Nummer 24 **März 1999**

Mitteilungen der Sprecher

Liebe Mitglieder der Fachgruppe Computeralgebra,

am 5. März fand die letzte Sitzung der alten Fachgruppenleitung und im Anschluß daran die konstituierende Sitzung der neuen Fachgruppenleitung in Leipzig statt. Der Wahlleiter, Prof. Hantzschmann, gab das Ergebnis der Wahl bekannt. Es wurden keine ungültige und 141 gültige Stimmen abgegeben, die sich folgendermaßen verteilten.

Dr. Johannes Grabmeier	*Heidelberg*	*99*
Prof. Dr. Volker Weispfenning	*Passau*	*94*
Prof. Dr. G.-M. Greuel	*Kaiserslautern*	*66*
Prof. Dr. H. Michael Möller	*Dortmund*	*57*
Prof. Dr. Adalbert Kerber	*Bayreuth*	*54*
Prof. Dr. Michael E. Pohst	*Berlin*	*52*
Prof. Dr. Gerhard Schneider	*Göttingen*	*49*
Prof. Dr. Wolfram Koepf	*Leipzig*	*46*
Prof. Dr.-Ing. Dr. rer.nat. Volker Strehl	*Erlangen-Nürnberg*	*46*
Dr. Joachim Apel	*Leipzig*	*44*
Heiko Knechtel	*Stadthagen*	*43*
Dr. H.-W. Henn	*Karlsruhe*	*42*
Prof. Dr. Wilhelm Werner	*Heilbronn*	*42*
Dr. Hans-Gert Gräbe	*Leipzig*	*36*
Prof. Dr. Gerhard Hiß	*Aachen*	*35*
Prof. Dr. Gunter Malle	*Kassel*	*33*

Damit sind die ersten neun Kandidaten gewählt. Die weiteren sieben Kandidaten sind in der Reihenfolge der Stimmenverteilung auf der Nachrückliste.

Mit den neu benannten, bzw. bestätigten Vertretern der Trägergesellschaften, den Herren

K. Hantzschmann (GI), B. H. Matzat (DMV), S. E. Rump (GAMM),

und den gemäß unserer Ordnung nach 7.1 berufenen Fachexperten, den Herren

F. W. Hehl (Physik), W. Werner (Fachhochschulen), H. Knechtel (Schulen),

ist die neue Fachgruppenleitung für die Amtszeit 1999 – 2002 komplett. Wir danken den nicht gewählten Kandidaten für ihre Bereitschaft, sich zur Wahl zu stellen und sich auch weiterhin für die Belange der Fachgruppe Computeralgebra einzusetzen. Gleicher Dank gilt den Wahlleitern, Herrn Hantzschmann und Herrn Matzat. für die Durchführung der Wahl !

In seinem Rechenschaftsbericht ging der scheidende Sprecher, Herr Grabmeier, auf die wichtigsten Ereignisse und Aktionen der vergangenen drei Jahre ein. Höhepunkt war zweifellos das International Symposium on Symbolic and Algebraic Computations *im Jahr 1998 (ISSAC'98). Diese weltweit wichtigste Computeralgebratagung findet jährlich statt. Die ISSAC'98 wurde von der Fachgruppe initiiert und von ihr mit Unterstützung der GI organisiert. Die lokalen Organisation stand unter der Leitung von Karl Hantzschmann aus Rostock. General Chair war Volker Weispfenning aus Passau.*

Die gelungene Veranstaltung (vgl. den letzten Rundbrief) war ein Prestigegewinn für die Computeralgebra in Deutschland und auch finanziell ein Erfolg. International ist die Fachgruppe durch ihren Sprecher weiterhin im ISSAC-Leitungsgremium vertreten.

Zur Förderung der Computeralgebra im Schulbereich, einem der Hauptziele in der vergangenen Amtsperiode, hatte die Fachgruppe im Sommer 1997 die Ministerien der 16 Bundesländer angeschrieben und angeboten, zum Thema Curriculumsentwicklung Computeralgebra *mit ihnen in die Diskussion zu treten. Die Resonanz bislang dazu war sehr positiv.*

Im April 1998 wurde deshalb ein Symposium zu Thema Computeralgebra in Lehre, Ausbildung und Weiterbildung *in Schloß Thurnau im April 1998 veranstaltet. Die organisatorische Verantwortung lag bei A. Kerber aus Bayreuth. Ein Bericht über dieses Symposium war im letzten Rundbrief zu lesen.*

Von Herrn W. Werner wurde im März 1998 ein Workshop Computeralgebra in Forschung und Lehre *an der Fachhochschule in Künzelsau organisiert, vgl. Heft 22 des Rundbriefs. Dieser Workshop wurde von der Fachgruppe unterstützt. Desweiteren wurden wie auch in den vorangegangenen Amtszeiten Computeralgebra-Sektionen bzw. Workshops auf den Jahresversammlungen unserer Trägergesellschaften zum Teil von Mitgliedern der Fachgruppenleitung organisiert bzw. mitgetragen.*

Die wichtigste Informationsquelle der Fachgruppe, der Computeralgebra-Rundbrief, wurde auch in dieser Amtsperiode wieder von Herrn Schwardmann in bewährter Weise redaktionell betreut. Die alte Fachgruppenleitung bedankte sich herzlich bei ihm für die geleistete Arbeit. Die von Herrn Schneider betreuten WWW-Seiten CAIS sind von Karlsruhe zur GWDG nach Göttingen umgezogen. Dieser Umzug ist noch nicht ganz abgeschlossen. Trotzdem auch jetzt schon Dank an Herrn Schneider für seine Arbeit.

Die Initiative der Fachgruppe zum weit gefaßten Thema Benchmarks in der Computeralgebra *hat mit der Einberufung eines Treffens unter der Leitung von Heinz Kredel aus Mannheim am Rande der ISSAC-Konferenz in Rostock einen wichtigen Schritt unternommen. Sein Referat und eine strukturierte Zusammenstellung der bislang bekannten Aktivitäten finden Sie im CAIS.*

Der scheidende Sprecher der Fachgruppe dankte allen Mitgliedern der Fachgruppenleitung 1996 – 1999 für die geleistete Arbeit.

Nach der Entlastung der Sprecher der alten Fachgruppenleitung hat sich die neue Fachgruppenleitung konstituiert. Da Herr Grabmeier nicht erneut kandidierte, wurde unter seiner Leitung der neue Sprecher gewählt. Einstimmig fiel die Wahl auf H.M.Möller. Ebenfalls einstimmig wurde M. Pohst zum Stellvertreter gewählt.

Für die kommenden drei Jahre sollen die bisherigen Arbeitsschwerpunkte wieder durch Referenten der Fachgruppenleitung besonders gefördert werden. Die bisherigen Referenten Schneider (für CAIS), Koepf (Didaktik und Lehre), Kerber (Chemieanwendungen) wurden bestätigt, Herr Strehl kommt als Referent für Computational Engeneering hinzu. Weitere wichtige Schwerpunkte in der neuen Amtsperiode werden die Gebiete Computeralgebra in der Physik, Benchmarks, Computeralgebra an Fachhochschulen und an Schulen sein. Während wir für die Benchmarks einen Referenten aus den eigenen Reihen noch zu finden hoffen, werden die anderen drei Schwerpunkte durch Fachexperten in unserer Fachgruppenleitung vertreten. Wie in der letzten Amtsperiode sind Herr F.W. Hehl für die Physik und Herr W. Werner für die Fachhochschulen zuständig. Herr Knechtel ist jetzt Fachexperte für Schulen. Diese Berufung war nur dadurch möglich, daß Herr Schwardmann auf seine Funktion als Fachexperte verzichtete, denn wir dürfen satzungsgemäß maximal drei Fachexperten in der Fachgruppenleitung haben. Herr Schwardmann wird aber weiterhin den Rundbrief betreuen und an den Sitzungen der Fachgruppenleitung als verantwortlicher Redakteur teilnehmen.

H. Michael Möller *M. Pohst*

Hinweise auf Konferenzen

1. **GAMM-Jahrestagung**

   Metz, Frankreich, 12.4. – 16.4.1999

   Tagungsleitung: Marcel Berveiller (Metz), Alfred Louis (Saarbrücken).

   Eine der 25 Sektionen ist dem Thema *Computeralgebra und -analysis* gewidmet. Die Anmeldung der 15-Minuten-Beiträge geschieht bis zum 15.11.1998 mittels eines Vortragsformulars. Weitere Informationen über `http://www.lpmm.univ-metz.fr/gamm99`.

2. **ECCAD'99 – The East Coast Computer Algebra Day '99**

   Raleigh, North Carolina, USA, 24.4.1999

   Objective: Present/discuss current research on requirements, challenges, trends, recent algorithmic advances, tools in applications and in education, in an informal/interactive setting.

   Organizers: Hoon Hong (North Carolina State Univ. USA), Erich Kaltofen (North Carolina State Univ. USA), Dinesh Manocha (Univ. of North Carolina USA), John Reif (Duke University USA), Michael Singer (North Carolina State Univ. USA).

   Invited Speakers: Peter Borwein (Simon Fraser Univ. Canada), Gaston Gonnet (ETH Switzerland), Lakshman Y. N. (Bell Labs USA).

Publications: Abstracts of Posters/Demos in ACM-SIGSAM bulletin. Details in the WEB page `http://vega.math.ncsu.edu/`

Registration: FREE! but need to register for local arragement. Details in the WEB page `http://vega.math.ncsu.edu/`

Travel Support: Some funds are avaible. Details in the WEB page `http://vega.math.ncsu.edu/`

3. Neues Lernen mit Neuen Medien - Mathematikunterricht in der Zukunft

Münster, 25.5. – 28.5.1999

Die 3.Pfingsttagung an der WWU Münster wird in diesem Jahr von der Zentralen Koordination Lehrerausbildung der WWU in Zusammenarbeit mit dem Landesinstitut für Schule und Weiterbildung, Soest, mit Unterstützung von T^3 Europe veranstaltet.

Tagungsablauf:
25.5. Neues Lernen/Neue Medien – selbstständige Schülerinnen, HV: E. Lehmann
26.5. Neues Lernen/Neue Medien – Glasperlenspiel zwischen Problem und Anwendung, HV: G. Steinberg
27.5. Neues Lernen/Neue Medien – aber bitte mit Prüfung!, HV: J. Elschenbroich
28.5. Neues Lernen/Neue Medien – nur Motivation und Faszination?, HV: C. Laborde.

Aktuelle Informationen finden Sie unter `http://www.uni-muenster.de/Lehrerausbildung/ti92tag.html`

4. COCOA – VI, and An International School on Computer Algebra

Villa Gualino, near Turin, Italy, 31.5. – 5.6.1999

This year will see some innovations in the style of the proceedings. The COCOA meeting proper will be preceded by a three and a half day intensive School on Computer Algebra, offered to a limited number of doctoral students and recent post doctoral fellows. The School will be followed by two and a half days of the COCOA meeting, in its more usual format, i.e. invited lectures, contributed papers and demonstrations of computer algebra systems.

Dates:
School: monday, may 31. - thursday, june 3.1999
COCOA VI: thursday, june 3 - saturday, june 5.1999

COCOA VI: As mentioned above, the COCOA VI meeting will formally begin on Thursday afternoon (June 3) and continue until Saturday afternoon (June 5). The meeting will take place in the Villa Gualino.

There is space in the programme for a limited number of research communications and demonstrations. We encourage potential speakers to submit abstracts for consideration by the Organizers. They should be submitted by email to either Geramita or Robbiano at the email addresses given above.

The International School: There will be two intensive courses offered in the School:
Course A: Monomial Ideals - B. Sturmfels
Course B: Ideals of Points - A. Geramita, L. Robbiano
(Assistants for the Courses: A. Bigatti, M. Kreuzer)

There is space for at most 18 participants, who should currently be enrolled in a doctoral programme somewhere in the world or be recent post doctoral fellows. All students who are accepted for admission to the School will receive a scholarship which will cover some of the expenses associated with their participation. Those wishing to participate in the School should submit a "letter of application" by email to either

Lorenzo Robbiano `robbiano@dima.unige.it` or
Anthony Geramita `geramita@dima.unige.it` or `tony@mast.queensu.ca`

Included in this Letter of Application should be the (email) address of one mathematician who can act as referee for the application as well as a statement as to why the application is being made.

