Computeralgebra-Rundbrief

Nr. 32 März 2003

Fachgruppe Computeralgebra

Inhalt

Impressum

Der Computeralgebra-Rundbrief wird herausgegeben von der Fachgruppe Computeralgebra der GI, DMV und GAMM (verantwortlicher Redakteur: Dr. Markus Wessler, Universität Kassel, Fachbereich Mathematik/Informatik, Heinrich-Plett-Str. 40, 34132 Kassel, Telefon: 0561-8044192, Telefax: 0561-8044646, wessler@mathematik.uni-kassel.de).

Der Computeralgebra-Rundbrief erscheint halbjährlich, Redaktionsschluss 28.02 und 30.09. ISSN 0933-5994. Mitglieder der Fachgruppe Computeralgebra erhalten je ein Exemplar dieses Rundbriefs im Rahmen ihrer Mitgliedschaft. Fachgruppe Computeralgebra im Internet:
http://www.fachgruppe-computeralgebra.de.

Konferenzankündigungen, Mitteilungen, einzurichtende Links, Manuskripte und Anzeigenwünsche bitte an den verantwortlichen Redakteur.

Die Geschäftsstellen der drei Trägergesellschaften:

GI (Gesellschaft für Informatik e.V.)
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Telefon 0228-302-145
Telefax 0228-302-167
gs@gi-ev.de
http://www.gi-ev.de

DMV (Deutsche Mathematiker-Vereinigung e.V.)
Mohrenstraße 39
10117 Berlin
Telefon 030-20377-306
Telefax 030-20377-307
dmv@wias-berlin.de
http://www.mathematik.uni-bielefeld.de/DMV/

GAMM (Gesellschaft für Angewandte Mathematik und Mechanik e.V.)
Technische Universität Dresden
Institut für Festkörpermechanik
01062 Dresden
Telefon 0351-463-33448
Telefax 0351-463-37061
GAMM@mailbox.tu-dresden.de
http://www.gamm-ev.de

Mitteilungen der Sprecher

Liebe Mitglieder der Fachgruppe Computeralgebra,
die letzte Sitzung der Fachgruppenleitung fand am 21. Februar 2003 am Konrad-Zuse-Zentrum in Berlin statt. Zunächst möchten wir Sie auf folgende personelle Änderungen in der Fachgruppenleitung hinweisen:

1. *Herr Dr. Joachim Apel ist von seinem Amt zurückgetreten, da er seit kurzem eine neue Anstellung gefunden hat und nicht mehr im Bereich der Computeralgebra tätig ist.*

   Nach unserer Satzung rückt Prof. Dr. Hans-Wolfgang Henn als gewähltes Mitglied an die Stelle von Herrn Apel nach. Die Fachgruppenleitung beschließt, den Bereich Benchmarks, der von Herrn Apel vertreten wurde, zunächst ruhen zu lassen.

2. *Der Fachexperte Physik Dr. Georg Weiglein ist von seinem Amt zurückgetreten, da er seit geraumer Zeit in England beschäftigt ist und die Anreise zu den Sitzungen der Fachgruppenleitung auf Dauer zu weit ist. Herr Dr. Weiglein schlägt Herrn Dr. Thomas Hahn vom MPI für Physik in München als seinen Nachfolger vor. Herr Hahn ist Autor einschlägiger Computeralgebra-Software für das Fachgebiet Physik.*

   Die Fachgruppenleitung berief Herrn Hahn auf der letzten Sitzung zum neuen Fachexperten Physik. Wir freuen uns auf eine gute Zusammenarbeit!

Die Fachgruppe Computeralgebra bedankt sich herzlich bei Dr. Apel und Dr. Weiglein für ihre Mitarbeit und wünscht ihnen alles Gute auf ihrem weiteren beruflichen Weg.

Schnappschuss auf der Sitzung der Fachgruppenleitung in Berlin

Nach einer ausgesprochen unerfreulichen Debatte mit der Inhaberin der Domain `www.computeralgebra.de`*, der Firma Schumanns Verlagshaus, ging dann im Dezember letzten Jahres die Domain unserer neuen Homepage* **`http://www.fachgruppe-computeralgebra.de`** *ans Netz. Die Gestaltung erfolgte in Anlehnung an den Rundbrief. Statt der Erstattung der Auslagen für die Domain-Reservierung und -Einrichtung verlangte die Firma Schumanns Verlagshaus eine Erstattung der von ihr erwarteten Gewinne in einer von uns nicht nachvollziehbaren Höhe von 8000 € jährlich. Unter diesen Umständen mussten wir auf die Übernahme dieser Domain verzichten.*[1]

[1] Unsere Mitglieder sollten ihre eigenen Schlussfolgerungen aus dem Nicht-Kooperationsverhalten dieser Firma ziehen.

Inzwischen sind die meisten Rubriken unserer neuen Homepage ins neue Layout umgesetzt worden. Hierbei haben wir Wert darauf gelegt, dass die Seiten auch inhaltlich auf den neuesten Stand gebracht wurden. Verbesserungsvorschläge unserer Mitglieder sind immer herzlich willkommen und können an den Referenten Internet Herrn Schwardmann oder an den Sprecher gesandt werden.

Nach einem Beschluss der Fachgruppenleitung werden die Seiten des CAIS in Karlsruhe und Göttingen für einen vorübergehenden Zeitraum von ca. einem halben Jahr zu unserer Homepage umgeleitet und dann geschlossen.

Das elektronische Anmeldeformular `www.fachgruppe-computeralgebra.de/Aufnahmeantrag.html` *ist inzwischen schon mehrfach genutzt worden und hat den schriftlichen Aufnahmeantrag weitestgehend abgelöst.*

Nachdem die GI nun inzwischen die auftretenden Probleme bei der Umstellung der Mitgliederverwaltung auf eine neue Software überstanden zu haben scheint, konnten wir unsere Mitgliederliste einsehen. Bei der Durchsicht der Mitgliederunterlagen sind uns allerdings nicht nur einige veraltete Adressen aufgefallen, welche wir ausgebessert haben, sondern vor allem, dass nur bei wenigen Mitgliedern eine e-mail-Adresse eingetragen ist. Bei einer Probe-Post bzgl. unserer Tagung im Mai wurde dann noch festgestellt, dass auch viele e-mail-Adressen nicht mehr gültig sind.

Sollten Sie die e-mail bzgl. unserer Tagung im Mai nicht erhalten haben, möchten wir Sie bitten, dem Sprecher eine e-mail mit Ihrer gültigen e-mail-Adresse zuzuschicken. Sollten Sie den Rundbrief an eine falsche – vielleicht alte – Adresse geliefert bekommen, bitten wir Sie ferner auf demselben Weg um Mitteilung Ihrer korrigierten Adressdaten. Damit sollte unsere Adressdatenbank wieder auf den neuesten Stand kommen.

Wir möchten Sie nochmals auf die wissenschaftliche Tagung hinweisen, welche die Fachgruppe vom 15.–17.05.2003 in Kassel veranstaltet. Die Abstracts der Hauptvorträge finden Sie im nächsten Abschnitt. Anmeldungen ohne Vortrag sind noch bis 15. April möglich.

Wir bedanken uns bei unseren Mitgliedern, die sich sehr positiv zum neuen Outfit des Rundbriefs geäußert haben. Heute liegt Ihnen ja nun der zweite Rundbrief der neuen Generation vor.

Wir hoffen, Sie mit dem vorliegenden Heft wieder gut zu informieren. Anregungen aus unserem Leserkreis sind jederzeit willkommen.

Wolfram Koepf *H. Michael Möller*

Tagungen der Fachgruppe

Computeralgebra: 15.-17.05.2003, Kassel

In der Zeit vom 15.–17.05.2003 führt die Fachgruppenleitung in Kassel eine Tagung zum Thema Computeralgebra durch. Ziel dieser Tagung ist es hauptsächlich, Nachwuchswissenschaftlern die Vorstellung ihrer Ergebnisse ermöglichen. Auf der anderen Seite wird in verschiedenen Übersichtsvorträgen auch zum aktuellen Stand in einigen wichtigen Gebieten der Computeralgebra berichtet sowie über in Deutschland mitentwickelte Computeralgebra-Software informiert.

Als Hauptvortragende haben wir gewonnen:

- Prof. Dr. Wolfram Decker (Saarbrücken): *Computeralgebramethoden in der algebraischen Geometrie*

  Algebraische Geometer studieren Kurven, Flächen oder andere geometrische Objekte, die als Lösungsmengen polynomialer Gleichungen auftreten. Ein wichtiges Hilfsmittel ist ein geometrisch-algebraisches Wörterbuch, das geometrische Eigenschaften in algebraische Eigenschaften übersetzt und umgekehrt. Dieses Wörterbuch erlaubt es insbesondere, moderne Computeralgebramethoden zur intensiven Beispielrechnung heranzuziehen. Durch solche Experimente kann man mathematische Zusammenhänge erkennen oder etwa Gegenbeispiele zu Vermutungen finden. In meinem Vortrag spreche ich unter anderem folgende Fragen an: Was kann heute in der algebraischen Geometrie berechnet werden? Welche Computeralgebrasysteme sind für diese Rechnungen geeignet? Was sind typische Anwendungen?

- Prof. Dr. Bettina Eick (Braunschweig): *Algorithmische Gruppentheorie mit dem Computeralgebrasystem GAP*

  Gruppen spielen eine wichtige Rolle in der Algebra: sie werden verwendet, um die Symmetrien von Objekten zu studieren, und sie haben Anwendungen, die von der Unlösbarkeit von Gleichungen 5. Grades bis hin zur Kristallographie reichen.

  Die algorithmische Gruppentheorie ist ein wichtiges Hilfsmittel zur Untersuchung und Klassifizierung von Gruppen. So kann man zum Beispiel mit Hilfe von

Algorithmen den Rubik's Cube sehr leicht im Detail studieren; ein Projekt, welches ohne den Einsatz von Computern nicht so einfach ist. Weitere Anwendungen der algorithmischen Gruppentheorie sind in der Untersuchung von kristallographischen Gruppen oder von topologischen Gruppen zu finden.

In der Entwicklung von Algorithmen zur Behandlung von Gruppen spielt die Darstellung der gegebenen Gruppen eine fundamentale Rolle. Daher kann man die algorithmische Gruppentheorie in eine Reihe von Teilgebieten einteilen; sehr bekannt sind hier zum Beispiel Algorithmen für Permutationsgruppen, Algorithmen für Matrixgruppen oder Algorithmen für endlich präsentierte Gruppen. Weniger bekannt, aber trotzdem sehr interessant sind zum Beispiel Methoden zum Rechnen mit freien Gruppen oder mit polyzyklischen Gruppen.

