralgebra), G. Pfister, V.
  Computeralgebra, G. Pfister, S.

- **Universität Köln**
  Elliptische Kurven und Faktorisierung, N. Klingen, S2.

- **Universität Leipzig**
  Computergeometrie, W. Laßner, V2.
  Konstruktive Invariantentheorie, H.-G. Gräbe, V2.
  REDUCE-Praktikum, H.-G. Gräbe, P2.
  Oberseminar Computeralgebra, H.-G. Gräbe, W. Laßner, S2.

- **RISC Linz**
  Überblick über Symb. Computation, B. Buchberger, F. Winkler, V2.
  Geometrische Grundlagen für Symbolic Computation, S. Stifter,V2.
  Algorithmische Kombinatorik, P. Paule, V2.
  Rewriting in Computer Science and Logic, F. Winkler , V2.
  Quantifier Elimination, G. Collins, V2.
  Mathematikunterricht mit DeriveII , B. Kutzler, V2.

- **Universität Mannheim**
  Anwendungen der Computer-Algebra in Mathematik, VWL und BWL. H. Kredel, H.-G. Kruse, K2.

- **Universität-Gesamthochschule Paderborn**
  Mathematik am Computer, Chr. Nelius: V4.
  Konstruktive Galoistheorie, Chr Nelius: V2, Ü2.
  Primzahltests, K.H. Indlekofer, J.Jarai: V2, Ü1.
  Rechnen in endlichen Koerpern, von zur Gathen: V2.
  Elementare Algorithmen in der Computeralgebra, B. Fuchssteiner: V2.
  MuPAD Seminar, MuPAD Gruppe: S2.
  Automath Seminar, N. Dourdoumas,B. Fuchssteiner, J. Lueckel, F. Rammig: S2.
  Oberseminar Faktorisieren, von zur Gathen: S2.

- **Universität Passau**
  Oberseminar Computeralgebra, V. Weispfenning, S2.

- **Universität Rostock**
  Symbolisches Rechnen I, K. Hantzschmann, V2.
  Maple, O. Becken, V1, Ü1.
  Algebraische Programmierung, U. Lämmel, V2.
  Termersetzungssysteme, A. Widiger, S2.

- **Universität des Saarlandes Saarbrücken**
  Algorithmen in Algebra und Zahlentheorie, H. G. Zimmer, S2.

- **Universität Tübingen**
  Einführung in das Symbolische und Algebraische Rechnen, R. Loos, V2
  Praktikum Symbolisches und Algebraisches Rechnen, R. Loos, P4
  Seminar Computeralgebra, R. Loos, S2
  Seminar Formale Methoden der Hardware-Verifikation, R. Bündgen, U. Kebschull, W. Küchlin, S2
  Gröbner-Basen, B. Amrhein, V2 + Ü1

- **ETH Zürich**
  Computer Algebra II, B. F. Caviness, V2, Ü1.
  Computer Algebra Seminar, M. Bronstein, R. Mäder, C. Williamson, S2.

Kurze Mitteilungen

- An der Rheinisch–Westfälischen Technischen Hochschule Aachen ist eine neu eingerichtete

  Universitätsprofessur (C4)

  für technisch-wissenschaftliches Hochleistungsrechnen

  zu besetzen.
  Es ist beabsichtigt, der Inhaberin oder dem Inhaber dieser Professur die wissenschaftliche Leitung des Rechenzentrums zu übertragen. Dabei soll dieses unter besonderer Berücksichtigung der Hochleistungsrechnertechnologie zu einem Kompetenzzentrum an der RWTH entwickelt werden. Einstellungsvoraussetzungen sind Habilitation oder gleichwertige wissenschaftliche Leistungen sowie pädagogische Eignung.
  Die Bewerberinnen und Bewerber werden gebeten, sich mit den üblichen Unterlagen(Lebenslauf, Darstellung des wissenschaftlichen bzw. beruflichen Werdegangs, Schriftenverzeichnis) bis zum 31. März 1994 an den Dekan der Mathematisch-Naturwissenschaftlichen Fakultät, RWTH Aachen, Templergraben 64, D-52056 Aachen zu wenden.

- **STELLENAUSSCHREIBUNG**

  Universität-GH Paderborn

  Lehrstuhl für Algorithmische Mathematik

  An diesem neu eingerichteten Lehrstuhl sind zum Sommersemester 1994 zwei Stellen als
  Wissenschaftliche Mitarbeiter

  zu besetzen. Besoldung nach BAT IIa, Vierjahresvertrag. Bei in der Laufzeit abgeschlossener Promotion kann Verlängerung um ein weiteres Jahr erfolgen.
  Forschungsgebiete: Algorithmen für die Computeralgebra; effizientes Rechnen in endlichen algebraischen Strukturen, insbesondere endlichen Körpern (Faktorisieren von Polynomen, Permutationspolynome, Normalbasen); algebraische Komplexitätstheorie. Anwendungen: Kodierungstheorie, Kryptographie, Robotik.
  Voraussetzung: Diplom in Mathematik oder Informatik. Auch promovierte Bewerber sind eingeladen, sich zu bewerben.
  Auskunft erteilt: Joachim von zur Gathen, Department of Computer Science, University of Toronto, Toronto, Ontario, Canada M5S 1A4, E-Mail: gathen@cs.toronto.edu, Phone: (416) 978-6024, Fax: (416) 978-1931

- Der Springer-Verlag, Postfach 31 13 40, D-10643 Berlin, bei dem bisher 15 Bücher zu Computeralgebraerschienen sind, gibt einen eigenen Prospekt zu Computeralgebra heraus.