Applications should be submitted by March 1, 1999 and the final decisions will be made by March 15, 1999 by the Organizing Committee (V. Ancona, A. Conte, A. Geramita, L. Robbiano).

Those accepted to participate in the School are expected to arrive at the Villa Gualino by Sunday evening, May 30 (as the courses will begin on Monday morning) and remain at least until midday on Thursday, June 3. All participants in the School are encouraged (but not obliged) to remain for the COCOA VI meeting, which will begin in the afternoon of June 3.

5. CASC-99 The Second Workshop on Computeralgebra in Scientific Computing

München, 31.5. – 4.6.1999

Topics: The methods of Scientific Computing play an important role in research and engineering applications in the field of the natural and engineering sciences.

The importance of computer algebra methods and computer algebra systems for scientific computing has increased considerably in recent times. During the last decade, a new generation of general-purpose computer algebra systems such as Mathematica, Maple, MuPAD and Axiom have been developed, which enable the user to solve the following three important tasks within a uniform framework of the same system: symbolic manipulations, numerical computations, visualization.

A further development of such systems, including their adaptation to parallel environments, puts them at the forefront in scientific computing and enables the practical solution of many complex applied problems in the domains of natural sciences and engineering knowledge.

Topics for CASC unites many important questions and methods of Scientific Computing and the application of computer algebra, like numerical simulation using computer algebra systems, parallel symbolic-numeric computations, symbolic-numeric interfaces, symplectic integration, construction of approximate solutions of differential, equations and dynamical systems, symbolic-numeric methods in celestial mechanics and general, relativity, algebraic methods for nonlinear equations and inequalities, computer algebra methods in pure mathematics, computational group theory, applications to the theory of error-correcting codes, problem-solving environments for partial differential equations, algorithmic and complexity considerations in computer algebra.

The workshop is intended to provide a forum for researchers and engineers in the fields of mathematics, informatics, numerical analysis, etc. An important goal of the workshop is to unite all these specialists for the purpose of an efficient solution of many current questions and problems in advanced Scientific Computing.

Workshop co-chairs: Vladimir Gerdt (Dubna), Ernst Mayr (Munich).

Program Committee: Victor Edneral (Moscow), Marc Gaetano (INRIA, Sophia), Victor Ganzha (Munich, co-chair), Richard Liska (Prague), Roman Maeder (Zuerich), Yuri Matiyasevich (St. Petersburg), Stanly Steinberg (Albuquerque), Nikolay Vassiliev (St. Petersburg), Evgenii Vorozhtsov (Novosibirsk, co-chair), Paul S. Wang (Kent), Volker Weispfenning (Passau), Christoph Zenger (Munich).

Local Organizing Committee: Herbert Fischer, Victor Ganzha, `ganzha@in.tum.de`,
Ernst Mayr (chair), `mayr@in.tum.de`, Michal Mnuk (secretary), `mnuk@in.tum.de`,

Proceedings: It is planned to have proceedings published by Springer Verlag, containing the full papers and available at the Workshop.

Location: The workshop will take place in a conference center in Herrsching (Lake Ammersee), about 30km from the city of Munich and easily reached from there by public transportation.

Important dates: (these are still tentative)
15 Jan 1999 Submission of the full paper (up to 20 pages) or extended abstract (up to 4 pages)
20 Feb 1999 Notification of acceptance
20 May 1999 Camera-Ready papers must be received
2 May 1999 Deadline for advance registration at Workshop

Notes: In addition to submitted research papers, these will also be invited talks and software presentations.

Further, updated informations are available at:

`http://wwwmayr.informatik.tu-muenchen.de/konferenzen/CASC99/`

6. MATHTOOLS'99 – 2nd International Conference "Tools for Mathematical Modelling"

Saint-Petersburg, Russia, 14.6. – 19.6.1999

MATHTOOLS'99 is a multidisciplinary conference on latest advances in the theory of mathematical modelling and the role of the theory for explanation of some nonlinear effects arising in real systems as well as demonstration of up-to-date efficient methods for solving of applied technical problems, providing an ideal forum for researchers to disseminate knowledge, research results and applications in many sectors of activity. This will be the second of a series of conferences initiated in 1996, and organized by the State Technical University of Saint-Petersburg. Conference sessions will be started by a 1-hour invited lecture followed by contributed papers, 20 minutes each. Invited talks will highlight some of the major accomplishments, trends and problems in the theory.

Working languages: The working languages are English and Russian.

Topics of interest: Papers may address a broad range of research fields of current interest. A list of possible topics includes (but is not limited to) the following:

Mathematical modelling, Computer algebra, Design techniques, Numerical methods, Parallel and distributed algorithms, Computer modeling in dynamical systems, Mathematical models in biology, medicine, ecology etc., Applications to physics, electrotechniques and electronics, Dynamic economic models, General macro-economic models, Market models.

Organizing committee: Chairman - G.S.Osipenko (St.Petersburg Technical University)

Secretary - Yuri Ivanov (St.Petersburg Technical University)

Scientific committee: Gillian Tardivel (UK), Alexander Kasterin (Russia), Daniel Dytte (Denmark), Mika Seppala (Finland), Giorggio Picci (Italy), Benno Fuchssteiner (Germany), Alexei Zhizchenko (Russia), Olga Plechova (Russia), Jens Hugger (Denmark), Flemming Topsoe (Denmark), Sergei Znamensii (Russia), Marian Mrozek (Poland), Valeriy Tkachenko (Ukraine), Leonid Belous (Ukraine), Vyacheslav Zavadskii (Belorussia), Vasiliy Malozemov (Russia), Alexander Petukhov (Russia).

Dates to remember:
Abstracts due: April 30, 1999
Registration form: April 30, 1999
Meeting in St. Petersburg: June 14-19, 1999.

Abstract: The paper selection for the meeting will be made on the basis of an abstract. This should describe, in 1-2 complete pages, the objectives, methods and techniques if applicable, essential results already obtained and conclusions of the work.

Abstract in camera-ready copy must be sent by normal mail (2 copies), to the meeting secretariat. As rule we do not use an electronic version of abstract.

Notify the organization by e-mail to: `lab@osipenko.stu.neva.ru`, `math@math.hop.stu.neva.ru`

Meeting secretariat: Yuri Ivanov, MATHTOOLS'99, Dept. of Mathematics, State Technical University, Polytechnicheskaya st., 29, St.Petersburg 195251, Russia, Fax.: +7+812+5343314, +7+812+5341404.

Meeting site: Saint-Petersburg State Technical University, Polytechnicheskaya st. 29, St. Petersburg

Proceedings:

It is suggested to publish Proceedings of the meeting, including all papers accepted for presentation and invited talks.

Registration fees: Participant: 100 (US dollars), Student: 25 (US dollars), Participant from the Former Soviet Union (FSU-participant): 25 (US dollars).

We hope to reduce the fee for Russian participants as Russian Foundation for Basic Research gives a support.

For the publication of abstracts it is necessary to bring in an advance payment at a rate of 100 roubles to the address (to write in Russian): 193231, St.-Petersburg, John Rid street, house 7, flat 255, Ivanov Yuri

7. IMACS Conference on Applications of Computer Algebra 1999

El Escorial (near Madrid), Spain, 25.6. – 27.6.1999

Recent information: `http://math.unm.edu/ACA/1999.html`

Organizers:

Honorary President: Rafael Puyol (Rector of the Universidad Complutense de Madrid) *General Chair:* Eugenio Roanes-Lozano (Univ. Complutense de Madrid, Spain) *Program Chairs:* Victor Edneral (Moscow State Univ., Russia), Laureano Gonzalez-Vega (Univ. de Cantabria, Spain), Jaime Gutierrez (Univ. de Cantabria, Spain) *Organizing Committee:* Stanly Steinberg (Univ. New Mexico, USA), Michael Wester (Cotopaxi, USA), Eugenio Roanes-Macias (Univ. Complutense de Madrid, Spain), Luis Laita (Univ. Politecnica de Madrid, Spain) *Local Committee:* Martin Garbayo (Univ. Complutense de Madrid, Spain), Mercedes Hidalgo (Univ. Complutense de Madrid, Spain), Dolores Rodriguez-Soalleiro (CPR Leganes)

Methods for admitting talks:

a) This conference is organized in "sessions". A proposal for organizing a session must be submitted to the program chairs who decide upon its acceptance.

b) A proposal for a talk is sent directly to the corresponding "session organizer", who acts as referee of the paper or extended abstract (possibly together with members of the scientific committee and/or experts in the subfield), and decides upon the acceptance of the proposal.

Call for invited sessions: The Program Committee is soliciting proposals for invited sessions. Proposals should be sent to the program chairs. Information about current sessions can be found in our web site.

Call for papers: Full papers or extended abstracts should be directly sent to the corresponding session organizer.

Proceedings: There are no printed proceedings. Extended abstracts or full papers are available at the web site. Some session organizers have published the papers presented in their sessions in special volumes of well known journals such as "Mathematics and Computers in Simulation", the "Journal of Symbolic Computation", "The International Journal of Computer Algebra in Mathematics Education"...

Keynote Lectures: The following invited speakers have confirmed their willingness to give a 1 hour talk at the conference (as in previous IMACS-ACA, there will be no plenary lectures, and these talks will take place within normal sessions):

Victor Edneral (Moscow State Univ., Russia) Title: Computer Algebraic Approximations - Creation of Approximated Solutions of Scientific and Engineering Problems in Symbolic Form,
Richard Liska (Tech. Univ. Prague, Czech Republic), Title: Applications of Quantifier Elimination,
Tomas Recio (Univ. de Cantabria, Spain), Title: Missing points and branches of real parametric curves,
Stanly Steinberg (Univ. New Mexico, USA), Title: The Study of Stability using Computer Algebra.

The session "Education" Call for Submissions for the session Ëducationïn the frame of the 1999 IMACS-ACA (Applications of Computer Algebra) Conference.

Education has become one of the fastest growing application areas for computers in general and computer algebra in particular. Computer algebra tools such as TI-92/89, DERIVE, MATHEMATICA, MAPLE, AXIOM, REDUCE, MACSYMA, or MUPAD make powerful teaching tools in mathematics, physics, chemistry, biology, economy e.a. .

The goal of this session is to exchange ideas and experiences, to hear about classroom experiments, and to discuss all issues related with the use of computer algebra tools in classroom (such as assessment, change of curricula, new support material, ...)

If you have anything of the above which you would like to share with colleagues in the inspiring atmosphere of an IMACS-ACA conference, then please make a submission comprising title, author(s), abstract (10 lines min, 20 lines max).

Format of submission: Plain ASCII text in English. (The presentation itself may be in English or Spanish as there will be a simultaneous English/Spanish interpretation available throughout the Education Session.)

Deadline for submission: April 23, 1999

The session: "Applications of Quantifier Elimination"

Organizers: Volker Weispfenning and Hoon Hong

What is Quantifier Elimination? Quantifier elimination for the real numbers is a very comprehensive and flexible tool for handling a large variety of problem types in real algebra and geometry. It is a paradigm for a generic algorithm in computer algebra, since it deals with parametric problems uniformly for all real values of the parameters. The roots of the method date back to the real root counting algorithms of Descartes, Budan, Fourier, Sturm, Sylvester and Hermite. Formally established by Tarski in the 1930s, it has developed rapidly since the 1960s, leading to a first completely implemented method by Collins in 1975. Since then intensive research has lead to asymptotically more efficient approaches and to other universal and special purpose implemented quantifier elimination methods.