In diesem Vortrag soll ein Überblick über verschiedene, aktuelle Teilgebiete und den Stand der Technik in diesen Gebieten gegeben werden.

- Dr. Claus Fieker (Sydney): *Konstruktive Klassenkörpertheorie in globalen Körpern*

  Endliche Erweiterungen von Polynomringen über endlichen Körpern haben viele Gemeinsamkeiten mit endlichen Erweiterungen von $\mathbb{Q}$, speziell sind dies Körper, in denen die Produktformel gilt. Diese Körper heißen „Globale Körper".

  Klassenkörpertheorie klassifiziert abelsche Erweiterungen durch Invarianten des Grundkörpers. Die Grundlagen der Theorie sind um 1930 entwickelt worden. Es wurde gezeigt, dass abelsche Erweiterungen durch verallgemeinerte Klassengruppen (Strahlklassengruppen) beschreibbar sind. Es ist jedoch ein offenes Problem, explizite Erzeuger für Klassenkörper zu bestimmen.

  Nachdem es in den letzten Jahren durch Fortschritte in der konstruktiven Zahlentheorie möglich geworden ist, mit Hilfe von algorithmischen Methoden für abelsche Erweiterungen von Zahlkörpern Erzeuger zu bestimmen, ist es nun an der Zeit, generische Algorithmen für globale Körper zu entwickeln.

  In diesem Vortrag werde ich erklären, wie die Klassengruppen zu Strahlklassengruppen verallgemeinert werden und wie dies für die Bestimmung expliziter Erzeuger benutzt werden kann. Ich werde sowohl auf die Gemeinsamkeiten als auch auf die Unterschiede der beiden Typen globaler Körper eingehen und damit auch die Grenzen der generisch „globalen" Methoden aufzeigen.

  Explizite Klassenkörpertheorie für Funktionenkörper hat wichtige Anwendungen in der Kodierungstheorie: Viele der derzeit besten Codes korrespondieren direkt zu abelschen Erweiterungen geeigneter Funktionenkörper. Um diese Codes benutzen zu können, ist das Bestimmen expliziter Erzeuger der erste Schritt.

- Prof. Dr. Martin Kreuzer (Dortmund): *Effiziente Berechnung von Gröbnerbasen*

  Viele wichtige Verfahren der Computeralgebra basieren auf der Berechnung von Gröbnerbasen. Deshalb ist es von zentraler Bedeutung, Algorithmen zu finden, die Gröbnerbasen effizient berechnen sowie bekannte Algorithmen wie den Buchberger-Algorithmus zu optimieren.

  Im ersten Teil des Vortrags betrachten wir verschiedene Möglichkeiten zur Optimierung des Buchberger-Algorithmus im homogenen Fall. Ein wesentlicher Aspekt ist dabei die Minimierung der abzuarbeitenden kritischen Paare. Wann man jedoch ein kritisches Paar als überflüssig betrachen kann, hängt vom Kontext der Berechnung ab. Sicherlich kann man sich auf eine Menge von kritischen Paaren beschränken, die ein minimales Erzeugendensystem des Syzygienmoduls der Leitterme der Gröbnerbasis darstellt. Der neue Algorithmus von Caboara-K.-Robbiano zeigt, dass eine derartige minimale Menge kritischer Paare effizient während einer Gröbnerbasisberechnung gefunden werden kann.

  Im zweiten Teil des Vortrags behandeln wir einige speziellere Fälle von Gröbnerbasisberechnungen, in denen bessere Methoden als der Buchberger-Algorithmus bekannt sind. Unter Anderem betrachten wir die Frage der Berechnung des Kerns einer K-linearen Abbildung $K[x_1, \ldots, x_n] \longrightarrow K^s$, wenn bekannt ist, dass dieser ein Ideal darstellt. Spezialfälle dieses allgemeinen Problems sind z. B. die multivariate Interpolation, Hermite-Interpolation und homogene Implizitisierung. Wir zeigen verschiedene Versionen des Buchberger-Möller Algorithmus, die die Aufgabe über verschienenen Grundkörpern K effizient lösen. Im Fall der Berechnung des homogenen Verschwindungsideals eines projektiven nulldimensionalen Schemas treten weitere Schwierigkeiten auf, weil der Zielvektorraum nicht mehr endlichdimensional ist. Führt man die Endlichkeit dadurch herbei, dass man gradweise vorgeht, so benötigt man ein effizientes Stoppkriterium, wie es z. B. im vorliegenden Fall von Abbott-Bigatti-K.-Robbiano gefunden wurde.

- Prof. Dr. Tsuyoshi Takagi (Darmstadt): *Cryptographical Algorithms*

  Der Vortrag befasst sich mit beweisbarer sicherer Kryptographie. Die Kryptographie ist die fundamentale Infrastruktur für die sichere Kommunikation über das Internet, nämlich SSL/WTSL, IPSEC, WAP, usw. Um das Sicherheitslevel der Kryptographie korrekt einschätzen zu können, benötigen wir Sicherheitsmodelle. Eines dieser Standardmodelle ist die sogenannte Semantische Sicherheit. Im Vortrag wird NICE-X präsentiert, das beweisbar sicher in Hinsicht auf semantische Sicherheit ist und auf quadratischen Zahlkörpern beruht.

Die lokale Leitung liegt in den Händen von Gunter Malle (`malle@mathematik.uni-kassel.de`). Die Anmeldung zur Tagung ist noch bis zum 15. April möglich. Ein Anmeldeformular finden Sie auf der Seite `http://www.mathematik.uni-kassel.de/compmath/ca.htm`. Dort wird demnächst auch das Tagungsprogramm zu finden sein.

Computeralgebra in Lehre, Ausbildung und Weiterbildung IV: 13.-16.04.2004, Kloster Schöntal

Wir möchten an dieser Stelle bereits auf unsere Tagung *Computeralgebra in Lehre, Ausbildung und Weiterbildung IV* hinweisen, die 2004, wieder in der Woche nach Ostern, im Kloster Schöntal stattfinden wird. Rechts sehen Sie ein Foto von einem Vortrag bei der Schöntal-Tagung im vergangenen Jahr. Weitere Informationen, auch zu den vorangegangenen Tagungen, finden Sie auf der Internetseite `http://www.fachgruppe-computeralgebra.de/CLAW`.

Themen und Anwendungen der Computeralgebra

Der folgende Artikel ist unter gleichem Titel in den Mitteilungen der Deutschen Mathematiker-Vereinigung, Heft 4-2002, 14–21 erschienen. Wir bedanken uns für die Erlaubnis, ihn hier in einer gekürzten und aktualisierten Fassung abdrucken zu dürfen.

Ein Durchbruch für „Jedermann“

Folkmar Bornemann

Zusammenfassung

„New Method Said to Solve Key Problem in Math“ titelte die New York Times am 8. August 2002 und meinte den Nachweis von PRIMES $\in \mathcal{P}$, ein bislang großes offenes Problem der algorithmischen Zahlentheorie und theoretischen Informatik. Manindra Agrawal, Neeraj Kayal und Nitin Saxena vom Indian Institute of Technology war es durch einen überraschend eleganten und brilliant einfachen Algorithmus gelungen, die binnen weniger Tage von der Korrektheit überzeugte Fachwelt ins Schwärmen zu versetzen: „This algorithm is beautiful“ (Carl Pomerance), „It’s the best result I’ve heard in over 10 years“ (Shafi Goldwasser).

Vier Tage vor der Schlagzeile in der *New York Times*, an einem Sonntag, hatten die Drei einen neunseitigen Preprint mit dem Titel „PRIMES is in $\mathcal{P}$“ verschickt. Montag früh befand Carl Pomerance das Resultat für korrekt, organisierte in seiner Begeisterung für den Nachmittag ein spontanes Seminar und informierte die *New York Times*. Dienstag wurde der Preprint im Internet frei zugänglich [1]. Donnerstag beendete Hendrik Lenstra Jr. eine kurze Nörgelei im E-Mail-Verteiler `NMBRTHRY` mit dem Diktum:

> The remarks [. . .] are unfounded and/or inconsequential. The proofs [. . .] do NOT have too many additional problems to mention. The only true mistake is [. . .], but that is quite easy to fix. Other mistakes [. . .] are too minor to mention. The paper is in substance completely correct.

Und bereits am Freitag stellte Dan Bernstein einen auf eine Seite verkürzten, geglätteten Beweis des Hauptresultats ins Netz [2].

Diese für die Mathematik ungewöhnlich kurze Prüfungsphase spiegelt neben der Kürze und Eleganz des Arguments auch seine technische Einfachheit wider, „suited for undergraduates“. Zwei der Autoren, Kayal und Saxena, haben selbst erst dieses Frühjahr ihren Bachelor-Abschluss in Computer Science erworben. Handelt es sich also ausnahmsweise um einen für „Jedermann“ verstehbaren Durchbruch?

Hans-Magnus Enzensberger positionierte in seiner Rede auf dem Berliner ICM 1998 die Mathematik sowohl im „Jenseits der Kultur“ als auch in einem goldenen Zeitalter durch Erfolge einer Qualität, die er beim Theater oder Sport vermisste. Allerdings stellen etliche jener Erfolge selbst viele Mathematiker vor die Frage nach dem Jenseits und Diesseits *innerhalb* der Mathematik.

So bastelt jeder an seiner Zinne des Turms zu Babel namens Mathematik und hält die hier erzielten Erfolge für die wesentlichen. Selten genug stellt sich wie jetzt Anfang August ein Erfolg, ja gar ein Durchbruch ein, der vom Fundament des Turms aus für „Jedermann“ in sich verstehbar wäre.

Angesichts dessen sprach Paul Leyland aus, was viele dachten: „Everyone is now wondering what else has been similarly overlooked.“

Kann dies erklären, was Agrawal in großes Erstaunen versetzte („I never imagined that our result will be of much interest to traditional mathematicians“); nämlich warum auf die eigens eingerichtete Webseite innerhalb der ersten zehn Tage über zwei Millionen Zugriffe erfolgten und dreihunderttausendfach der Preprint heruntergeladen wurde?

Als Numeriker kein algorithmischer Zahlentheoretiker, außerhalb meiner Zinne solch ein „Jedermann“, wollte ich die Probe aufs Exempel machen.