- In der ersten Nummer der neuen Zeitschrift

  > Hrsg: T. Ciriani, B. Kernighan, C. Wolfram: *Mathematech, The Global Review of Mathematics and its Applications*, Parrish Platt International

  befinden sich unter anderem auch Artikel zu Themen der Computeralgebra:

  – C. Wolfram on Mathematica
  – D. Pinchon on AXIOM.

- **European Academic Software Award '94**
  Der Europäische Akademische Software Preis, eine gemeinsame Initiative von verschiedenen europäischen Organisationen, auf deutscher Seite die ASK Karlsruhe, ruft alle europäischen Autoren von Software-Produkten, die an einer Universität oder höheren Erziehungs- oder Forschungseinrichtung beschäftigt sind, zur Unterbreitung ihrer Entwicklungen bis zum 30.4.1994 auf.

- Im Rahmen des RISC, Linz, erscheint eine neue Reihe für Monographien:

Hrsg.: B. Buchberger, G. E. Collins: *Texts and Monographs in Symbolic Computation*, Johannes Kepler University, Linz, Austria

This series publishes research monographs and textbooks by researchers and visiting researchers of the Research Institute for Symbolic Computation at the University of Linz, Austria.

- Journal Announcement and Call for Papers for a Full-Service, Refereed Electronic Mathematics Journal:

  THE NEW YORK JOURNAL OF MATHEMATICS

  The New York Journal of Mathematics is a refereed mathematics journal being launched by the University at Albany, State University of New York.

  The journal is broadly based in subject matter, covering algebra, modern analysis, and geometry/topology.

  The New York Journal will be accessible by a combination of listserv and gopher/ftp (*gopher nyjm.albany.edu*, *ftp ftp_nyjm.albany.edu* in the directory */pub/nyjm*).

  Mark Steinberger, The University at Albany, State University of New York Editor in Chief, New York Journal of Mathematics

- Prof. Paulo Ney de Souza in Berkeley führt eine Liste von Computeralgebra-Systemen, die einen Teil der Berichte im Report Computeralgebra in Deutschland abdeckt bzw. ergänzt.

  Zugriff erfolgt entweder via anonymous ftp auf `math.berkeley.edu` im Directory `pub/Symbolic_Soft` oder via Gopher mit der
  `Document URL gopher://math.berkeley.edu/00/Symbolic_Soft`.

- **Gopher-Zugang der eLib**

  Das Informationssystem der Fachgruppe Computeralgebra, die eLib am Konrad-Zuse-Institut in Berlin, ist neben dem bisherigen telnet-Zugang nun auch über Gopher erreichbar. Gopher ist ein weltweites Informationssystem, das auf dem Client-Server-Modell beruht. Die Client-Software am Arbeitsplatz kann mit einem Server (üblicherweise der Server des lokalen Rechenzentrums) Kontakt aufnehmen und wird von diesem dann an andere Server bei Bedarf weiterverwiesen.

  Da auch das Konrad-Zuse-Institut einen solchen Gopher-Server betreibt, ist die eLib direkt von der jeweiligen Client-Software ansprechbar. Damit entfällt für den Nutzer die Notwendigkeit, sich wie bisher über Zeilenkommandos in die jeweiligen Menuepunkte vorzutasten, statt dessen kann mouse-gesteuert gesucht werden.

  Erforderlich ist lediglich die Client-Software am Arbeitsplatz, die für unterschiedliche Betriebssysteme auf PD-Servern bereitgehalten wird. Im UNIX-Bereich setzt sich sehr schnell die Mosaic-Oberfläche durch. Der offizielle Server für dieses Produkt ist `ftp.ncsa.uiuc.edu`, allerdings ist die Software an den meisten Rechenzentren in angepaßter Form bereits im Einsatz und sollte zur Entlastung der internationalen Verbindungen auch von dort bezogen werden.

  Das Standard-Einstiegs-Menü Ihres lokalen Gopher-Servers hat auch den Punkt *Externe Informationssysteme*, der auf den zentralen deutschen Gopher-Server in Clausthal-Zellerfeld verweist. Von dort geht es per Mouse-Klick weiter nach Berlin an den Gopher-Server des ZIB, der den Menu-Punkt `SIG(Opt-Net, Computeralgebra)` enthält. Wer direkt in das Menu will, kann im Mosaic über `OPEN...` auch die
  `Document URL gopher://serv03.zib-berlin.de/11/.sig/Computeralgebra` benutzen.

  Gerhard Schneider (Karlsruhe)

- Diesem Rundbrief liegt eine Informationsbroschüre des Birkhäuser-Verlags bei.