Applications of Quantifier Elimination. During the last few years the power of these implementations has increased in such a way that serious problems from many diverse application areas have come into the realm of these methods. They include:
– Real implicitization of parametric algebraic surfaces.
– Automatic theorem proving and finding in real geometry.
– Geometric reasoning about three-dimensional objects, including parallel and central projections of objects, the reconstruction of objects from projections, lighting and shading, equi-distance surfaces.
– Rounding,blending and boundary representation of solids.
– Collision and motion planing in robotics.
– The Birkhoff interpolation problem.
– Sign behaviour of univariate polynomials.
– Implementation of guarded expressions for coping with degenerate cases in the evaluation of algebraic expressions.
– Stability analysis for ode's and pde's.
– Control theory.
– Simulation and error diagnosis of technical networks.
– Non-convex parametric linear and quadratic optimization problems.
– Parametric scheduling.

Topics of the session The session is intended as a forum for surveys on the current status of real quantifier elimination,related methods, and applications, and for new ideas in the field. The organizers also encourage software demonstrations relevant to the field.

The session will include two one hour *invited keynote lectures* presented by
Richard Liska (Tech. Univ. Prague, Czech Republic), Title: "Applications of Quantifier Elimination" and
Stanly Steinberg (Univ. New Mexico, USA), Title: "The Study of Stability using Computer Algebra"

8. Explicit Methods in Number Theory

Oberwolfach, 4.–10.7.1999

Veranstalter: H. Cohen, H. W. Lenstra, D. B. Zagier

9. Workshop Algorithmic Galois Theory

Dagstuhl, 19.–23.7.1999

Organizing Committee: B. H. Matzat, J. McKay, K. Yokoyama.

The **main topics** of the workshop will be the direct Galois problem, the inverse Galois problem, special Galois groups, generic polynomials and complexity considerations.

One of the **purposes** of this meeting is to collect contributions to a special volume of the Journal of Symbolic Computation, devoted to this subject and edited by the organizers.

Further informations are available via email from `matzat@iwr.uni-heidelberg.de`

10. ISSAC'99 – International Symposium on Symbolic and Algebraic Computation

Vancouver, Kanada, 29.7. – 31.7.1999

ISSAC is a yearly international symposium that provides an opportunity to learn of new developments and to present original research results in all areas of symbolic mathematical computation.

Conference activities The planned activities include invited presentations, research and survey papers, poster sessions, tutorial courses, vendor exhibits, and software demonstrations. Proceedings will be distributed at the symposium.

Proposals for workshops, tutorial courses, demonstrations, panel discussions, or related activities are welcome. User-groups, editorial boards, or other associations desiring meeting space during the course of the symposium are encouraged to contact the conference organizers.

Conference Location: ISSAC'99 will be held at Simon Fraser University in Vancouver, British Columbia. The University maintains a campus in the centre of Vancouver, called the Harbour Centre. It is close to hotels, restaurants, and shopping.

Organizing Committee:
General Chair: Keith Geddes, Dept. of Computer Science, University of Waterloo, Waterloo ON N2L3G1, CANADA, (1) 519-888-4567 Ext. 4668, `issac99@cecm.sfu.ca`.
Program Chair: Bruno Salvy, Projet ALGO, INRIA Rocquencourt, 78153LeChesnayCedex, FRANCE, (33) 1 39 63 55 20, `Bruno.Salvy@inria.fr`.
Local Arrangements: Michael Monagan, Dept. of Math and Statistics, Simon Fraser University, Burnaby BC VSA1S6, CANADA, (1) 604-2914279, `monagan@cecm.sfu.ca`.

Conference Topics: Topics of the meeting include, but are not limited to:
Algorithmic mathematics: Algebraic, symbolic, and symbolic-numeric algorithms including: simplification, polynomial and rational function manipulations, algebraic equations, summation, integration, linear algebra and matrix computations, number theory, ODE/PDE, complex computation, group computations, and geometric computing.

Computer science: Theoretical and practical problems in symbolic mathematical computation including: computer algebra systems, problem solving environments, programming languages and libraries for symbolic computation, user interfaces, data structures, software architectures, parallel/distributed computing, mapping algorithms to architectures, concrete analysis and benchmarking, complexity of computer algebra algorithms, artificial intelligence techniques, automatic differentiation and code generation, mathematical data exchange protocols.

Applications: Problem treatments incorporating algebraic, symbolic or symbolicnumeric computation in an essential or novel way, including engineering, economics and finance, physical and biological sciences, computer science, logic, mathematics, statistics, and use in education.

Instructions to Authors: ISSAC '99 is foremost a conference for new and topical ideas of significance to the community and which deserve to be disseminated rapidly. Research results and insightful analyses of current concerns are the primary focus. Papers will be reviewed by a program committee and additional referees.

Survey articles may be suitable for submission, if clearly identified as such, and will be considered in a separate category from the research papers.

Simultaneous submission for publication elsewhere is not allowed.

Papers must be in English and should not exceed 8 pages in the standard format for ACM proceedings, or 20 to 22 pages of text in LaTeX 12pt article style. The necessary files for article and bibliography style can be obtained from the ISSAC '99 web site `http://www.cecm.sfu.ca/ISSAC99/`. Each paper should have an introductory section that: (1) Describes the problem; (2) Motivates the study of the problem; (3) States the main results; (4) Compares other work (including theoretical or empirical performance); and (5) Summarizes the original contribution.

Further information: `http://www.cecm.sfu.ca/ISSAC99/` .

11. EQUADIFF 99

Berlin, 1.8 – 7.8.1999

Diese Konferenzreihe ist allen mathematischen Aspekten von Differentialgleichungen gewidmet und findet im zweijährigen Wechsel in Tschechien/Slowakei oder in einem westeuropäischen Land statt. Es sind 37 Minisymposia geplant, eines davon unter der Leitung von J. Sanders behandelt in der Gruppierung *Computational Aspects* das Thema *Computer Algebra Tools*. Weitere Informationen im Internet auf der Seite `http://www.math.fu-berlin.de/~equadiff/`.

12. ICTMT4 – The Fourth International Conference on Technology in Mathematics Teaching

Plymouth, England 9.8. – 13.8.1999

About ICTMT: The first International Conference on Technology in Mathematics Teaching was held in Birmingham, England in 1993. The conference is held every two years; ICTMT2 was held in Edinburgh, Scotland and ICTMT3 was in Koblenz, Germany. The aim of the conference is to bring together classroom practitioners, curriculum developers and mathematics education researchers, all of whom share a desire to improve the quality of student learning. ICTMT4 is being held in Plymouth, England from 9th to 13th August 1999. The conference is being organised jointly by the Centre for Teaching Mathematics at the University of Plymouth and the University College of St. Mark and St. John, Plymouth. The strands of the conference will be in conjunction with the themes of ICTMT and will be . using technology in the teaching and learning of mathematics in schools . using technology in the teaching and learning of mathematics in college and university . applications of technology to teaching other subjects which are also of interest to mathematics educators . applications of technology in industry and commerce which are also of interest to mathematics educators A solar eclipse provides a special theme: There is a major event of astronomical interest on 11th August 1999 with a total eclipse of the sun. One of the best places in Europe to experience the totality of the eclipse is in the South West of England. The conference has been organised around this date and in the strand "applications of technology to teaching other subjects which are also of interest to mathematics educators" the application of mathematics to astronomy will feature prominently. Throughout the week there will be activities associated with the eclipse.

The themes of ICTMT are the impact of technology on teaching and learning, access to education through technology, technology and assessment, ways forward - future trends in technology in mathematics.
The programme will consist of invited plenary lectures by distinguished speakers, contributed presentations, workshops, discussion groups, poster presentations.

All talks and workshops will be refereed by members of an International Programme Committee. Particular emphasis will be given to providing opportunities for formal and informal interaction between conference participants. To facilitate this there will be discussion groups and a social event each day.

Local Conference Committee: John Berry and Roger Fentem (joint Conference Chairmen), Karen Eccles (Conference secretary), Jenny Sharp (Academic programme), Ted Graham (Social programme), Tony Churchley (Exhibition coordinator), Michael McCabe (University of Portsmouth, Astronomy theme).
Contributions: There will be three forms of contributions to ICTMT4: talks of 30 minutes duration, workshops of 75 minutes using computers or handheld technology, posters A1 size. Your contribution should fall into one of the strands of the conference. To submit a contribution for ICTMT4 please send an abstract (maximum 500 words) describing your talk or workshop to the address below (email contributions preferred, attached files should be Word 6 for Windows 3.1).
Conference Address for Correspondence: Karen Eccles, The Centre for Teaching Mathematics, The University of Plymouth, Drake Circus, Plymouth PL4 8AA, England Phone: +44 (1752) 232772 Fax: +44 (1752) 232772 email: `keccles@plymouth.ac.uk`
ICTMT4 - WEB address: `http://www.tech.plym.ac.uk/maths/CTMHOME/ictmt4.html`
Timetable:
Call for Papers, Workshops, Posters: 1st September 1998
Bookings taken from: 1st September 1998
Deadline for Submissions: 31st December 1998
Initial Programme available: 1st April 1999

13. Recent Research on DERIVE/TI-92-Supported Mathematics Education

Gösing, Österreich, 25.8. – 28.8.1999

This conference is the fifth in a series of conferences on DERIVE and/or TI-92-supported mathematics education initiated by ACDCA: Krems (Austria) 1992, Krems 1993, Honolulu (USA) 1995, Sarö (Sweden) 1997.

Typical **topics** within the scope of the conference are: - Reports about successful classroom experiments,
- New ways of mathematics teaching and learning,
- Improvements in the design of mathematics software systems based on mathematical experience,
- Examples of successful, new computer-based mathematics texts, lectures, training units, etc.,
- Influence on assessment,
- Similar studies with other computer algebra systems.

How to submit: Please send title and abstract (15-20 lines) to Bernhard Kutzler. E-mail address: `b.kutzler@eunet.at`, Postal address: Kariglstrasse 5/6, A-4060 Leonding, Austria

Time table:
May 15, 1999: Deadline for submissions
May 31, 1999: Notification of acceptance and publication of a detailed program
June 25, 1999: Deadline for early bird registration.

Conference Co-chairmen: Josef Böhm: `nojo.boehm@pgv.at`, Helmut Heugl: `hheugl@netway.at`, Bernhard Kutzler: `b.kutzler@eunet at`.

14. IMS 99 – International Mathematica Symposium

Linz, Österreich, 26.8. – 29.8.1999

The Symposium is organized by RISC (Research Institute for Symbolic Computation) on behalf of the IMS 99.

For more information, please visit `http://www.risc.uni-linz.ac.at/conferences/summer99/ims99/`

Scope: Principal topics of interest are applications of computer algebra and in particular Mathematica in mathematics, computer science, the physical and biological sciences, economics, engineering, the arts, and education. The conference will provide a forum for researchers and users from diverse fields to present original work, and to learn about current developments and uses of advanced scientific computing. Besides keynote lectures and contributed papers, the symposium offers tutorials, discussion forums, poster presentations and software demonstrations.

Conference venue: The "International Mathematica Symposium IMS99" is organized by the Research Institute for Symbolic Computation (RISC) of the Johannes Kepler University Linz. The conference will be held in the Castle of Hagenberg, the home of RISC.

Hagenberg is located about 25km North-East from Linz, Austria.

Contributed Papers: Authors are invited to submit a 1-page abstract to the organizers by December 31, 1998. In order to facilitate submissions by persons with limited access to the internet and/or typesetting facilities, we will accept submissions in the following three forms:
– Email: plain ASCII text, to `veikko.keranen@ramk.fi` .
– Ordinary mail: Gautam Dasgupta, 620 Mudd, Columbia University, New York, NY 10027, USA.
– Fax: Gautam Dasgupta, at 1-212-854-6267.

Important dates:
December 31, 1998: Deadline for the submission of papers.
February 15, 1999: Decision about papers and notification of authors.
August 26-29, 1999: Conference.