Das Problem

Erfreulicherweise motivieren die Drei ihre Arbeit nicht mit der Bedeutung von Primzahlen für die Kryptographie, sondern sie übernehmen zu Beginn vom geschichtsbewussten Don Knuth ein Zitat des großen Carl Friedrich Gauß aus dem Artikel 329 der *Disquisitiones Arithmeticae* (1801), hier wiedergegeben in der Maserschen Übersetzung von 1889:

> Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten als auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. [...] ausserdem dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen.

Kann die Primalität sehr großer Zahlen *prinzipiell* effizient entschieden werden? Diese Frage wird im Rahmen der modernen Komplexitätstheorie mathematisch durch die Forderung einer *polynomialen* Laufzeit konkretisiert, wobei die Eingabelänge der Zahl proportional zur Anzahl der Dualstellen, also in etwa $\log_2 n$ ist. Gibt es also einen deterministischen Algorithmus, der mit einem festen Exponenten κ für jede natürliche Zahl n in $O(\log^\kappa n)$ Rechenschritten entscheidet, ob diese prim ist oder nicht; kurz die bislang große offene Frage: Gilt $\textsc{primes} \in \mathcal{P}$?

Stand der Dinge vor August 2002

Spätestens seit Gauß ist die Entscheidung über die Primalität einer Zahl im Falle der Zusammengesetztheit nicht länger mit einer (partiellen) Faktorisierung verbunden. Im Artikel 334 der *Disquisitiones* heißt es:

> Die letztere [Bemerkung] aber verdient insofern den Vorzug, als sie meistens eine einfachere Rechnung gestattet, indessen giebt sie nicht immer [...] die Factoren der zusammengesetzten Zahlen selbst, jedoch unterscheidet auch sie die zusammengesetzten Zahlen von den Primzahlen.

Ausgangspunkt vieler solcher Verfahren ist der kleine Satz von Fermat. Er besagt, dass für eine *Primzahl* n und eine zu n teilerfremde Zahl a stets gilt

$$a^n \equiv a \mod n.$$

Leider ist die Umkehrung falsch, Primzahlen lassen sich auf diese Weise nicht charakterisieren. Andererseits „using the Fermat congruence is so simple, that it seems a shame to give up on it just because there are a few counter examples“ (Carl Pomerance). So nimmt es nicht Wunder, dass Verfeinerungen dieses Kriteriums Grundlage wichtiger Algorithmen sind:

Der elementare *probabilistische* Algorithmus von Miller und Rabin aus dem Jahre 1976 bemüht einen Zufallszahlengenerator und stellt nach k Durchläufen entweder fest, dass die Zahl *mit Sicherheit* zusammengesetzt ist, oder dass die Zahl *höchstwahrscheinlich* prim ist, wobei die Wahrscheinlichkeit eines Irrtums bei unter 4^{-k} liegt. Die Zeitkomplexität liegt bei $O(k \log^2 n)$, wobei das Groß-O eine relativ kleine Konstante enthält. Der Algorithmus ist in der Praxis also sehr schnell und findet seine Verwendung in der Kryptographie zur Produktion von „industrial-grade primes“ (Henri Cohen). In der Sprache der Komplexitätstheorie heißt dies knapp $\textsc{primes} \in \text{co-}\mathcal{RP}$.

Beim *deterministischen* Algorithmus von Adleman, Pomerance und Rumely aus dem Jahre 1983 wird sehr viel mehr Theorie betrieben und der kleine Fermatsche Satz so auf ganze Zahlen eines Kreisteilungskörpers verallgemeinert, dass Primzahlen vollständig charakterisiert werden können. Die Laufzeit liegt bei superpolynomialem $(\log n)^{O(\log \log \log n)}$, die beste für einen deterministischen Algorithmus vor dem August 2002. Der dreifache Logarithmus im Exponenten wächst allerdings so langsam, dass sich praktische Varianten im Rekordfieber von Primalitätsbeweisen für Zahlen mit mehreren tausend Dezimalstellen exzellent geschlagen haben.

Eine andere Klasse moderner Algorithmen benutzt elliptische Kurven beziehungsweise abelsche Varietäten höheren Geschlechts. So konnten Adleman und Huang 1992 in einem sehr schwierigen und technischen Büchlein zeigen, dass es einen *probabilistischen* Algorithmus polynomialer Laufzeit gibt, der nach k Durchläufen entweder eine definitive Antwort liefert (Irrtum ausgeschlossen) oder gar keine, letzteres aber mit einer Wahrscheinlichkeit kleiner 2^{-k}. In der Sprache der Komplexitätstheorie heißt dies knapp $\textsc{primes} \in \mathcal{ZPP}$.

Vor diesem Hintergrund, angesichts des erreichten Schwierigkeitsgrades und des Ausbleibens weiterer Erfolge in über zehn Jahren, war nicht zu erwarten, dass die Ausgangsfrage kurz, elegant und für „Jedermann“ verständlich beantwortet werden könnte.

Manindra Agrawal

Auftritt Manindra Agrawal

Der Informatiker und Komplexitätstheoretiker Manindra Agrawal erwarb 1991 seinen Doktortitel am Department of Computer Science & Engineering des Indian Institute of Technology in Kanpur (IITK). Nach einem Aufenthalt als Humboldt-Stipendiat an der Universität Ulm 1995/96 („I really enjoyed the stay in Ulm. It helped me in my research and career in many ways.“) kehrte er als Professor nach Kanpur zurück. Er hatte vor zwei Jahren auf sich aufmerksam gemacht, als er eine abgeschwächte Form der Isomorphie-Vermutung der Komplexitätstheorie bewies.[2]

Um 1999 arbeitete er mit seinem Doktorvater Somenath Biswas an der Frage, mit probabilistischen Algorithmen die Gleichheit von Polynomen zu entscheiden. Als unschuldige Anwendung findet sich in der Publikation „Primality and Identity Testing via Chinese Remaindering“ ein neuer probabilistischer Primalitätstest.

Ausgangspunkt war dabei eine Verallgemeinerung des kleinen Fermatschen Satzes auf *Polynome*, die eine leichte Übungsaufgabe für eine einführende Zahlentheorie- oder Algebra-Vorlesung sein könnte: Sind die natürlichen Zahlen a und n teilerfremd, so ist n *dann und nur dann* prim, wenn im Ring der Polynome $\mathbb{Z}[x]$ gilt

$$(x-a)^n \equiv (x^n - a) \mod n.$$

Eine sehr elegante Charakterisierung von Primzahlen, aber zunächst keine brauchbare. Allein die Berechnung von $(x-a)^n$ verlangt mehr Rechenzeit als das Sieb des Eratosthenes. Aber gerade für Polynome dieser Größe hatten Agrawal und Biswas einen probabilistischen Gleichheitstest beschränkter Irrtumswahrscheinlichkeit entwickelt, der auf die vollständige Aufstellung der Polynome verzichtete. Leider befand sich der resultierende Test polynomialer Laufzeit weit außer Konkurrenz zu dem von Miller und Rabin. Eine neue Idee war geboren und taugte zunächst nur für eine Fußnote in der Geschichte der Primalitätstests.

Zwei Jahre später begann Agrawal, mit seinen Studenten am IITK das Potential der neuen Primzahlcharakterisierung, an das er fest glaubte, genauer zu untersuchen.

Zwei Bachelor-Arbeiten

Das Zulassungsverfahren zum Studium am Indian Institute of Technology ist äußerst streng und selektiv. Für das Studium an einem der sieben Standorte des IIT und zwei weiteren Institutionen gibt es ein zweistufiges gemeinsames Zulassungsverfahren („Joint Entrance Examination (JEE)“). So bewarben sich für die Zulassung im letzten Jahr 150 000 Inder, nach einer ersten dreistündigen Klausur in Mathematik, Physik und Chemie wurden 15 000 zur zweiten Prüfung eingeladen, bestehend aus je einer zweistündigen Klausur in den drei Fächern. Schließlich wurden 2900 Studienplätze vergeben, davon 45 für Informatik am sehr renommierten IIT in Kanpur. Kein Wunder, dass in Indien gutes Geld mit der Vorbereitung der Kandidaten auf die gefürchtete JEE verdient wird und Absolventen des IIT in aller Welt mit Kusshand eingestellt werden.

Mit solch hochmotivierten Studenten arbeitete Agrawal nun weiter am Primalitätstest. Mit Rajat Bhattacharjee und Prashant Pandey kam die Idee auf, statt der viel zu großen Polynompotenzen $(x-a)^n$ nur deren Reste nach Division durch $x^r - 1$ zu betrachten. Bleibt r logarithmisch in n, so lassen sich diese sehr viel kleineren Reste mit geschickten Algorithmen direkt in polynomialer Laufzeit berechnen.

Ist n eine Primzahl, so ist sicherlich[3]

$$(x-a)^n \equiv x^n - a \mod (x^r - 1, n) \qquad (T_{r,a})$$

für jedes r und zu n teilerfremde a. Welche a und r erlauben den umgekehrten Schluss, dass n prim ist?

Die beiden Studenten fixierten in ihrer gemeinsamen Bachelor-Arbeit $a = 1$ und untersuchten die nötigen r. Durch Auswertung von Experimenten mit $r \leq 100$ und $n \leq 10^{10}$ gelangten sie zu folgender Vermutung. Falls r und n teilerfremd sind und

$$(x-1)^n \equiv x^n - 1 \mod (x^r - 1, n) \qquad (T_{r,1})$$

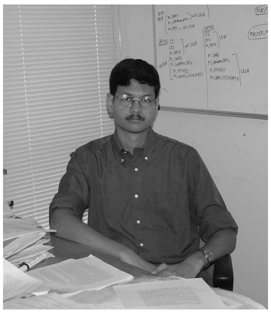
gilt, ist entweder n prim oder es gilt $n^2 \equiv 1 \mod r$. Letzteres ist für eine der ersten $\log_2 n$ Primzahlen r

[2] Die Isomorphie-Vermutung von Berman und Hartmanis impliziert $\mathcal{P} \neq \mathcal{NP}$.

[3] Ich folge der Notation von Agrawal et al. und bezeichne mit $p(x) \equiv q(x) \mod (x^r - 1, n)$ die Gleichheit der Reste der Polynome $p(x)$ und $q(x)$ nach Division durch $x^r - 1$ und Division der Koeffizienten durch n.

nicht der Fall, so dass man einen Nachweis der Primalität von n in polynomialer Laufzeit $O(\log^{3+\varepsilon} n)$ erhalten würde.

Neeraj Kayal



Nitin Saxena

Nun traten die bislang fehlenden Helden unserer Geschichte auf, die Studenten Neeraj Kayal und Nitin Saxena. Beide waren Mitglieder der indischen Mannschaft bei der internationalen Mathematik-Olympiade 1997. Informatik statt Mathematik studierten sie wegen der besseren Berufsaussichten, fanden aber in der Komplexitätstheorie einen Weg, sich weiterhin mit Mathematik auf hohem Niveau zu befassen.