Program Committee: Paul Abbott, University of Western Australia, Australia; Bruno Autin, CERN, Geneva, Switzerland; Vladimir Buber, Murmansk State Technical University, Russia Greg Chaitin, IBM, USA; Gautam Dasgupta, Columbia University, USA; Vladimir Demidov, Murmansk State Pedagogical Institute, Russia; Bradford Garton, Columbia University, USA; Alexander Georgiev, Albemarle Corporation, USA; Juha Haataja, CSC-Center of

Scientific Computing, Finland; Allan Hayes, De Montfort University, UK; Antero Hietamaki, Rovaniemi Polytechnic, Finland; Christian Jacob, University of Erlangen-Nuremberg, Germany; Jarkko Kari, Iterated Systems Inc., USA; Veikko Keranen, Rovaniemi Polytechnic, Finland; Robert Kragler, Fachhochschule Ravensburg-Weingarten, Germany; Shigeki Matsumoto, Konan University, Japan; Philip Miller, Carnegie-Mellon University, USA; Alexander Papusha, Murmansk State Technical University, Russia; Henry Power, Wessex Institute of Technology, UK; Philip Ramsden, Imperial College, UK; Jack Robertson, US Military Academy, USA; Heikki Ruskeepaa, University of Turku, Finland; Susumu Sakakibara, Iwaki Meisei University, Japan; Dana Scott, Carnegie-Mellon University, USA; Felix Ulmer, Université de Rennes, France; Paul Wellin, WRI, USA.

15. DMV – Jahrestagung 1999

Mainz, 5.9. – 11.9.1999

Die Tagung findet vom 5. September (Anreisetag) bis zum 11. September 1999 an der Johannes-Gutenberg-Universität Mainz statt. Das wissenschaftliche Programm beginnt am 6. September und endet am Nachmittag des 10. September. Vormittags sind Plenarveranstaltungen für die Hauptvorträge und nachmittags Sitzungen der Sektionen vorgesehen.

Im Zusammenhang mit der Tagung werden die ordentliche Mitgliederversammlung der DMV und auch Sitzungen der Fachgruppen stattfinden. Für den 8. und 9. September ist die Studentenkonferenz Mathematik vorgesehen. Ein Tag wird der Lehrerfortbildung gewidmet sein und ein Nachmittag interessierten Schülerinnen und Schülern. Allen Teilnehmenden und ihren Begleitpersonen wird ein vielseitiges Rahmenprogramm angeboten. Um die Öffentlichkeit an mathematischen Themen zu interessieren und Schulklassen in die Erlebniswelt Mathematik einzuführen, ist eine Ausstellung "Mathematik zum Anfassen" im Rathaus-Foyer geplant. Verlage werden ihre neueste Literatur, Softwarehäuser ihre neuesten System-Kreationen präsentieren; auch an eine Firmenpräsentation ist gedacht. Aktuelle Information ist zu finden unter `http://www.mathematik.uni-mainz.de/DMV99/`

16. ALCOMA99 Euroconference – Algebraic Combinatorics and Applications

Gößweinstein bei Bayreuth, Deutschland 12.9. – 19.9.1999

The aim of the conference is to bring together leading researchers from mathematical theory (including related computer science) and its applications in chemistry and physics in order to stimulate fruitful interdisciplinary discussions and to generate an impact regarding future research in this area.

Topics to be presented: Finite group actions, other combinatorial tools like generating functions, species and computer algebra, applications of combinatorics in chemistry, connection of mathematics with physics, a special emphasis will be on the presentation of related software packages

Current list of **keynote speakers:** M. Clausen: Computational Representation Theory and Fast Fourier Transforms, A. Dress:New Approaches to Clustering Theory, D. Foata: to be announced, P. Fowler: Systematics of the Fullerenes - Enumeration, Construction and Characterisation, J. Grabmeier: to be announced, I. Gutman: The Energy of a Graph: Old and New Result, A. Lascoux: Bruhat order on affine Coxeter groups, R. Laue: Constructing objects up to isomorphism, T. Lulek: Group actions and classification of quantum states of Heisenberg model of magnetism, A. Morris: The combinatorics of the character theory of some group extensions, P. Paule: to be announced, V. Strehl: to be announced, K. Varmuza: From spectral data via isomer generation to chemical structure, K. H. Zimmermann: to be announced.

Further information is available on the WWW: `http://www.mathe2.uni-bayreuth.de/home/alcoma99.html` .

17. Computeralgebra-Symposium Konstanz (CASK)

Konstanz, 9.3. – 10.3.2000

Örtliche Tagungsleitung: Prof. Dr. Elkedagmar Heinrich, Dr. Hans-Dieter Janetzko

Nähere Informationen ab Ende März über die Homepage der FH: `http://www.fh-konstanz.de`

Adresse: Fachhochschule Konstanz, Brauneggerstr. 55, 78462 Konstanz, Email: `heinrich@fh-konstanz.de` .

18. Computeralgebra in Lehre, Ausbildung und Weiterbildung

Thurnau, 26.-28. April 2000

Aufgrund des großen Erfolgs der ersten Tagung dieser Art, welche vom 22.-25. April 1998 in Thurnau stattfand, veranstaltet die Fachgruppe Computeralgebra (FG CA) im Frühjahr 2000 eine zweite Tagung zum Thema *Computeralgebra in Lehre, Ausbildung und Weiterbildung* über den Einsatz von Computeralgebrasystemen im Unterricht.

Ziel ist es, den im ersten Treffen initiierten Austausch zwischen den Kultusministerien, den für die Fortentwicklung der curricularen Lehrpläne zuständigen Instituten und den Experten aus Wissenschaft, Lehre und Schule weiterzuführen. Wir erhoffen uns insbesondere wieder Berichte über die in den einzelnen Bundesländern stattfindenden Lehrversuche und über geplante Lehrplanreformen.

Verantwortlich ist das Organisations- und Programmkomitee in Zusammenarbeit mit der Fachgruppe Computeralgebra. Es besteht aus

- Prof. Dr. A. Kerber, Bayreuth (FG CA, Leitung und lokale Organisation),
- Prof. Dr. Wolfram Koepf, Leipzig (FG CA, Referent für Lehre und Didaktik),
- Heiko Knechtel, Bückeburg (FG CA, Fachexperte Schule),

- Dr. Günter Schmidt, Mainz (MNU),
- Prof. Dr. Günter Törner, Duisburg (Fachgruppe Didaktik der Mathematik der DMV) und
- Prof. Dr. Hans-Georg Weigand, Gießen (Gesellschaft für Didaktik der Mathematik).

Wegen des auf ca. 45 Teilnehmer beschränkten Umfangs bitten wir um frühzeitige Anmeldung bei Prof. Kerber oder Prof. Koepf (s. Adressen Fachgruppenleitung).

Berichte von Konferenzen

1. Algorithmen und Zahlentheorie

Dagstuhl, 12.10. – 30.10.98

Leiter:
H. Niederreiter, Academy of Sciences, Vienna, Austria,
A. M. Odlyzko, AT&T Florham Park, USA,
M. E. Pohst, TU Berlin, Germany.

This seminar was the third one on number theoretical algorithms at Dagstuhl over the past 7 years. A major goal was always to bring together number theorists who develop the theory for efficient algorithms and people writing the corresponding software for applications. This year we had 42 participants from 13 countries.

In the last few years number theoretical applications to Coding Theory and Cryptography have become more and more important. Hence, it was no surprise that the majority of talks was on topics related to these applications.

G. Frey: Arithmetic of Modular Curves; F. Morain: Elliptic Curves and Primality Proving; A. Pethö: $pm1$ Representations of Integers; K. Geißler: Computation of Galois Groups; C. Fieker: Constructive Classfield Theory; M. Olivier: The Class Number One Problem for some Non-Abelian Normal CM-Fields; I. Gáal: Power Integral Bases in Algebraic Number Fields; H. Cohen: Efficient Computations on Elliptic Curves; F. Lemmermeyer: Elliptic Curves and 2-Class Field Towers of Cubic Fields; J.-M. Couveignes: Isomorphisms between Artin-Schreier Towers; H.-G. Rück: Elliptic Curves and Discrete Logarithms; M. Holder: A Sequential Implementation of the Black-Box Niederreiter Algorithm for Factoring Polynomials over GF(2); B. Vallée: Average Analysis of Various Euclidian Algorithms: Dynamical Methods and Functional Analysis; A. Schiemann: An LLL Algorithm for Totally Positive Lattices over Number Fields; H. te Riele: Numerical Verification of the Conjecture of Ankeny, Artin, and Chowla for the Primes $< 10^{11}$; E.-U. Gekeler: Zeroes of Eisenstein Series; S. Schmitt: The Mordell-Weil Group of Elliptic Curves over Number Fields; M. Conrad: Bases of Cyclotomic Units; R. Schertz: Numerical Construction of Class Fields by Elliptic Functions; K. Nakamula: Actual Computation of Units by the Cyclo-Elliptic Method; J. von zur Gathen: Finite Field Algorithms; I. Shparlinski: Distribution of Residues of Exponential Functions and some Algorithmic Problems; D. Coppersmith: Divisors of Residue Classes, Constructively; V. Shoup: Efficient Computation of Minimal Polynomials of Extensions of Finite Fields; H. Dobbertin: New Permutation Polynomials and Applications; F. Leprevost: On some Elliptic Surfaces and Elliptic Curves Related to Discriminants of Cubic or Quartic Polynomials; D. Bernstein: Ten Topics in Computional Number Theory; J. Klüners: Explicit Galois Realizations of Transitive Groups of Degree up to 15; S. Paulus: Function Fields with a Totally Ramified Prime at Infinity; E. V. Flynn: Chabauty Techniques; A. Stein: A Kangaroo Approach to Function Fields; T. Herend'i: Uniform Distribution of Recurrence Sequences Modulo Prime Powers; D. Ford: Polynomial Factorization over Q_p via the Zassenhaus Round Four Algorithm; S. Gao: Polytopes and Polynomials;

C. Fieker (Berlin)

Polynomial Decomposition

Polynomial decomposition is the problem of representing a given polynomial $f(x)$ as a functional composition $g(h(x))$ of polynomials of smaller degree. Polynomial decomposition is useful in simplifying the representation of field extensions of high degree and is provided as a primitive by many major symbolic algebra systems. Decomposition problems for multivariate polynomials and for rational and algebraic functions are also of interest.

The theory of polynomial decomposition was initiated by Ritt in 1922 [19] and further developed in [9, 8]. A survey was presented in [20]. Decompositions of $f(x) \in F[x]$ are intimately related to the intermediate fields between $F(f)$ and $F(x)$ [8, 19].

The problem breaks into two cases, the *tame* and the *wild*. The tame case is when the characteristic of F does not divide the degree of g, including characteristic 0. In the tame case, the problem is rational—that is, if f decomposes over an extension of F, then it decomposes over F [20]—and maximal decompositions are unique up to insertion of linear decomposition factors and commutativity of powers of x and Chebyshev polynomials [19]. Both facts may fail in the wild case [8, 20].

The first analyzed algorithms for decomposition of polynomials were provided by Barton and Zippel [3] and Alagar and Thanh [1], who considered polynomials over fields of characteristic zero. Both solutions involved polynomial factorization and took exponential time. For some time, the problem of finding nontrivial decompositions was considered to be computationally hard; a cryptographic protocol was based on its supposed intractability [5].

Kozen and Landau [17] discovered the first polynomial-time algorithms in the tame case that do not require factorization. The time bounds were $O(n^3)$, $O(n^2)$ if F supports an FFT. A similar algorithm was discovered independently by Gutierrez et al. [15]. Kozen and Landau also gave efficient NC algorithms (parallel polylog time on polynomially many processors) with a time bound of $O(\log^2 n)$. In the wild case, they reduced the problem to factorization and gave an $O(n^{\log n})$ algorithm for the decomposition of irreducible polynomials over general fields admitting a polynomial-time factorization algorithm and an NC algorithm for irreducible polynomials over finite fields. The sequential bounds in the tame case were improved by von zur Gathen [10] to $O(n \log^2 n \log \log n)$, $O(n \log^2 n)$ if F supports an FFT. He also gave an improved algorithm for the wild case, yielding a polynomial-time reduction to factorization, and observed undecidability over sufficiently general fields [11].