Sie untersuchten in ihrer gemeinsamen Bachelor-Arbeit die Beziehung des Tests $(T_{r,1})$ zu bekannten Primalitätstest-Primitiven und führten im Zusammenhang einer von ihnen untersuchten Gruppe „introspektiver" Zahlen eine Beweisidee ein, die sich später als wesentlich erweisen sollte.

Die im April 2002 abgegebene Arbeit der beiden trägt den Titel „Towards a deterministic polynomial-time primality test". Eine Vision, das Ziel ist schon fest im Auge.

Veränderung des Blickwinkels

Sie fuhren in diesem Sommer zunächst nicht zur Familie nach Hause, sondern begannen sofort mit dem Doktorstudium. Saxena hatte eigentlich ins Ausland gehen wollen, aber – Ironie des Schicksals – kein Stipendium für die Universität seiner Wahl erhalten.

Nur eine kleine Veränderung des Blickwinkels ist noch nötig. Beide Bachelor-Arbeiten haben den Test $(T_{r,a})$ für festes $a = 1$ und variierendes r studiert. Was kommt heraus, wenn man stattdessen r fixiert und a variieren lässt? Am Morgen des 10. Juli gelang der Durchbruch: Bei geeigneter Wahl der Parameter erhält man nichts weniger als eine Charakterisierung von *Primzahlpotenzen.*

Das durch Dan Bernstein geglättete Ergebnis lautet nun wie folgt.

Satz von Agrawal-Kayal-Saxena. *Für $n \in \mathbb{N}$ seien q, r prim und $s \leq n$ so gewählt, dass $q \mid r-1$, $n^{(r-1)/q} \not\equiv 0, 1 \mod r$ und*

$$\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}.$$

Gilt dann für alle $1 \leq a < s$, dass (i) a teilerfremd zu n ist und (ii) im Ring der Polynome $\mathbb{Z}[x]$ $(x-a)^n \equiv x^n - a \mod (x^r - 1, n)$ gilt, so ist n eine Primzahlpotenz.

Der einfache, kurze und ideenreiche Beweis des Satzes bereitet soviel Vergnügen, dass er jedem Leser zur Lektüre ans Herz gelegt sei.

Der Satz führt unmittelbar zum mittlerweile so genannten **AKS-Algorithmus**:

1. Entscheide, ob n echte Potenz einer natürlichen Zahl ist. Wenn ja, gehe zu Schritt 5.
2. Wähle (q, r, s) gemäß den Voraussetzungen des Satzes.
3. Für $a = 1, \ldots, s-1$ tue jeweils folgendes:
   (i) Ist a Teiler von n, gehe zu Schritt 5.
   (ii) Ist $(x-a)^n \not\equiv x^n - a \mod (x^r - 1, n)$, gehe zu Schritt 5.
4. n ist prim. Fertig.
5. n ist zusammengesetzt. Fertig.

Schritt 1 lässt sich mit Varianten der Newton-Iteration in polynomialer Laufzeit erledigen. Die Laufzeit des dominierenden Schrittes 3 ist bei Verwendung schneller FFT-basierter Arithmetik gegeben durch $\tilde{O}(s\, r \log^2 n)$, wobei die Tilde über dem Groß-O weitere logarithmische Faktoren in s, r und $\log_2 n$ unterdrückt.

Wir müssen also für unser Ziel s und r höchstens polynomial in $\log n$ wachsen lassen. Dies ist Aufgabe des Schritts 2. Schauen wir uns zunächst an, was prinzipiell möglich ist. Wählt man $s = \theta q$ mit einem festen Faktor θ, so liefert die Stirlingsche Formel die Asymptotik

$$\log \binom{q+s-1}{s} \sim c_\theta^{-1} q.$$

Die Bedingungen des Satzes erfordern demnach asymptotisch

$$q \gtrsim 2c_\theta \lfloor\sqrt{r}\rfloor \log n.$$

Für große n kann das im wesentlichen nur funktionieren, wenn es wenigstens unendlich viele Primzahlen r gibt, so dass $r-1$ einen Primfaktor $q \geq r^{1/2+\delta}$ besitzt. Dabei handelt es sich um ein gut studiertes Problem der analytischen Zahlentheorie.

Sophie Germain und die Fermatsche Vermutung

Das bestmögliche Preis-Leistungsverhältnis q/r erhält man für die nach Sophie Germain benannten ungeraden Primzahlen q, für welche auch $r = 2q + 1$ prim ist. Sie hatte 1823 für diese Primzahlen gezeigt, dass der sogenannte erste Fall der Fermatschen Vermutung gilt: $x^q + y^q = z^q$ besitzt keine ganzzahlige Lösung mit $q \nmid xyz$. Deshalb begann man sich brennend dafür zu interessieren, ob es denn wenigstens unendlich viele dieser freundlichen Primzahlen gibt. Unglücklicherweise weiß man es bis auf den heutigen Tag nicht. Heuristische Überlegungen führten Hardy und Littlewood 1922 jedoch zu folgender sehr präzisen Vermutung über die tatsächliche Dichte von Germain-Primzahlen

$$\#\{q \leq x \mid q \text{ und } 2q+1 \text{ sind prim}\} \sim \frac{2C_2\, x}{\ln^2 x},$$

wobei $C_2 = 0,6601618158\ldots$ die Primzahlzwillings-Konstante ist.

Wäre diese Vermutung richtig, so könnte man Primzahlen q und $r = 2q+1$ der Größe $O(\log^2 n)$ finden, welche den Voraussetzungen des Satzes der Drei entsprechen. Der AKS-Algorithmus hätte dann die polynomiale Laufzeit $\tilde{O}(\log^6 n)$. Da die Vermutung bis $x = 10^{10}$ eindrucksvoll bestätigt worden ist, wird sich der AKS-Algorithmus in jedem Fall für bis zu 100 000-stellige Zahlen n wie einer der Komplexität $\tilde{O}(\log^6 n)$ verhalten.

Fast zehn Jahre vor dem endgültigen Beweis der Fermatschen Vermutung durch Andrew Wiles bewiesen Adleman, Fouvry und Heath-Brown 1985, was mit Hilfe der Germain-Primzahlen nicht gelungen war, nämlich dass der erste Fall für unendlich viele Primzahlen richtig ist [3]. Dabei hatten Adleman und Heath-Brown in Verallgemeinerung der Germain-Primzahlen genau jene Paare (q, r) studiert, die auch für den AKS-Algorithmus eine große Rolle spielen.

Eine Fields-Medaille

Präzise verlangten sie, dass die Abschätzung

$$\#\left\{r \leq x \mid q, r \text{ prim}; \ q \mid r-1; \ q \geq x^{1/2+\delta}\right\} \geq c_\delta \frac{x}{\ln x}$$

einen zulässigen Exponenten $\delta > 1/6$ besitzt. Die Jagd nach dem größten δ hatte 1969 mit Morris Goldfeld [4] begonnen, der $\delta \approx 1/12$ erhalten hatte. Étienne Fouvry [5] beendete sie vorläufig 1985 mit $\delta = 0,1687 > 1/6$. Alle diese Arbeiten benutzen sehr tiefe Methoden aus der analytischen Zahlentheorie, welche das *große Sieb* des Enrico Bombieri weiterentwickeln. Dieses Sieb hatte er 1965 im Alter von 25 Jahren publiziert, 1974 erhielt er die Fields-Medaille. Es dürfte also „Jedermann“ schwer fallen, den Beweis dieser Abschätzung im Detail verstehen zu wollen. Manindra Agrawals Antwort auf meine Frage, ob sich einer der Drei dieser Mühe unterzogen hätte, lautet:

> We tried! But Sieve theory was too dense for us – we have no background in analytical number theory. So after a while we just gave up.

Sie brauchten es auch nicht, „the result was stated there in precisely the form we needed“, und sie konnten sich seiner Korrektheit im Vertrauen auf Begutachtungen und eines gewissen zeitlichen Abstandes gewiss sein. Umso mehr als das Ergebnis von Fouvry im Zusammenhang mit der heiß umkämpften Fermatschen Vermutung stand und in den *Inventiones* erschienen war.

Oder doch nicht? Fouvry vergaß bei der Zitation eines Lemmas von Bombieri, Friedlander und Iwaniec eine Bedingung mit anzugeben und mit zu berücksichtigen. Diese zusätzliche Bedingung *verkleinert* den ermittelten Wert von δ auf $\delta = 0,1683 > 1/6$. Er hätte auch unterhalb der kritischen Schwelle sein können. Fouvry hat diese Korrektur später Roger Baker mitgeteilt und sie ist in einem Überblicksartikel [6] von diesem und Glyn Harman 1996 publiziert worden.

Agrawal, Kayal und Saxena waren übrigens auf Fouvrys Artikel über eine Internetsuche mit *Google* in der Literaturliste einer Arbeit von Pomerance und Shparlinski gestoßen. Auf Nachfrage nach dem besten bekannten Wert für δ hatte Ersterer sie dann auf die Arbeit von Baker und Harman verwiesen.

Unabhängig vom bestmöglichen Wert reicht $\delta > 0$ aus, um ein für den AKS-Algorithmus zulässiges Tripel (q, r, s) der benötigten polynomialen Größe zu garantieren,

$$r = O(\log^{1/\delta} n), \qquad q, s = O(\log^{1+1/2\delta} n).$$

Der AKS-Algorithmus hat damit insgesamt eine garantierte Laufzeit von $\tilde{O}(\log^{3+3/2\delta} n)$. Damit ist die Aussage PRIMES $\in \mathcal{P}$ bewiesen, der Durchbruch gelungen.[4] Gratulation! Fouvrys korrigierter Wert für δ liefert $\tilde{O}(\log^{11,913} n)$, oder einfacher zu merken und dann auch ohne Tilde: $O(\log^{12} n)$.

Der Direktor des IIT in Kanpur, Sanjay Dhande, war so begeistert von der Schlagzeile in der New York Times, dass er sich sicher zeigte, Agrawal würde für die höchsten Auszeichnungen in der Mathematik nominiert.[5] In vier Jahren wird er 40 Jahre alt sein.

Wie praktisch!?

In den Newsgroups und den Zeitungen wird schnell die Frage nach der praktischen Verwertbarkeit gestellt, sind doch große Primzahlen heute wichtiger Bestandteil der Kryptographie. Halten wir zunächst einmal fest, dass ein wichtiges *theoretisches* Problem gelöst wurde, an dem

[4] Am 22. Januar 2003 stellte Dan Bernstein eine Version seines Papiers [2] ins Netz, die eine leichte Variation des Satzes von Agrawal-Kayal-Saxena enthält und es erlaubt, ganz ohne tiefliegende analytische Zahlentheorie auszukommen. Nach Anwendung eines Satzes von Tschebyscheff (das Produkt der Primzahlen $\leq 2k$ ist mindestens 2^k) ergibt sich nämlich, dass der Algorithmus mit $r, s = O(\log^5 n)$ funktioniert. Somit ist heute der Nachweis von PRIMES $\in \mathcal{P}$ vollständig elementar und bis ins letzte für „Jedermann“ nachvollziehbar. Diese Variation wurde Bernstein bereits am 14. August 2002 von ihrem Erfinder Hendrik Lenstra mitgeteilt. Vielleicht hat Paulo Ribenboim ja recht, wenn er mir schreibt: „Our specialists should reflect about their convoluted reasoning.“

[5] Am 30. Oktober 2002 wurde ihm bereits der *Clay Research Award* verliehen. Bisherige Preisträger waren Andrew Wiles, die Stochastiker Smirnov und Schramm und die Träger der Fields-Medaille Connes, Lafforgue und Witten.

sich mehrere Jahrzehnte die Fachwelt vergeblich versucht hat. Agrawal selbst betont stets, dass ihn das Problem als intellektuelle Herausforderung interessiert hat und der AKS-Algorithmus gegenwärtig sehr viel langsamer ist als jene Algorithmen, mit welchen die Rekorde der Stellenanzahl von Primzahlbeweisen auf derzeitig 5020 Dezimalstellen[6] hochgetrieben wurden. Man darf schließlich nicht vergessen, dass es sich bei der Definition von Komplexitätsklassen wie $\mathcal{P}$ um das rein theoretische Konzept einer asymptotischen Aussage für $n \to \infty$ handelt. Der Laufzeitvorteil eines polynomialen gegenüber eines superpolynomialen Algorithmus kann daher im Einzelfall sehr wohl erst für so große n in Erscheinung treten, für die keiner der beiden Algorithmen auf gängiger Hardware noch zu unseren Lebzeiten eine Antwort liefern würde. Es kommt in der Praxis auch auf die Konstanten im Groß-O der Komplexitätsabschätzung an.

„Industrial-grade primes“ unterer Qualitätsstufe mit 512 Dualstellen werden auf einem handelsüblichen 2GHz-PC mit Hilfe des Miller-Rabin-Tests in Bruchteilen einer Sekunde erzeugt. Bei Bedarf kann in wenigen Sekunden mit dem auf elliptischen Kurven basierenden ECPP-Verfahren nach Atkin-Morain ihre Primalität tatsächlich *bewiesen* werden.[7] Die Laufzeitkomplexität dieses *probabilistischen* Algorithmus ist zwar eine „cloudy issue“ (Carl Pomerance), aber heuristische Überlegungen legen nahe, dass der Erwartungswert gerade auch bei $\tilde{O}(\log^6 n)$ liegt.

Hingegen ist wegen der hohen Kosten der polynomialen Kongruenzen im dritten Schritt des AKS-Algorithmus die Konstante im vermuteten $\tilde{O}(\log^6 n)$-Laufzeitverhalten so groß, dass er an einer 512-Bit-Primzahl zur Zeit etwa ein paar Tage arbeiten müsste.[8] Dabei ist diese Konstante dank Dan Bernstein, Hendrik Lenstra, Felipe Voloch, Bjorn Poonen und Jeff Vaaler bereits gegenüber der ursprünglichen Formulierung des Algorithmus um wenigstens den Faktor $2 \cdot 10^6$ verbessert worden – Stand vom 25. Januar 2003, vgl. [2].

Es fehlt also noch etwa ein Faktor 10^5 zur Konkurrenzfähigkeit. Auch das ECPP-Verfahren startete mit einer völlig inpraktikablen, aber grundlegend neuen Idee von Goldwasser und Kilian. Und die jetzt von Agrawal, Kayal und Saxena vorgelegte Methode ist so unvorhergesehen neu und brilliant, dass wir getrost abwarten können, wozu sie im weiteren Reifungsprozess noch alles fähig sein wird.

Zukunftspläne

Die Drei planen, ihre Arbeit bei den *Annals of Mathematics* einzureichen und befinden sich hierzu im Kontakt mit Peter Sarnak. Sie wollen den Artikel neu aufschreiben, „in a more ‘mathematical’ way as opposed to ‘computer science’ way as that would be more suitable in Annals“.

Und zur Gefühlslage und Zukunft der beiden Doktoranden Kayal und Saxena sagt Agrawal:

> They are happy, but at the same time quite cool about it. I would say they are very level-headed boys. As for their PhD, yes I am sure that this work will qualify for their PhD. But I have advised them to stay back for a couple of years since this is the best time they have for learning. They still need to pick up so many things. But they are free to make the decision – they already have an offer from TIFR [Tata Institute of Fundamental Research].

Danksagung

Mein herzlicher Dank gilt Manindra Agrawal für die Bereitwilligkeit, mit der er trotz tausender Gratulationen per E-Mail meine Fragen nach Hintergrundinformationen sehr persönlich und ausführlich beantwortete.

Stark gekürzte und aktualisierte Fassung des Beitrags gleichen Titels in den *Mitteilungen der Deutschen Mathematiker-Vereinigung*, Heft 4-2002, 14–21.

Adresse des Autors:
Prof. Dr. Folkmar Bornemann
Zentrum Mathematik
Technische Universität München
85747 Garching bei München
`bornemann@ma.tum.de`

Literatur

[1] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, PRIMES *is in P*, IIT Kanpur, Preprint vom 6. 8. 2002, `www.cse.iitk.ac.in/news/\\primality.html`.

[2] Daniel Bernstein, *Proving Primality after Agrawal-Kayal-Saxena*, Fassung vom 25. 1. 2003, `cr.yp.to/papers.html\#aks`.

[3] D. Roger Heath-Brown, *The First Case of Fermat's Last Theorem*, Math. Intelligencer 7(4), pp. 40–47&55, 1985.

[4] Morris Goldfeld, *On the number of primes p for which $p + a$ has a large prime factor*, Mathematika 16, pp. 23–27, 1969.

[6] Bitte nicht mit der Rekordjagd nach der *größten* bekannten Primzahl verwechseln, zur Zeit $2^{13\,466\,917} - 1$, eine Mersennesche Primzahl mit 4 053 946 Dezimalstellen. Diese Zahlen sind voller Struktur und lassen hochspezialisierte Algorithmen ans Werk.

[7] Z. B. mit dem unter `http://www.znz.freesurf.fr/pages/primo.html` frei verfügbaren Programm PRIMO von Marcel Martin, das derzeitig den Rekord hält.

[8] Ein entsprechendes Experiment dürfte in den nächsten Monaten sicherlich erfolgen.

[**5**] Étienne Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, Invent. Math. 79, 383–407, 1985.

[**6**] Roger C. Baker, Glyn Harman, *The Brun-Titchmarsh Theorem on Average*, in *Proceedings of a conference in honor of Heini Halberstam, Vol. 1*, pp. 39–103, 1996.

Polynomielle Gleichungen mit Massenwirkungskinetik

Karin Gatermann (Berlin)

Bei der Modellierung von chemischen Reaktionssystemen treten spezielle dünnbesetzte polynomielle Gleichungssysteme auf, die wir mit Methoden der Computeralgebra, algebraischen Geometrie und der diskreten Mathematik untersuchen. Ziel ist es, die Struktur der Gleichungen und ihre Konsequenzen so genau wie möglich zu verstehen.

Das zeitliche (bzw. raumzeitliche) Verhalten der Konzentrationen x_i von Chemikalien während einer Reaktion wird durch eine gewöhnliche Differentialgleichung (bzw. partielle Differentialgleichung) beschrieben. Das Standardmodell ist die sogenannte *Massenwirkungskinetik*, wodurch eine polynomielle Differentialgleichung

$$\dot{x} = Y_s I_a I_K \Psi(x), \quad \Psi_j(x) = x^{y_j}, j = 1, \ldots, n$$

entsteht. Dabei sind die Matrizen Y_s und I_a durch die Struktur der Reaktionen (Stöchiometrie) gegeben, während die Matrix I_K die Reaktionsgeschwindigkeiten k_{ij} als Parameter enthält, von denen oft nur die Größenordnung bekannt ist. Die Exponenten der auftretenden Monome sind im Wesentlichen Spalten der Matrix Y_s. Zusätzliche Bedingungen wie z. B. die Massenerhaltung werden durch lineare Gleichungen $v_i^t x - c_i = 0$ berücksichtigt. Die Hauptfrage, zu deren Antwort die Computeralgebra einen Beitrag leistet, ist die Frage nach positiven stationären Lösungen und deren Abhängigkeit von den Parametern. Diese Frage fällt folglich in das Gebiet der reellen algebraischen Geometrie.

Für Anwender ist die Analyse der Gleichungsstruktur von großer Bedeutung, da diese Struktur die Struktur der Lösungen impliziert. Insbesondere interessiert die Abhängigkeit von den Parametern. So können bei der Modellierung von chemischen Prozessen schon sehr früh Modelle verworfen werden (Modelldiskriminierung). Das ist der erste Schritt zum Verständnis des dynamischen Verhaltens. Insbesondere ist das Auftreten mehrerer reeller positiver Lösungen die Grundlage für die Existenz von Reaktions-Diffusions-Wellen. Außerdem ist es die Voraussetzung für die Anwendung der singulären Störungstheorie.

Über die stationären Lösungen der Differentialgleichungen, ihre Stabilität und Hopf-Verzweigung gibt es eine reichhaltige nicht-algebraische Literatur [1,3,4,5]. Sehr bekannt sind zum Beispiel das deficiency-zero-Theorem und das deficiency-one-Theorem von Feinberg [4,5]. Wie wir in [6] gezeigt haben, beruht das deficiency-one-Theorem darauf, dass eine homogene torische Varietät einen eindeutigen Schnitt mit einem Kegel hat (siehe Abbildung 1 auf Seite 16).

Um dies zu verstehen, ist die torische Geometrie, sind also die torischen Ideale und ihre zugehörigen Varietäten entscheidend.