Several extensions and variations have been investigated. Dickerson [7] and von zur Gathen [10] investigated the decomposition of multivariate polynomials. Gutierrez [13] gave a polynomial decomposition algorithm over factorial domains. Von zur Gathen and Weiss [12] gave an exponential method for finding decompositions of the form $f(x) = g(h(x), k(x))$ for homogeneous $g(y, z)$. Casperson et al. [6] gave an algorithm that, given an irreducible $f(x)$, finds $g(x)$ and $h(x)$ such that $f(x)$ divides $g(h(x))$. Binder [4] gave a fast method to compute the Lüroth generator of the union field of two polynomials.

Hommel and Kovács [16] defined and investigated the *sine-cosine decomposition problem*: determine whether a given bivariate polynomial $f(s, c)$ has a decomposition of the form $f(s, c) = g(h(s, c)) \bmod s^2 + c^2 - 1$. This problem has applications in robot kinematics. Gutierrez and Recio [14] gave a cubic-time algorithm that does not require factorization. It is based on approximating a root of $f(s, c) \bmod s^2 + c^2 - 1$.

Zippel [21] presented a polynomial-time algorithm to decompose rational functions over any field admitting efficient polynomial factorization. His approach uncovers a strong relation to Lüroth's theorem. Alonso et al. [2] gave two exponential-time algorithms for rational function decomposition that compare favorably with Zippel's in practice. They also presented several applications: faithful reparametrization of unfaithfully parameterized curves, computing intermediate fields in a simple purely transcendental extension of F, and providing a birationality test for subfields of $F(x)$.

Kozen, Landau, and Zippel [18] addressed the decomposition problem for algebraic functions. They uncovered a connection to univariate resultants over algebraic function fields and showed that the decomposition problem essentially asks whether some power of a given irreducible bivariate polynomial

$f(x, z)$ can be expressed as the resultant with respect to y of two bivariate polynomials $g(x, y)$, $h(y, z)$. They determined necessary and sufficient conditions for the existence of a nontrivial decomposition and classified all such decompositions up to isomorphism. They also gave an exponential-time algorithm for finding a nontrivial decomposition if one exists.

Jaime Gutierrez (Cantabria) and Dexter Kozen (Cornell)

Literatur

[1] V. S. Alagar and M. Thanh. Fast polynomial decomposition algorithms. In *Proc. EUROCAL85*, pages 150–153. Springer-Verlag Lect. Notes in Comput. Sci. 204, 1985.

[2] C. Alonso, J. Gutierrez, and T. Recio. A rational function decomposition algorithm by near-separated polynomials. *J. Symbolic Computation*, 19:527–544, 1995.

[3] D. R. Barton and R. E. Zippel. Polynomial decomposition algorithms. *J. Symb. Comp.*, 1:159–168, 1985.

[4] F. Binder. Fast computations in the lattice of polynomial rational function fields. In *Proc. ISSAC-96*. ACM Press, 1995.

[5] J. J. Cade. A public key cipher which allows signatures. In *Proc. 2nd Conf. on Appl. Linear Algebra*. SIAM, 1985.

[6] D. Casperson, D. Ford, and J. MacKay. An ideal decomposition algorithm. *J. Symbolic Computation*, 21(2):133–137, 1996.

[7] M. Dickerson. Polynomial decomposition algorithms for multivariate polynomials. Technical Report TR87-826, Comput. Sci., Cornell Univ., April 1987.

[8] F. Dorey and G. Whaples. Prime and composite polynomials. *J. Algebra*, 28:88–101, 1974.

[9] M. D. Fried and R. E. MacRae. On curves with separated variables. *Math. Ann.*, 180:220–226, 1969.

[10] J. von zur Gathen. Functional decomposition of polynomials: the tame case. *J. Symb. Comput.*, 9:281–299, 1990.

[11] J. von zur Gathen. Functional decomposition of polynomials: the wild case. *J. Symb. Comput.*, 10:437–452, 1990.

[12] J. von zur Gathen and J. Weiss. Homogeneous bivariate decompositions. *J. Symbolic Computation*, 19:409–434, 1995.

[13] J. Gutierrez. A polynomial decomposition algorithm over factorial domains. *Comptes Rendus Mathematiques de l'Academie des Sciences*, 13(2–3):81–86, April-June 1991.

[14] J. Gutierrez and T. Recio. Advances on the simplification of sine-cosine equations. *J. Symbolic Computation*, 26:31–70, 1998.

[15] J. Gutierrez, T. Recio, and C. Ruiz de Velasco. A polynomial decomposition algorithm of almost quadratic complexity. In *Proc. AAECC-6/88*, volume 357 of *Lect. Notes in Comput. Sci.*, pages 471–476. Springer-Verlag, 1989.

[16] G. Hommel and P. Kovács. Simplification of symbolic inverse kinematic transformations through functional decomposition. In *Proc. of the Conference Adv. in Robotics*, pages 88–95, 1992.

[17] D. Kozen and S. Landau. Polynomial decomposition algorithms. *J. Symb. Comput.*, 7:445–456, 1989.

[18] D. Kozen, S. Landau, and R. Zippel. Decomposition of algebraic functions. *Journal of Symbolic Computation*, 22(3):235–246, September 1996.

[19] J. F. Ritt. Prime and composite polynomials. *Trans. Amer. Math. Soc.*, 23:51–66, 1922.

[20] A. Schinzel. *Selected topics on polynomials.* University of Michigan Press, 1982.

[21] R. E. Zippel. Rational function decomposition. In Stephen Watt, editor, *International Symposium on Symbolic and Algebraic Computation*, pages 1–6, New York, July 1991. ACM.

Neues über Systeme und Hardware

Macsyma 2.4 for PCs and Macsyma 422 for UNIX

Macsyma(r) 2.4 for PCs with MS-Windows 95, 98, and Windows NT is now shipping. Macsyma 422 for UNIX systems is now shipping on Linux and five other Unix operating systems.
Macsyma 2.4 further enhances the help system. When users enter questions in their own words, Macsyma 2.4 makes "smarter" executable suggestions. One of the most appreciated new features in Macsyma 2.4 is a very simple one: color-coding of matching parentheses in input expressions makes it much easier to interpret multi-line input. Areas in Macsyma 2.4 with significant mathematical improvements include integration, solution of equations, linear algebra of sparse matrices, graph theory, special functions, and graphics. New Features of PC Macsyma 2.4 and of UNIX Macsyma 422 are here:
`http://www.macsyma.com/mx24nu.htm`

Macsyma Inc. (Arlington)

Das 'Mobile Klassenzimmer' am Isolde-Kurz-Gymnasium in Reutlingen

Die bisherigen Unterrichtsversuche mit Computeralgebra-Systemen zeigen, daß sich der Mathematikunterricht insbesondere in den Klassen 11 bis 13 stark verändern wird, wenn jede Schülerin und jeder Schüler über einen mobilen Computer ein Computeralgebra-System einsetzen kann. Um Erfahrungswerte über solche Veränderungen zu bekommen, hat im Rahmen des Leitprojekts "Bildung vernetzt" das Teilprojekt "Mobiles Klassenzimmer" höchste Priorität erhalten. Die Landesregierung hat deshalb am 15. Januar 1996 das Kultusministerium beauftragt, das "Pilotprojekt Mobiles Klassenzimmer" durchzuführen. Das Projekt wird seit dem Schuljahr 1996/97 beginnend mit vier Klassen der Klassenstufe 11 durchgeführt. Die Ausstattung mit mobilen Computern soll den Schülerinnen und Schülern ermöglichen, in der Schule und zu Hause interaktiv Lernprogramme zu nutzen, im projektorientierten Unterricht arbeitsteilig Lösungen zu entwickeln, Unterrichtsmaterialien zu kommunizieren oder auch Online-Infodienste abzufragen (Ministerium für Kultus und Sport, Baden-Württemberg).

Die vier Schulen sind das Gymnasium in der Taus in Backnang, das Hans-Thoma-Gymnasium in Lörrach, das Helmholtz-Gymnasium in Karlsruhe und das Isolde-Kurz-Gymnasium (IKG) in Reutlingen (`http://www.ikg.rt.bw.schule.de`). Inzwischen stehen die vier Pilotschulen kurz vor dem ersten Abitur mit einem Computeralgebra-System, bei dem 'der Spickzettel erlaubt ist', siehe `http://www.ikg.rt.bw.schule.de/mokla.html` . Das Abitur wird nicht zentral, sondern mit eigenen Aufgabenstellungen durchgeführt, die auf Laptops mit dem Computeralgebra-System Maple bearbeitet werden. Dabei stehen den Schülern alle Worksheets zur Verfügung, die sie im Laufe der zweieinhalb Jahre geschrieben und ausgetauscht haben. Damit ist klar, daß die Standard-Kurvendiskussion keine adäquate Aufgabenstellung mehr darstellt, sondern durch neue, meist anwendungsorientierte Aufgaben mit offener Fragestellung abgelöst wurde. Und so stand auch im Unterricht das Problemlösen und Modellieren im Vordergrund, da ja das Computeralgebra-System in dieser neuen experimentellen Mathematik die Rechenarbeit übernimmt. Trotzdem wurden die Schüler so unterrichtet, daß sie prinzipiell in der Lage sind, konventionelle Aufgaben auch ohne Maple zu lösen, bzw. die vom Computeralgebra-System gelieferten Ergebnisse 'von Hand' zu kontrollieren. Der Einsatz eines Computeralgebra-Systems bedingt aber auch neue Arbeitsformen wie selbständiges Arbeiten, Gruppenarbeit und Projekte. Gerade am IKG haben wir diese Arbeitsformen stark betont, mit dem Ziel, aus Konsumenten Produzenten zu machen: Die Schüler bearbeiten Themen über mehrere Wochen und stellen ihre Produkte (Worksheets, die wie eine Klausur gewertet werden) im Internet zur Verfügung. So entstand am IKG zunächst das 'Virtuelle Klassenzimmer' `http://www.ikg.rt.bw.schule.de/virkla/` mit dem erwünschten Nebeneffekt, daß die voll multimediafähigen Laptops auch in anderen Fächern eingesetzt wurden.

Parallel dazu wurde am IKG der CAS-Server für Baden-Württemberg aufgebaut (im Auftrag des Ministeriums und als Infrastrukturprojekt von 'Schulen ans Netz'): `http://notes.ikg.rt.bw.schule.de` Dieser Server ermöglicht den Austausch von Materialien, die nach Kategorien geordnet in einer Datenbank gehalten werden und mit Volltext- und Schlüsselwortsuche recherchierbar sind, sowie die Diskussion über diese Materialien. Damit ist für eine Kommunikationsplattform gesorgt, wenn in einigen Jahren in Baden-Württemberg flächendeckend Mathematik mit CAS unterrichtet wird. Denn daß die Modernisierung der Schulmathematik ohne Computer nicht denkbar ist, steht spätestens nach diesem Pilotprojekt fest. Unsere Erfahrungen zeigen aber auch, daß sich der Computer sehr gut in den Unterricht integrieren läßt, oder sogar als Hauptmedium eingesetzt werden kann. Das ist auch die Meinung der Projektschüler am IKG, die sich bei einer erneuten Wahl alle wieder für das Projekt entscheiden würden.

Deshalb wird nun das Projekt zumindest an vier Gymnasien im Oberschulamtsbezirk Tübingen fortgesetzt. Vorrangiges Ziel dabei ist, Unterrichtsmaterialien wie z.B. 'Elektronische Bücher' (vgl. `http://www.ikg.rt.bw.schule.de/mbuch.htm`) weiter auszuarbeiten und damit die Grundlage für einen neuen Mathematiklehrplan zu schaffen. Darüber hinaus sollen aber auch neue Formen der Leistungsmessung beim Abitur - etwa Seminararbeit mit Kolloquium - erprobt werden, damit in Zukunft die Schüler durch diese vorwissenschaftlichen Arbeitsweise besser auf ein Studium vorbereitet sind.