Im Gegensatz zur recht abstrakten Theorie betrachten wir Varietäten, die der Theoretiker als konkrete Einbettungen bezeichnet. Gegeben Polynome mit auftretenden Monomen $x^{y_1}, \ldots, x^{y_n}$ und Matrix der Exponenten, so bezeichnet man

$$I_{\hat{Y}} = \{f \in \mathbb{C}[z] \mid f(x_0 x^{y_1}, \ldots, x_0 x^{y_n}) = 0, \ \forall x, x_0\}$$

als homogenes torisches Ideal. Die Monome parametrisieren die zugehörige torische Varietät. In Singular und anderen CA-Systemen gibt es Implementationen effizienter Spezialalgorithmen für die Berechnung von Gröbnerbasen solcher torischen Ideale. Eine einfache und fundamentale Idee der algebraischen Geometrie ist, die Lösung des ursprünglichen Gleichungssystems auf die Lösung eines linearen, eines binomiellen und eines monomiellen Gleichungssystems zurückzuführen.

Ein wichtiges Ergebnis der torischen Geometrie betrifft die Anzahl der komplexen Lösungen von dünnbesetzen Gleichungssystemen. Diese sogenannte BKK-Anzahl kann man entweder durch eine gemischte Unterteilung der Newton-Polytope ausrechnen [2] oder aus dem Hilbert-Polynom des torischen Ideals ermitteln [11].

Eine Modifikation der Idee findet man in den Arbeiten von Clarke [1]. Bei unseren Betrachtungen wird der Kern von $Y_s I_a$ mit der *deformierten torischen Varietät* geschnitten. Da nur positive Lösungen chemisch sinnvoll sind, schränkt man den Kern der Matrix auf den positiven Orthanden ein. Diese Menge ist ein konvexer Kegel. Die Berechnung der minimalen Erzeuger dieses Kegels ist Gegenstand vieler Programme in der Chemie, Biochemie etc. Die Resultate bzgl. Stabilität der stationären Lösung und Hopf-Verzweigung in den Arbeiten von Clarke [1] und anderen [3,10] basieren auf diesen Kegelerzeugern.

Unsere Arbeit hebt hervor, dass es zwei unterschiedliche Typen von Kegelerzeugern gibt. Der erste Typ ist durch die chemischen Reaktionen selbst gegeben, während der zweite Typ die involvierten chemischen Spezies berücksichtigt. Wir begründen mathematisch, warum diese speziellen Polynome die fundamentalen Voraussetzungen eines chemisch sinnvollen Modells erfüllen. Entscheidend ist dabei die Struktur der Newton-Polytope, der konvexen Hülle der Exponenten (siehe Abbildung 2 auf Seite 16).

In [8] untersuchen wir das Auftreten von Multistationarität, d. h. das gleichzeitige Auftreten von mehreren positiven Lösungen. Zuerst stellt man fest, für welche Parametergebiete sogenannte complex balancing Lösungen auftreten. Dies wird mit dem Cayley-Trick bewiesen. Weit entfernt von diesem Parametergebiet kann es zu Multistationarität kommen. Ursache dafür ist die Deformation des torischen Ideals zu Untersystemen, die durch Kegelerzeuger des zweiten Typs gegeben sind. Deren entartetes Gitter ist der Grund von Multistationarität.

Im Laufe dieser Untersuchungen wurde unter anderem ein neues Ergebnis für allgemeine polynomielle Differentialgleichungen bewiesen. Das Zählen von stationären Lösungen mit der Viro-Methode wurde auf stabile Lösungen verallgemeinert [7].

Auch die Hopf-Verzweigung kann mit diesen algebraischen Methoden bearbeitet werden. Während Clarke [1] und andere gewisse diskrete Strukturen für die Hopf-Verzweigungspunkte verantwortlich machen, betrachten wir verschiedene Repräsentanten des Restklassenringes mittels Gröbnerbasen, um verfeinerte Aussagen auch über das Parametergebiet zu treffen. In [10] wurden zum Beispiel die periodischen Lösungen eines Modells für Kalziumoszillationen in einer Zelle behandelt. Andere berechnete Beispiele beinhalten die Elektrooxidation von Ameisensäure.

Literatur

[1] Clarke, B. L., *Stability of Complex Reaction Networks.* Adv. Chem. Phys. 42, 1–213, 1980.

[2] Cox, D. and Little, J. and O'Shea, D., *Using Algebraic Geometry.* Springer, 1998.

[3] Eiswirth, M., Bürger, J., Strasser, P. and Ertl, G., *Oscillating Langmuir-Hinshelwood Mechanisms.* J. Phys. Chem. 100, 19118–19123, 1996.

[4] Feinberg, M., *The existence and uniqueness of steady states for a class of chemical reaction networks.* Arch. Rational Mech. Anal. 132, 311–370, 1995.

[5] Feinberg, M., *Multiple Steady States for Chemical reaction networks of deficiency one.* Arch. Rational Mech. Anal. 132, 371–406, 1995.

[6] Gatermann, K., Huber, B., *A family of sparse polynomial systems arising in chemical reaction systems.* Journal of Symbolic Computation, 33, 275–305, 2002.

[7] Gatermann, K., *Counting stable solutions of sparse polynomial systems in chemistry.* In Symbolic Computation: Solving Equations in Algebra, Geometry, and Engineering, Green, E. et al (ed.), Contemporary Mathematics 286, 53–69, AMS, 2001.

[8] Gatermann, K., Wolfrum, M., *Bernstein's 2nd theorem and Viro's method for sparse polynomial systems in chemistry.* In Vorbereitung 2003.

[9] Gatermann, K., Sensse, A., *Storch – Stability analysis of reactions in chemistry.* Software in Maple, 2002. Erhältlich unter `http://www.zib.de/gatermann/massaction.html`.

[10] Sensse, A., *Algebraic methods for the analysis of Hopf bifurcations in biochemical networks.* Diplomarbeit an der HU Berlin, 2002.

[11] Sturmfels, B., *Gröbner Bases and Convex Polytopes.* University Lecture Series 8, AMS, 1996.

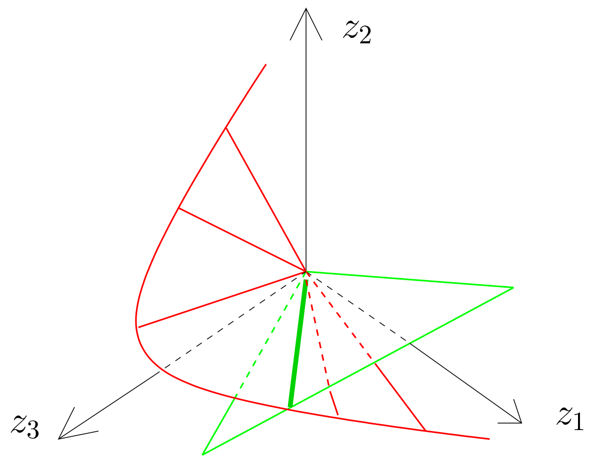


Abbildung 1: Illustration des deficiency-one-Theorems. Die homogene torische Varietät schneidet einen Kegel.

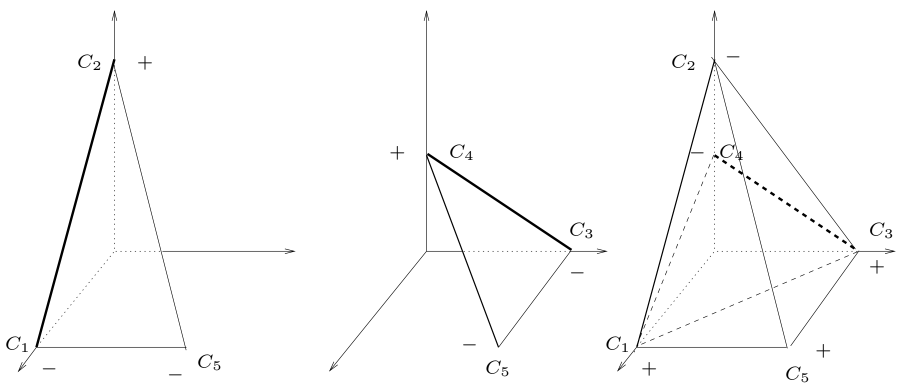


Abbildung 2: Newton-Polytope mit Vorzeichen der Koeffizienten.

Neues über Systeme

Magma

Claus Fieker (Sydney)

Über Magma
MAGMA ist ein Computeralgebrasystem mit dem Schwerpunkt im Bereich Algebra. MAGMA wird an der Universität von Sydney unter der Leitung von John Cannon entwickelt. Im Vergleich zu anderen CA-Systemen ist MAGMA auf diesem Gebiet das weitaus vollständigste System. Es enthält unter anderem Module für

- Gruppentheorie
- Zahlentheorie
- kommutative Algebra
- Geometrie
- Lie-Theorie
- Codierungstheorie, Kryptographie
- Graphentheorie

um nur einen ganz groben Überblick zu geben. Eine vollständige Liste gibt es unter `http://magma.maths.usyd.edu.au/magma/Features/Features.html`. Die Stärke von MAGMA liegt sowohl in der Breite des abgedeckten Spektrums als auch darin, dass MAGMA versucht, in allen Bereichen die schnellste Implementierung zu bieten. Obwohl dies nicht überall gelingt, so schneidet es doch in fast allen Benchmarkproblemen sehr gut ab. Der Laufzeitverlust ist im Vergleich zu spezialisierten Programmen – wenn überhaupt vorhanden – minimal und wird meist durch die mathematische Breite mehr als kompensiert. Durch die Breite bietet sich oftmals die Möglichkeit, mehr Theorie einzusetzen oder auch nur die Gelegenheit mehr „mathematisch“ (d. h. direkt mit den mathematischen Objekten statt mit Datenstrukturen) zu programmieren, was Zeit spart. Auch wenn z. B. alle Operationen mit endlichen abelschen Gruppen auf Operationen mit Matrizen abgebildet werden können, so ist es oft hilfreich, wenn dies für den Benutzer nicht sichtbar ist.

MAGMA hat eine eigene Programmiersprache, die zunächst etwas gewöhnungsbedürftig ist, jedoch durch ihre Nähe zur Mathematik besticht. Die Leistungsfähigkeit der Sprache kann man daran sehen, dass ein Großteil der aktuellen MAGMA-Entwicklung in ihr stattfindet. Vom Design her ist MAGMA ähnlich wie Gap oder Maple: Um einen in C geschriebenen Kernel herum gibt es Module, die in MAGMA selber geschrieben werden. Die Geschwindigkeit von MAGMA erklärt sich durch die etwas Kernel-lastige Gewichtung: die meisten Algorithmen sind in C implementiert, die neueren Gebiete werden im Wesentlichen in MAGMA erschlossen, wobei Module, die als zeitkritisch erkannt werden, in den Kern übernommen werden.