M. Komma (Reutlingen)

Publikationen über Computeralgebra

- Articolo, G., *Partial differential equations and boundary value problems with Maple V*, Academic Press , ISBN 0-120-64475-4, 1998, pp. , £34.95.

- Betten, A., Fripertinger, H., Kerber, A., Wassermann, A., Zimmermann, K.-H., *Codierungstheorie, Konstruktion und Anwendung linearer Codes*, Springer Verlag, ISBN 3-540-64502-0, 1998, DM 69,00.

- Cheung, C.-K., Keough ,G. E., May, M. , *Getting Started with Maple*, John Wiley & Sons, ISBN 0-471-25249-2, 1998, £23.95.

- Cohen, A. M., Cuypers, H., Sterk, H., (Eds.), *Some Tapas of Computer Algebra*, Springer Verlag, ISBN 3-540-63480-0, 1999, DM 79,00.

  Das Buch wird in diesem Rundbrief auf Seite 17 besprochen.

- Coombes, K. R., Hunt, B. R., Lipsman, R. L., *Differential Equations with Maple*, John Wiley & Sons, ISBN 0-471-17696-6, DM 38,00.

- Corless, R. M., *Symbolic Recipes, Scientific Computing with Maple*, Springer Verlag, ISBN 3-540-94210-6, 1998, DM 62,00.

- Eikelberg, M., *Einführung in die Arbeit mit Maple V* , Fachbuchverlag Leipzig , ISBN 3-446-19458-4, 1998, ca DM 58,- .

- Grätzer, G., *General Lattice Theory, Second edition*, Birkhäuser Verlag, ISBN 3-7643-5239-6, 1999, pp. 663.

- Habib, M., McDiarmid, C., Ramirez-Alfonsin, J., Reed, B., (Eds.), *Probabilistic Methods for Algorithmic Discrete Mathematics*, Springer Verlag, ISBN 3-540-64622-1, 1998, DM 149,00.

- Kamerich, E., Yorke, J. A., *A Guide to Maple*, Springer Verlag, ISBN 3-540-94116-9, 1998, DM 69,00.

- di Martino, L., Kantor, W. M., Lunardon, G., Pasini, A., Tamburini, M. C., Editors, *Groups and Geometries*, Birkhäuser Verlag, ISBN 3-7643-5922-6, 1999, pp. 261.

- Matzat, B. H., Greuel, G.-M., Hiss, G., *Algorithmic Algebra and Number Theory*, Springer Verlag, ISBN 3-540-64670-1, 1999.

- Migliore, J. C. , *Introduction to Liaison Theory and Deficiency Modules*, Birkhäuser Verlag, ISBN 0-8176-4027-4, 1999, pp. 215.

- Reckziegel, H., Kriener, M., Pawel, K., *Elementare Differentialgeometrie mit Maple*, Vieweg Verlagsges., ISBN 3-528-06991-0, 1998, ca DM 69,-.

- Sagan,B. E., Stanley, R. P., Editors, *Mathematical Essays in Honor of Gian-Carlo Rota*, Birkhäuser Verlag, ISBN 0-8176-3872-5, 1999, pp. 463.

- Sorgatz, A., *Dynamic Modules, User's Manual and Programming Guide for MuPAD 1.4*, Springer Verlag, ISBN 3-540-65043-1, 1999, DM 89,00.

  Das Buch wird in diesem Rundbrief auf Seite 18 besprochen.

- Stroyan, K. D., *Calculus : The language of change, 2nd Ed.*, Academic Press , ISBN 0-126-73030-X, 1998, £34.95.

- Walz, A., *Maple V, Rechnen und Programmieren mit Rel. 4*, Verlag Oldenbourg, ISBN 3-486-24280-6, 1998, DM 68,00,

- Waterloo Maple Inc., *Maple V Learning Guide (Version A) : for Release 5* , Springer Verlag, ISBN 0-387-98397-X, 1998, DM 49.50.

- Wei-Chi Yang, Lewin, J., *Exploring mathematics with scientific notebook*, Springer Verlag, ISBN 981-3083-88-3, 1999 ,209 Seiten, CD

  Das Buch wird in diesem Rundbrief auf Seite 19 besprochen.

- Wolf, M., Gloor, O., Richard, C., *Analysis Alive – Ein interaktiver Mathematik-Kurs*, Birkhäuser Verlag, ISBN 3-7643-5966-8, 1999, pp. 372.

Besprechungen zu Büchern der Computeralgebra

Cohen, Arjeh M., Cuypers, Hans, Sterk, Hans (Eds.)
Some Tapas of Computer Algebra

Springer-Verlag, Berlin Heidelberg, 1999, ISBN 3-540-63480-0, HC DM 79,00.

In einem Restaurantführer von Mallorca wird von den sagenhaften vielfältigen Appetithäppchen *Tapas* gesprochen und diese dann weiter beispielhaft erläutert: kleine gebackene Calamares, Serrano-Schinken mit Melone oder in Fetteig gebackene Gemüsehäppchen.

Ist man so eingestimmt, dann sollte einem Computeralgebraiker das Wasser im Munde zusammenlaufen, wenn ihm oder ihr ein Buch mit dem Titel *Some Tapas of Computer Algebra* vorgelegt wird. Es handelt sich in der Tat um ein ungewöhnliches Buch über Computeralgebra!

Das Buch ist als vierter Band in der vom Springer-Verlag aufgelegten Reihe *Algorithms and Computations in Mathematics* erschienen. Die drei Herausgeber haben insgesamt neunzehn Autoren gewonnen bei dem Projekt mitzuwirken, das aus Kurzeinführungen in die Computeralgebra an der Technischen Universität in Eindhoven entstanden ist. Das Buch teilt sich in zwei Teile, mehr als drei Viertel des Buches sind elf Appetitanregern zu teilweise ganz verschiedenen Themen der Computeralgebra gewidmet, die meisten zentralen Themen der Computeralgebra sind angesprochen. Der zweite Teil enthält dann sieben Projektvorschläge, die auf den zuvor behandelten Themen aufsetzen.

So wird beispielsweise von H. Cuypers, Leonhard H. Soicher und Hans Stark auf 24 Seiten im Tapas *Working with Finite Groups* eine Kurzeinführung in *Computational Group Theory* gegeben. Es werden zum einen Permutationsgruppen mit Algorithmen zur Bestimmung von Bahnen und Stabilisatoren, insbesondere der Schreier-Sims-Algorithmus behandelt, zum andern Gruppen, die durch Erzeugende und Relationenen gegeben sind. Der Todd-Coxeter-'Algorithmus' zur Abzählung von Nebenklassen erlaubt – wenn er terminiert – eine Darstellung als Permutationsgrupppe von Nebenklassen einer Untergruppe. Ein eher beschreibender Stil, der Ideen und Zusammenhänge verbunden aber mit zahlreichen Hinweisen zu weiterführender Literatur aufzeigt, macht den Beitrag zu einem Appetitanreger, der dann im Projekt 6 *The Small Mathieu Groups* von denselben Autoren sowie im Projekt 5 *Explorations with the Icosahedral Group* von A.M. Cohen, H. Cuypers und R. Riebeck weiter gestillt werden kann.

G. Ivanyos und L. Ronyai erläutern in *Computations in Associative and Lie Algebras* einige Methoden zur Bestimmung von Radikalen, einfachen Komponenten sowie von Nullteilern in endlich-dimensionalen Algebren.

Dem zentralen Thema *Gröbnerbasen* sind mehrere Tapas und Projekte gewidmet. Zum einen gibt A. Cohen eine dreißigseitige Einführung in Gröbnerbasen, während – darauf aufbauend – L. Gonzalez-Vega, F. Roiullier und M.-F. Roy elf *Symbolic Recipes for Polynomial System Solving* für den Fall von nur endlich vielen Lösungen geben. Die Rezepte sind in drei Klassen eingeteilt, zum einen die grundlegenden Techniken zur Bestimmung von Lösungen aus der Theorie der Gröbnerbasen, dann Methoden aus der Linearen Algebra (Eigenwerte, Vielfachheiten, Satz von Stickelberger, Spur) und schließlich die Jakobi-Determinante für den Fall von gleich vielen Gleichungen und Unbestimmten, bevor dann Gröbnerbasen und numerische Approximation in Zusammenhang gebracht werden.

G. M. Ziegler stellt dann die von Conti und Traverso hergestellte Beziehung zwischen *Gröbner Bases and Integer Programming* aus dem Gebiet der Optimierung und Operations Research dar – ein sehr interessanter, wenn auch vermutlich von einem Praxiseinsatz noch weit entfernter Zusammenhang –, während M. de Boer und R. Pellikaan *Gröbner Bases for Codes* in der Codierungstheorie einsetzen.

Dieser Abschnitt ist eine Kurzeinführung in Grundbegriffe der Codierungstheorie, wobei Gröbnerbasen nur kurz bei der Bestimmung aller Codewörter von zyklischen Codes – es operiert die zyklische Gruppe auf den Codewörtern, oder äquivalent dazu, die Codewörter bilden ein Ideal des Polynomrestklassenring über einem endlichen Körper (modulo $x^n - 1$) – mit Minimalgewicht sowie in einem Zusammenhang mit Gewichtsfunktionen eine Rolle spielen. Dies wird dann aber im Projekt 7 für Golay-Codes ausgearbeitet. Im Abschnitt 11 *Gröbner Bases for Decoding* von denselben Autoren wird erläutert in welcher Weise Gröbnerbasen bei gewissen Klassen von Codes zum Dekodieren benutzt werden können.

Ein weiterer Abschnitt von L. Gonzalez-Vega, F. Rouillier, M.-F. Roy und G. Trujillo widmet sich den verschiedenen symbolischen Techniken, wenn man speziell an reellen Lösungen interessiert ist: Verallgemeinerung wie Sylvester-Habicht der Sturmschen Ketten zur Abzählung der reellen Nullstellen eines Polynoms, aber auch für Systeme von Polynomgleichungen; Quantorenelimination.

Der LLL-Gitter-Reduktionsalgorithmus von Lentra, Lenstra und Lovacs wird von F. Beukers in einem zehnseitigen Abschnitt präsentiert. Neben der traditionellen Faktorisierungsalgorithmen für Polynome von Berlekamp sowie die Idee von Cantor-Zassenhaus und der Faktorisierung mit Hilfe von Hensels Lemma kann dann auch deren Faktorisierungsalgorithmus mit polynomialer Laufzeit im nächsten Abschnitt vom selben Autor dargestellt werden.

M. van der Put stellt im Abschnitt *Symbolic Analysis of Differential Equations* einige Methoden zur Integration von Funktionen sowie für Gleichungen der Ordnung 2 (Kovacic) vor, nachdem zuvor einige Grundideen der Differential-Galoistheorie (Picard-Vessiot) erläutert werden: Analog zum klassischen Fall von Wurzeln eines Polynoms werden auch hier die Lösungen in Zusammenhang zu Gruppen gebracht, aus deren Struktur dann im Prinzip die Lösungen entwickelt werden können. Auffallend ist für mich hier, daß bei den Literaturverweisen zur Integrationstheorie nur auf ein Vorlesungsmanuskript, nicht aber auf die in der selben Reihe erschienenen Monographie dazu von M. Bronstein verwiesen wird.

Die weiteren Projekte behandeln u.a. die Themen Robotersteuerung, Interpolation, Quaternionen sowie automatisches Beweisen von geometrischen Sätzen durch Modellierung einer Fragestellung, ob ein Polynom – der Implikation des Satzes entsprechend – im Ideal – erzeugt von den Polynomen, die den Voraussetzungen des Satzes entsprechen – enthalten ist.