MAGMA ist leider nicht frei und die Sourcen (des C-Kernels) sind nicht erhältlich. MAGMA ist jedoch auch nicht kommerziell, die Einnahmen aus den Lizenzen decken lediglich einen Teil des technischen Supports ab. Dadurch erklärt sich auch das etwas spartanische User-Interface: Textmodus, keine Farben, keine Grafik, aber funktional. Bestandteil von MAGMA sind ca. 3000 Seiten Dokumentation. Sowohl ein Referenz-Handbuch als auch eine Einführung werden mitgeliefert. Die Weiterentwicklung von MAGMA ist in der Hand von John Cannon und seiner Gruppe, die von zahlreichen Besuchern ergänzt werden, so dass neue Algorithmen oft sehr schnell in MAGMA eingebaut werden. In vielen Gebieten werden Teile des Codes von externen Gruppen bereitgestellt. Die Zahlentheorie zum Beispiel ist weitestgehend von Michael Pohst und der Kant-Gruppe in Berlin an der TU entwickelt worden und die reelle Arithmetik basiert auf Henri Cohens Pari, um nur zwei Beispiele zu nennen.

Für viele Anwendungen ist MAGMA zweifelsfrei das beste System: MAGMA enthält zum Beispiel einen der besten Point-Counting-Algorithmen für elliptische Kurven über endlichen Körpern. Zusammen mit dem Geometrie-Modul ist MAGMA damit ein extrem nützliches Werkzeug in der Kryptographie.

Die vorhandenen Datenbanken der besten bekannten Codes über $\mathbb{F}_2$ und $\mathbb{F}_4$ sowie die Unterstützung für lineare Codes über Erweiterungen von $\mathbb{Z}/4\mathbb{Z}$ zeigen MAGMAs Stärke auch in der Codierungstheorie.

In anderen Gebieten (z. B. Gruppentheorie oder Zahlentheorie) ist MAGMA zwar nicht mächtiger als spezialisierte stand-alone Pakete (Pari, Gap), jedoch sind die Anwendungsmöglichkeiten durch die Breite von MAGMA viel größer. Bedingt durch eine einheitliche Sichtweise der verschiedenen Strukturen ist es einfach, Anwendungen zu entwickeln, die in mehreren Bereichen zu Hause sind: So ist es zum Beispiel möglich, Klassenkörpertheorie auf Funktionenkörper anzuwenden, um gute Codes zu finden. MAGMA unterstützt alle hierzu notwendigen Werkzeuge:

- Arithmetik von Funktionenkörpern
- Explizite Klassenkörpertheorie (Bestimmen von definierenden Gleichungen)
- Riemann-Roch-Raum-Berechnung
- Codierungstheorie

Andere Kombinationen, z. B. Gruppentheorie, Invariantentheorie, Zahlkörper und Klassenkörpertheorie in Zahlkörpern zusammen mit der Möglichkeit, Galoisgruppen (mit der Operation der Gruppe auf den Nullstellen) für Zahl- und Funktionenkörper (bis Grad 23 einschließlich) zu berechnen, machen MAGMA zu einem mächtigen Werkzeug in der inversen Galoistheorie.

Die Möglichkeit, zahlentheoretische Blickwinkel mit geometrischen Aspekten zu verbinden, öffnet einen interessanten Zugang zu der Geometrie von Kurven.

Eine Beispielsitzung

Um einen Einblick in MAGMA zu geben, betrachten wir nun ein etwas längeres Beispiel in dem wir mit Hilfe von Klassenkörpertheorie einen Zahlkörper mit einer interessanten Galois Gruppe konstruieren werden.

```
> magma
Magma V2.10-1     Tue Feb  4 2003
11:04:28 on galois
[Seed = 3722240088]
Type ? for help.  Type <Ctrl>-D to quit.
```

Wenn MAGMA gestartet wird, sind zunächst keine Strukturen oder Variablen definiert. Um Zahlkörper zu definieren, benötigen wir Polynome; um ein Polynom eingeben zu können, muss zunächst ein Polynomring erzeugt werden.

```
> Zx<x> := PolynomialRing(Integers());
> K := NumberField(x^3-21*x-7);
> K;
Number Field with defining polynomial
x^3 - 21*x - 7 over the Rational Field
> M := MaximalOrder(K);
```

(Der Körper K ist zyklisch mit Führer 7.) Als nächstes werden wir eine Strahlklassengruppe erzeugen, um eine abelsche Erweiterung zu erhalten.

```
> R, mR := RayClassGroup(7*13*M);
> R;mR;
Abelian Group isomorphic to Z/3 + Z/12
Defined on 2 generators
Relations:
3*r.1 = 0
12*r.2 = 0
Mapping from: GrpAb: R to Set of ideals
of M
```

Der Strahlklassenkörper modulo $7 \cdot 13 \cdot M$ ist normal über $\mathbb{Q}$ vom Grad $3 \cdot 3 \cdot 12$. Im Weiteren wollen wir mit dem 3-Anteil arbeiten:

```
> A := AbelianpExtension(mR, 3);
```

Der 3-Strahlklassenkörper ist nach Konstruktion normal über $\mathbb{Q}$, nun wollen wir seine Automorphismengruppe untersuchen:

```
> IsAbelian(A:All);
false
> G := AutomorphismGroup(A:All);
```

Die Gruppe der $\mathbb{Q}$-Automorphismen ist als endlich erzeugte Gruppe mit Erzeugern und Relationen gegeben. Um die Gruppe analysieren zu können, muss sie zunächst in eine andere Form gebracht werden. Da es sich um eine 3-Gruppe handelt, kann G einfach in eine PC-Gruppe konvertiert werden:

```
> H := pQuotient(G, 3, 3);
> SubgroupLattice(H);

Partially ordered set of subgroup classes
-----------------------------------------

[1] Order 1 Length 1 Maximal Subgroups:
---
[2] Order 3 Length 1 Maximal Subgroups: 1
[3] Order 3 Length 1 Maximal Subgroups: 1
---
[4] Order 9 Length 1 Maximal Subgroups: 2
[5] Order 9 Length 1 Maximal Subgroups: 2 3
[6] Order 9 Length 1 Maximal Subgroups: 2
[7] Order 9 Length 1 Maximal Subgroups: 2
---
[8] Order 27 Length 1 Maximal Subgroups:
                                    4 5 6 7
```

Wie wir sehen, gibt es nicht-normale Untergruppen der Ordnung 3, die zu nicht normalen Körpern vom Grad 9 mit Galoisgruppe G korrespondieren. Um einen dieser Körper zu finden, müssen wir die Teilkörper von A untersuchen. Nach dem Existenzsatz der Klassenkörpertheorie korrespondieren die Teilkörper zu C_3-Quotienten von R:

```
> l := Subgroups(R:Quot := [3]);
```

Klassenkörper in MAGMA werden über die Abbildung von einer endlichen abelschen Gruppe in eine Strahlklassengruppe definiert. Um dies zu tun, müssen die Quotienten zu den Untergruppen in l gebildet werden. Die kanonischen Projektionen zusammen mit der Strahlklassengruppenabbildung mR definieren die Körper:

```
> lA := [ AbelianExtension(Inverse(mq)*mR)
        where _, mq := quo<r|x`subgroup> :
        x in l];
```

Wir sind an nicht-normalen Körpern interessiert:

```
> [ IsNormal(x:All) : x in lA];
[ false, false, false, true ]
```

Um die Galoisgruppe zu berechnen, müssen wir zunächst definierende Gleichungen finden, dies geschieht, indem wir die abelsche Erweiterung *formal* in einen Zahlkörper umwandeln. Dieser ist zunächst über K definiert und wird daher als nächstes in eine einfache Erweiterung von $\mathbb{Q}$ umgewandelt.

```
> F := NumberField(lA[1]);
> F;
Number Field with defining polynomial
$.1^3 + 1/3*(-169*K.1^2 + 5408*K.1
     - 157339)*$.1 + 1/9*(-2466724*K.1^2
     + 5994599*K.1 + 38938445) over K
> Fa := AbsoluteField(F);
> G := GaloisGroup(Fa); G;
Permutation group acting on a set of
cardinality 9
    (1, 4, 7)(2, 8, 5)
    (1, 2, 3, 4, 5, 6, 7, 8, 9)
```

Schließlich wollen wir noch herausfinden, welche Gruppe wir nun konstruiert haben, d. h. wo sie in der Liste der transitiven Gruppen auftritt:

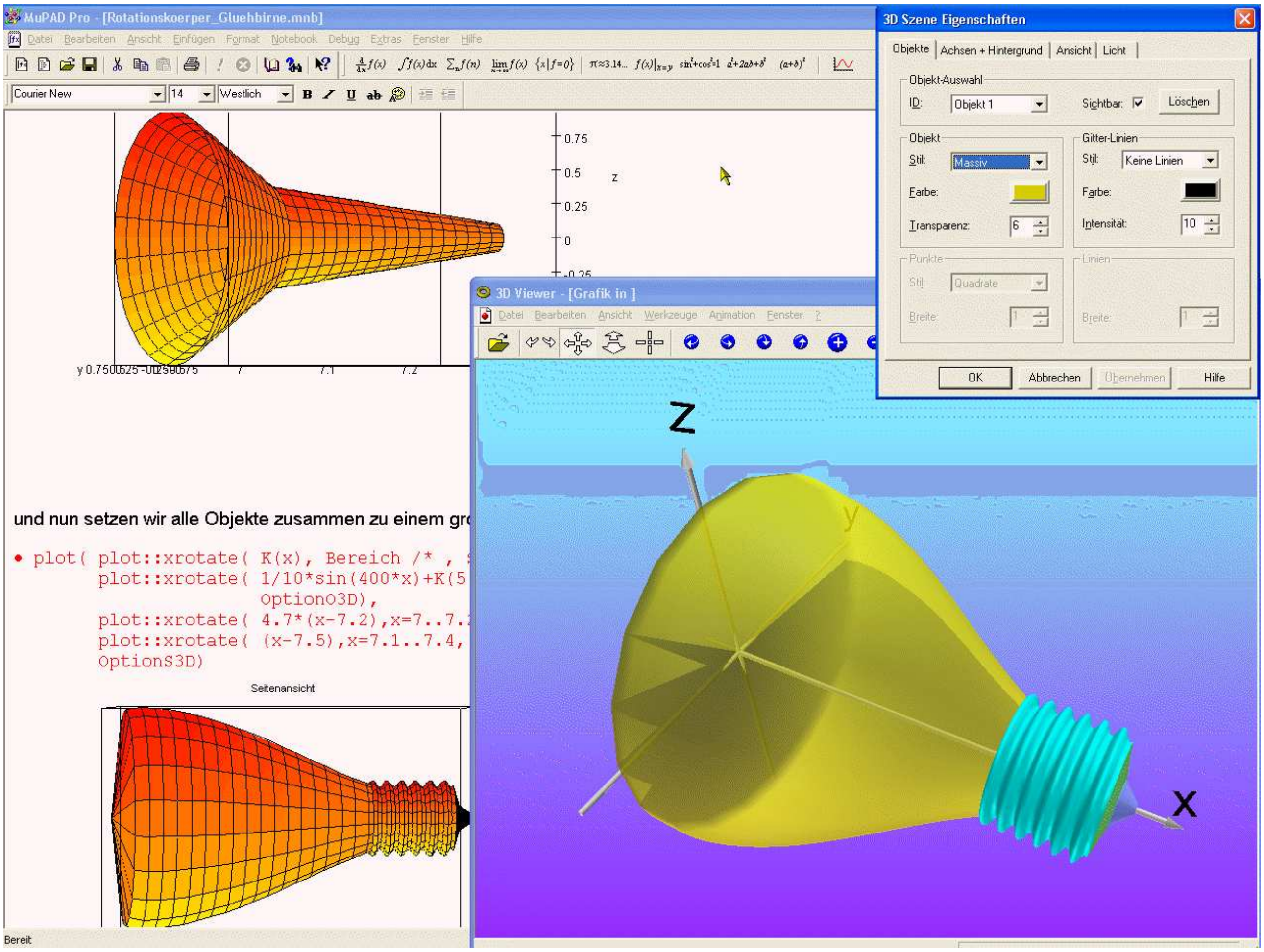
```
> TransitiveGroupIdentification(G);
6 9
> TransitiveGroupDescription(6, 9);
```