Wie im Restaurant werden die vielfältigen und unterschiedlichen Appetithappen auf unterschiedliche Geschmäcker treffen. Der Verdienst dieser Zusammenstellung ist es aber schon, hier ein reichliches Angebot mit Kurzeinführungen zu wichtigen Themen der Computeralgebra gegeben zu haben. Diese können für allgemeine Vorlesungen zur Computeralgebra, für Seminare und Arbeitsgruppen als Startpunkte verwendet werden. Ich sehe auch den einen oder andern motivierten Gymnasiallehrer, der sich über die mathematischen Hintergründe der Computeralgebra-Systeme, die er oder sie oder die Schüler im Unterricht benutzen, weiterbilden will, mit Gewinn dieses Buch nutzen.

Johannes Grabmeier (Heidelberg)

Sorgatz, A., Dynamic Modules. User's Manual and Programming Guide for MuPAD

Springer-Verlag, Berlin Heidelberg 1999, ISBN 3-540-656043-1.

Verglichen mit den Anfängen der Computeralgebra werden heute die Systeme im häufiger in Verbindung mit anderen Programmen oder Programmbibliotheken eingesetzt. Hier spiegelt sich der Trend wieder, daß Computeralgebrasysteme immer mehr als nur ein Teil in einer komplexen *problem solving environment* angesehen werden, zu der z.B. auch Numerikbibliotheken oder Visualisierungstools gehören. Angesichts dessen ist es nicht verwunderlich, daß die meisten Systeme sich öffnen und Möglichkeiten zur Kommunikation mit anderen Programmen anbieten; als Beispiele seien nur MathLink und MathEdge für Mathematica bzw. Maple erwähnt.

Der klassische Weg zur Realisierung einer solchen Schnittstelle geht über *interprocess communication* (IPC). Dieser Ansatz führt aber zu einem beträchtlichen Kommunikationsoverhead, da Daten zwischen den verschiedenen Programmen explizit ausgetauscht werden müssen. Dies macht IPC vor allem dann langsam, wenn entweder sehr große Mengen an Daten transferiert werden (ganz abgesehen davon, daß diese Daten dann doppelt im Speicher gehalten werden müssen) oder allgemeiner die Verarbeitungszeit verhältnismäßig klein gegenüber der Kommunikationszeit ist.

Andreas Sorgatz von der Paderborner MuPAD-Gruppe hat in MuPAD einen anderen Ansatz zur Integration von Softwarepaketen realisiert: dynamische Module. Dynamisch bedeutet hierbei, daß diese Module zur Laufzeit zu MuPAD gelinkt werden können. Sie werden damit zu einem Teil des MuPAD-Prozesses und teilen sich vor allem den Speicher mit MuPAD. Damit muß kein Datentransfer mehr erfolgen. Um die Möglichkeiten dieses Ansatzes auszuschöpfen, benötigt der Entwickler dynamischer Module allerdings einige Kenntnisse von Interna von MuPAD.

Rein technische Fragen der Realisierung dynamischer Module wurden bereits in einem früheren Buch des Autors behandelt (A. Sorgatz, Dynamische Module, MuPAD-Reports, Teubner 1996, besprochen im Zentralblatt Zbl. 970.06779). Was bisher noch fehlte, war eine Beschreibung der dynamischen Module aus der Sicht des Anwenders, der entweder mit vorgegebenen Modulen arbeiten oder aber eigene Module entwickeln will. Diese Lücke wird durch das vorliegende Buch geschlossen. Es basiert auf der aktuellen MuPAD-Version 1.4.1, die auch auf der beiliegenden CD enthalten ist.

Wie der Untertitel des Buches bereits klar ausdrückt, handelt es sich hier in erster Linie um ein Handbuch, d.h. die wenigsten Leser werden es von vorne bis hinten durchlesen sondern es als Nachschlagewerk benutzen. Nach einigen einführenden Kapiteln, in denen die zugrundeliegenden Konzepte vorgestellt werden, wird das Buch denn auch sehr technisch. Dies gilt insbesondere für das zentrale Kapitel 6, das das MuPAD Application Programming Interface (MAPI) beschreibt. Das MAPI stellt eine umfangreiche Sammlung von vordefinierten Typen und Prozeduren dar, die es dem Entwickler von dynamischen Modulen gestatten, MuPAD-Objekte zu erzeugen bzw. zu manipulieren. Weitere Kapitel beschreiben u.a. die interne Struktur von MuPAD, den Modulgenerator zum Kompilieren und Linken von dynamischen Modulen oder geben Details zu speziellen Betriebssystemen, Programmiersprachen, shared/static libraries etc.

Erfreulicherweise enthält das Buch sehr viele Beispiele (oft mit komplettem Programmcode), die dem Anfänger den Einstieg in die Welt der dynamischen Module sehr erleichtern. Diese reichen von der einfachen Interaktion mit dem Betriebssystem über die Einbindung numerischer Bibliotheken bis hin zur Fensterprogrammierung unter Motif. Auf der CD finden sich auch noch einige größere Beispiele wie die Anbindung von Singular oder GB/RealSolving an MuPAD. Auch für eine Reihe von Kommunikationsprotokollen wie MP oder PVM existieren bereits dynamische Module.

Wer in MuPAD mit dynamischen Modulen arbeiten will, wird um dieses Buch nicht herumkommen. Die bereits realisierten Anwendungen zeigen das große Potential dieses Ansatzes zur Verknüpfung verschiedenster Programmsysteme. MuPAD bietet hier weit flexiblere Möglichkeiten als andere Computeralgebrasysteme; es liegt nun an den Benutzern, diese auch auszunutzen!

Werner M. Seiler (Mannheim)

Wei-Chi Yang, Lewin, J.,
Exploring mathematics with scientific notebook

Springer-Verlag, Berlin Heidelberg 1999, ISBN 981-3083-88-3, 209 Seiten, CD

Scientific Notebook ist eine „light“-Version von Scientific Workplace (Brooks-Cole), einer Software, die grob gesprochen die Macht von TEX und Maple unter einer komfortablen Benutzeroberfläche verbirgt; SWP ist sowohl in einer professionellen Version als auch als preiswerte Student Edition erhältlich. Zur Erstellung mathematischer Texte, ob Bücher, Fachartikel oder Übungsblätter, ist diese Software großartig; ähnlich wie die Formeleditoren, die aus diversen Office-Paketen bekannt sind, erzeugt man Formeln, die man von Maple auswerten lassen kann. Das Ergebnis der Maple-Rechnung wird unmittelbar wieder im TEX-Format eingefügt; dies reduziert Fehler, die ansonsten leicht bei der Übertragung in TEX vorkommen können. Insbesondere ziehen TEX-Anfänger aus Scientific Workplace/Scientific Notebook großen Nutzen. Die Software ermöglicht professionellen Formelsatz ohne die sonst notwendige langwierige Lernphase. *Exploring mathematics with scientific notebook* umfaßt neben einem konventionellen gedruckten Buch auch eine on-screen-Version des Buches auf CD und macht es so dem Leser leicht, die behandelten Beispiele nachzuvollziehen. Trotzdem hinterläßt das Buch einen zwiespältigen Eindruck: Will man wirklich die Mathematik „erkunden“, so ist man z.B. mit der Student Edition von Maple sehr viel besser bedient; SWP bietet nur einen Bruchteil der Möglichkeiten, die Maple beinhaltet. Trotzdem ist alles vorhanden, was an Analysis und linearer Algebra für Anfängervorlesungen oder den gymnasialen Unterricht erforderlich ist.

Ist man eher daran interessiert, einen mathematischen Text zu verfassen, so ist SWP sehr viel komfortabler als es derzeit jede Kombination von Maple und einer der vielen TEX-Implementationen ist, auch wenn sich Waterloo Maple Software viel Mühe gibt, die Oberfläche von Maple zu verbessern. Befremdlich wirkt es, daß etliche Beispiele für den Abdruck ungeeignet sind und das Buchformat sprengen; die Standardfußnote ist daher „The following expression will be fully visible only in the on-screen version of this text.“ Man kann das vorliegende Buch vor allen jenen als Entscheidungshilfe empfehlen, die eine intelligente mathematische Textverarbeitung suchen und mit der recht sparsamen Dokumentation von Scientific Notebook unzufrieden sind; das Vollprodukt Scientific Workplace enthält ein Handbuch mit ähnlicher Zielsetzung wie das vorliegende Buch. Da die beigefügte CD auch eine zeitlich limitierte Version von Scientific Notebook enthält, kann das Buch auch denjenigen empfohlen werden, die den Kauf der Software in Erwägung ziehen, zunächst aber ihre Möglichkeiten studieren wollen.

Wilhelm Werner, Heilbronn-Künzelsau

Lehrveranstaltungen über Computeralgebra im SS 1999

- **Rheinisch–Westfälische Technische Hochschule Aachen**
  Fachdidaktisches Seminar: Computer im Algebraunterricht, U. Schoenwaelder, U. Bettscheider, Ü4
  Algebraisches Praktikum, G. Hiß, F. Lübeck, Ü2
  Einführungspraktikum in das Formelmanipulationssystem MAPLE, G. Hiß, U. Klein, V. Dietrich, P2
  Praktikum: Programmieren in MAPLE, G. Hiß, U. Klein, P4
  Arbeitsgemeinschaft zu speziellen Problemen mit MAPLE, V. Dietrich, U. Klein, Ü2

- **Freie Universität Berlin**
  Algorithmische Singularitätentheorie, K. Gatermann, V2 + Ü2

- **Technische Universität Berlin**
  Konstruktive Zahlentheorie I, M. Pohst, V4 + Ü2
  Seminar Algorithmische Algebra und Zahlentheorie, M. Pohst, S2

- **Universität Bonn**
  Computeralgebra I, M.Clausen, V4

- **Technische Hochschule Darmstadt**
  Digitale Signaturen, I. Biehl, V2+Ü1
  Einführung in die Kryptographie, J. Buchmann, V2+Ü2
  Einführung in die algorithmische Zahlentheorie, J. Buchmann, V2+Ü2
  Elliptische Kurven und Kryptographie, S. Paulus, V2
  Praktikum Weiterentwicklung von LiDIA, J. Buchmann, T. Pfahler, P4
  Seminar Public-Key-Infrastrukturen, J. Buchmann, M.Ruppert, S2

- **Universität Erlangen-Nürnberg**
  Zahlentheoretische und algebraische Grundlagen der Kryptographie, H. Meyn, V4
  Probabilistic Methods in Algorithmics, V. Strehl, V2
  Mathematica as a Tool for Science, N. Jacob, V2
  Seminar Kryptographie, M. Bauer, S2

- **Technische Hochschule Hamburg-Harburg**
  Diskrete Mathematik I, K.-H. Zimmermann, V4+U2
  Programmieren in Maple, K.-H. Zimmermann, U1
  Kryptologie, K.-H.Zimmermann, V2
  Seminar Sicherheitsinfrastrukturen, K.-H.Zimmermann, P.Batra, S2

- **Martin-Luther-Universität Halle(Saale)**
  Mathematik mit MATHCAD, H. Benker, P2
  Numerische Mathematik mit MATLAB, H. Benker, J.Bruder, P2

- **Universität Kaiserslautern**
  Algebraic Geometry II with Computational Aspects, G. Pfister, V4 + Ü1
  Seminar Singularitäten und Computeralgebra, G. Pfister, S2

- **Pädagogische Hochschule Karlsruhe**
  Informatik II, J. Ziegenbalg, V2
  Hauptseminar Algorithmen / Computer / Informatik, J. Ziegenbalg, HS2

- **Universität Karlsruhe**
  Computeralgebra, J. Calmet, V4
  Computeralgebra und Theorembeweisen, J. Calmet, C. Ballarin, S2
  Computeralgebra-Praktikum, J. Calmet, W.M. Seiler, C. Ballarin, P4

- **Universität Leipzig**
  Such- und Graphalgorithmen, J. Apel, V2
  Grundlegende Algorithmen der Computeralgebra, H.-G. Gräbe, V2
  Algebraische Komplexitätstheorie , H.-G. Gräbe, V2
  Mechanisiertes Theorembeweisen in der Geometrie , H.-G. Gräbe, V2

- **Universität Linz, Research Institute for Symbolic Computation**
  Computer Algebra für Fortgeschrittene, F. Winkler, V2
  Rewriting in Computer Science and Logic, F. Winkler, V2
  Geometrische Grundlagen für Symbolic Computation, S. Stifter, V2 + Ü1
  Mathematikunterricht mit DERIVE, B. Kutzler, V2
  Elimination Theory, D. Wang, V2
  Programming in Mathematica, W. Windsteiger, P2
  Projektseminar Computer Algebra, F. Winkler, S2

- **Universität Oldenburg**
  Algebra und Anwendungen (CA), W. Schmale, S2

- **Universität-Gesamthochschule Paderborn**
  Computeralgebra I, F. Schwarz, V4
  Kryptographie, J. von zur Gathen, V4
  Praktikum Mathematik am Computer, F. Schwarz, P4
  Seminar Computergenriertes Beweisen, J. von zur Gathen, S2
  MuPAD Seminar, B. Fuchssteiner, S2
  Oberseminar Algorithmische Mathematik, J. von zur Gathen, S2

- **Universität Passau**
  Einführung in das Computeralgebra System REDUCE, V. Weispfenning, A. Dolzmann, T. Sturm, V2 + P4

- **Universität Rostock**
  Symbolisches Rechnen, K.Hantzschmann, V2

- **Universität Ulm**
  Symmetrie Analyse von Differentialgleichungen mit Mathematica, G. Baumann, V2
  Computeralgebra Praktikum mit Mathematica, G. Baumann, V4+Ü2

- **ETH Zürich**
  Computer Algebra II, G. Gonnet, V2 + U1

Aufnahmeantrag für Mitgliedschaft in der Fachgruppe Computeralgebra

(Im folgenden jeweils Zutreffendes bitte im entsprechenden Feld [ ] ankreuzen bzw. ____________ ausfüllen.)

Name: ______________________ Vorname: ______________

Akademischer Grad/Titel: ______________________

Privatadresse

Straße/Postfach: ______________________

PLZ/Ort: ______________________ Telefon: ______________

e-mail: ______________________ Telefax: ______________

Dienstanschrift

Firma/Institution: ______________________

Straße/Postfach: ______________________

PLZ/Ort: ______________________ Telefon: ______________

e-mail: ______________________ Telefax: ______________

Gewünschte Postanschrift: [ ] Privatadresse [ ] Dienstanschrift

1. Hiermit beantrage ich zum 1. Januar 199___ die Aufnahme als Mitglied in die Fachgruppe

   Computeralgebra (CA) (bei der GI: 2.2.1).

2. Der Jahresbeitrag beträgt DM 15,00 bzw. DM 18,00. Ich ordne mich folgender Beitragsklasse zu:

   [ ] **15,00 DM**. für Mitglieder einer der drei Trägergesellschaften
   - [ ] GI Mitgliedsnummer: ____________
   - [ ] DMV Mitgliedsnummer: ____________
   - [ ] GAMM Mitgliedsnummer: ____________

   Der Beitrag zur Fachgruppe Computeralgebra wird mit der Beitragsrechnung der Trägergesellschaft in Rechnung gestellt. (Bei Mitgliedschaft bei mehreren Trägergesellschaften wird dies von derjenigen durchgeführt, zu der Sie diesen Antrag schicken.) [ ] Ich habe dafür bereits eine Einzugsvollmacht erteilt. Diese wird hiermit für den Beitrag für die Fachgruppe Computeralgebra erweitert.

   [ ] **15,00 DM**. Ich bin aber noch nicht Mitglied einer der drei Trägergesellschaften. Deshalb beantrage ich gleichzeitig die Mitgliedschaft in der

   [ ] GI [ ] DMV [ ] GAMM.

   und bitte um Übersendung der entsprechenden Unterlagen.

   [ ] **18,00 DM** für Nichtmitglieder der drei Trägergesellschaften. [ ] Gleichzeitig bitte ich um Zusendung von Informationen über die Mitgliedschaft in folgenden Gesellschaften:

   [ ] GI [ ] DMV [ ] GAMM.

3. Die in dieses Formular eingetragenen Angaben werden elektronisch gespeichert. Ich bin damit einverstanden, daß meine Postanschrift durch die Trägergesellschaften oder durch Dritte nach Weitergabe durch eine Trägergesellschaft wie folgt genutzt werden kann (ist nichts angekreuzt wird c. angenommen).

   [ ] a. Zusendungen aller Art mit Bezug zur Informatik, Mathematik bzw. Mechanik.
   [ ] b. Zusendungen durch wissenschaftliche Institutionen mit Bezug zur Informatik, Mathematik bzw. Mechanik.
   [ ] c. Nur Zusendungen interner Art von GI, DMV bzw. GAMM.

Ort, Datum: ______________ Unterschrift: ______________________

Zurück an:

Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum
Ahrstraße 45
53175 Bonn
Tel.: 0228-302-149, Fax.: -167
e-mail: gs@gi-ev.de

oder

Deutsche Mathematiker-Vereinigung e.V. (DMV)
Mohrenstraße 39, 10117 Berlin
Tel.: 030-20377-306, Fax.: -307
e-mail: dmv@wias-berlin.de

oder

Gesellschaft für Angewandte Mathematik und Mechanik e.V. (GAMM)
NWF I – Mathematik, Univ. Regensburg
Universitätsstr. 31, 96053 Regensburg

Fachgruppenleitung Computeralgebra 1999-2002

Dr. Johannes Grabmeier
Heidelberg Scientific and Technical Center
IBM Deutschland Informationssysteme GmbH
Vangerowstr. 18, Postfach 10 30 68
69020 Heidelberg
Tel. 06221-59-4329,-4254(Sekr.)
Telefax: 06221-59-3500
`grabm@de.ibm.com`

Prof. Dr. G.-M. Greuel
Fachbereich Mathematik
der Universität Kaiserslautern
Postfach 3049
D-67653 Kaiserslautern
Tel. 0631-205-2850,-2339(Sekr.)
Telefax: 0631-205-3052
`greuel@mathematik.uni-kl.de`
`http://www.mathematik.uni-kl.de/~wwwagag/D/Greuel`

Vertreter der GI:
Prof. Dr. Karl Hantzschmann
Fachbereich Informatik
Universität Rostock
Albert-Einstein-Straße 21
18059 Rostock
Postanschrift: 18051 Rostock
Tel.: 0381-498-3400
Telefax: 0381/498-3399
`hantzschmann@informatik.uni-rostock.de`

Fachexperte Physik:
Prof. Dr. Friedrich W. Hehl
Institut für Theoretische Physik,
Universität Köln, Zülpicher Straße 77
D-50937 Köln
Tel.: 0221-470-4307,-4310 (Sekr.)
Telefax: 0221/470-5159
`hehl@thp.uni-koeln.de`

Referent Chemieanwendungen:
Prof. Dr. A. Kerber
Lehrstuhl II f. Mathematik
Univ. Bayreuth, 95440 Bayreuth
Tel. 0921-553387
Telefax: 0921-553385
`kerber@uni-bayreuth.de`
`http://www.mathe2.uni-bayreuth.de`

Fachexperte Schule:
Heiko Knechtel
An der Tränke 2a
31675 Bückeburg
Tel. 05722-23628
`HKnechtel@aol.com`

Referent Lehre & Didaktik:
Prof. Dr. Wolfram Koepf
Fachbereich IMN, HTWK Leipzig
Gustav-Freytag-Str. 42 A
D-04277 Leipzig
Tel.: 0341-307-6495
Telefax: 0341-301-2722
`koepf@imn.htwk-leipzig.de`
`http://www.imn.htwk-leipzig.de/~koepf`

Vertreter der DMV:
Prof. Dr. B. Heinrich Matzat
Interdisziplinäres Zentrum f.
Wissenschaftliches Rechnen
Univ. Heidelberg, Im Neuenheimer Feld 368
69120 Heidelberg
Tel. 06221-54-8242, -8318 (Sekr.)
Telefax 06221-54-8850
`matzat@iwr.uni-heidelberg.de`

Sprecher:
Prof. Dr. H. Michael Möller
Fachbereich Mathematik
Universität Dortmund
44221 Dortmund
Tel. 0231-755-3077
`Moeller@math.uni-dortmund.de`

Stellv. Sprecher:
Prof. Dr. M. Pohst
Fachbereich 3 Mathematik MA 8-1
Technische Universität Berlin
Straße des 17. Juni 136
10623 Berlin
Tel.: 030-314-25772, -24015 (Sekr.)
Telefax: 030-314-21604
`pohst@math.tu-berlin.de`

Vertreter der GAMM:
Prof. Dr. Siegfried M. Rump
Informatik III
TU Hamburg-Harburg
Eissendorfer Str. 38
21071 Hamburg
Tel. 040-42878-3027
`rump@tu-harburg.de`
`http://www.ti3.tu-harburg.de/rump/`

Referent CAIS:
Prof. Dr. Gerhard Schneider
GWDG, Am Faßberg
37077 Göttingen
Tel. 0551-201-1545
Telefax: 0551-21119
`Gerhard.Schneider@gwdg.de`

Referent Computational Engineering:
Prof. Dr. Volker Strehl
c/o Lehrstuhl Informatik 8 (Künstl. Intelligenz)
Universität Erlangen-Nürnberg
Am Weichselgarten 9
D-91058 Erlangen
Tel.: 09131-29914, -29907 (Sekr.)
Telefax: 09131-29905
`strehl@informatik.uni-erlangen.de`

Prof. Dr. V. Weispfenning
Lehrstuhl für Mathematik
Universität Passau
Innstraße 33
94030 Passau
Tel. 0851-509-3120, -3121 (Sekr.)
Telefax: 0851-509-3122
`weispfen@uni-passau.de`
`http://www.fmi.uni-passau.de/~weispfen`

Fachexperte Fachhochschulen:
Prof. Dr. W. Werner
FB TWK der FH Heilbronn
Außenstelle Künzelsau
Tel. 07940-1306-21 (Sekr.)
Telefax: 07940-1306-20
`werner@fh-heilbronn.de`

Verwaltungen der Fachgruppe Computeralgebra

Mitgliederverwaltung der GI, Anzeigenverwaltung:
Gesellschaft für Informatik e.V.
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Telefon 0228-302-145 (-164 Anzeigen)
Telefax 0228-302-167
el.Adr.: `gs@gi-ev.de`

Mitgliederverwaltung der DMV:
Deutsche Mathematiker-Vereinigung, Geschäftsstelle
Mohrenstraße 39
10117 Berlin
Telefon 030-20377-306
Telefax 030-20377-307, el.Adr.:
`dmv@wias-berlin.de`

Mitgliederverwaltung der GAMM:
Gesellschaft für Angewandte
Mathematik und Mechanik e.V.
NWF I – Mathematik,
Univ. Regensburg
Universitätsstr. 31
96053 Regensburg
`http://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/Mennicken/gamm/vorstand.html`

Impressum

Computeralgebra–Rundbrief Herausgegeben von der Fachgruppe Computeralgebra der GI (2.2.1), DMV und GAMM, Redaktionsschluß 28.02 und 30.09. Anschrift: Dr. Ulrich Schwardmann, Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), Am Fassberg, 37077 Göttingen, Telefax: 0551-21119, Internet: `uschwar1@gwdg.de` , ISSN 0933-5994. Mitglieder der Fachgruppe Computeralgebra erhalten je ein Exemplar dieses Rundbriefs im Rahmen ihrer Mitgliedschaft. Exemplare darüber hinaus bzw. außerhalb der Mitgliedschaft können über die GI bezogen werden.
WWW-Server der Fachgruppe Computeralgebra mit URL: `http://www.gwdg.de/~cais`,
Konferenzankündigungen, Mitteilungen und einzurichtende Links bitte an: `cais@rz.uni-karlsruhe.de`
Computeralgebra-Liste der Fachgruppe: `cais@rz.uni-karlsruhe.de` (Anm.:`SUBSCRIBE CAIS-L <vorname> <nachname>`)