Eine detaillierte Untersuchung der Gruppe ist nun einfach. Wenn es gewünscht wird, so ist es ebenfalls möglich, die Operation auf G auf den Nullstellen in einem geeigneten Zerfällungskörper zu erhalten. Dieses Beispiel demonstriert natürlich nicht alle Möglichkeiten, die MAGMA bietet, es soll nur zeigen wie die Sprache die Benutzung der verschiedenen Bereiche ermöglicht.

MuPAD PRO V2.5 - Mathematiksoftware Made in Germany

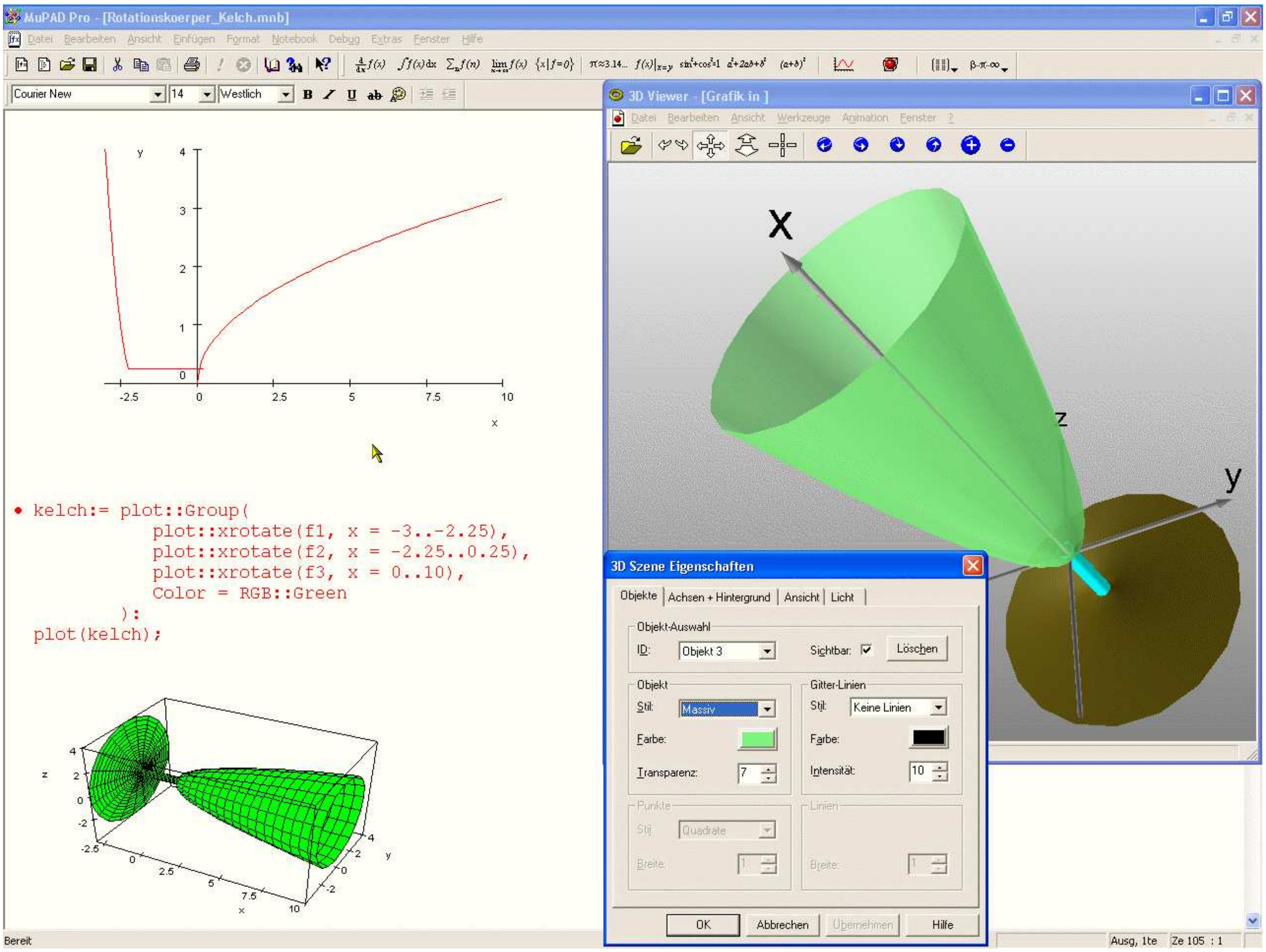
Thomas Beneke, W. W. Schwippert (Zierenberg)

Das geistige Kind von Studenten und Doktoranden des Instituts für Automatisierung und Instrumentelle Mathematik der Universität Paderborn trägt den Namen MuPAD, die sprachliche Kurzform für „Multi Processing Algebra Data Tool“. Dieses offene Computeralgebrasystem kann sich durchaus mit vergleichbaren Produkten aus dem englischsprachigen Raum messen. Darauf beruht wohl auch der Erfolg des Unternehmens SciFace Software GmbH & Co. KG, welches sich ausgehend von dem hochschulinternen Forschungsprojekt inzwischen am Markt etabliert hat und zudem vom Land Nordrhein-Westfalen Unterstützung erfährt. Die Software selbst erlaubt symbolische und numerische Operationen in einer offenen und benutzerfreundlichen Umgebung. Sie vereinigt Funktionen interaktiver Textverarbeitung, Grafikbearbeitung und Programmierung und nutzt dabei die von Windows angebotenen Anwenderhilfen. Zentrale Anlaufstelle des Programms ist das so genannte Notebookfenster mit seinen Ein- und Ausgabebereichen für Berechnungen von Formeln und Erstellung von Textsequenzen. Vergleichbar der Pascal-Syntax erlaubt die in MuPAD eingebettete Programmiersprache befehls- und objektorientierte Anweisungen und Befehlskategorien, so dass sich Programmerweiterungen erzeugen und damit auch zusätzliche externe Anwendungen einbinden lassen.



Eine ausführliche, hypertextgesteuerte Online-Dokumentation erleichtert gerade dem Einsteiger die Einarbeitung in das Programm, und das im Springer-Verlag erschienene MuPAD-Tutorium weist inhaltlich mehr als die oft üblichen Dokumentationen auf, die lediglich aus einem Extrakt der im Programm untergebrachten Hilfetexte bestehen. In dem über 350 Seiten umfassenden Buch bekommt man in einzelnen Kapiteln ausreichend Hinweise und Beispiele zum Umgang mit Bibliotheken, Listen, mathematischen Objekten, Transformationen, Substitutionen, Vereinfachungen, Auswerteverfahren etc. Dabei sollte dieses Buch nicht als Ersatz für mathematisches Hintergrundwissen, sondern als Zusatzhilfe für den Umgang mit dem Programm verstanden werden. Was die MuPAD-Programmiersprache wie auch die Programmiertechniken betrifft, wünscht man sich in diesem Tutorium allerdings mehr Informationen und Beispiele, worauf aber möglicherweise aus Gründen des Umfangs verzichtet worden ist. Wer darüber hinaus noch weitere Erläuterungen und Details benötigt, sollte einen Blick ins Internet riskieren und Seiten wie `ftp.mupad.de/MuPAD/mathpad/`, `www.mupad.de/SUPPORT/LEHRE/` oder `www.mupad.de/schule+studium/literatur` bzw. `.../material` aufsuchen. Bevorzugte Programmanwender wie Naturwissenschaftler und Mathematiker in Produktion, Forschung und Lehre, aber auch Studenten und Schüler, die als Zielgruppe ständig mit mathematischen Werkzeugen arbeiten, werden beim Durchstöbern dieser Internet-Seiten viele Zusatzinformationen finden. Hierzu gehören Unterrichtsmaterialien, Fachpublikationen und -bücher, eine Internetfachzeitschrift, Projektvorschläge für Lehrende und Ausbilder sowie diverse herunterladbare Bibliotheken mit Hinweisen zur Analysis und zur analytischen wie elementaren Geometrie.

Wird MuPAD gestartet, beginnt der Anwender in einer so genannten Sitzung mit der Formulierung der symbolischen und numerischen mathematischen Operationen, zu denen beispielsweise arithmetische Berechnungen mit langen und rationalen Zahlen und zur Zahlentheorie, Operationen zu Mengen und Listen, Funktionen zur Analysis, linearen Algebra, Statistik und Stochastik, Kombinatorik und Numerik oder der Umgang mit symbolischen Ausdrücken gehören. Dazu darf der Nutzer aus einem Pool von mehr als 2.500 Funktionen wählen. Erzielte Ergebnisse lassen sich bei Bedarf als 2D- oder 3D-Diagramme grafisch umsetzen. Die Textverarbeitungsfunktionen erlauben dann die Zusammenstellung von mathematischen Operationen, Texten und grafischen Darstellungen innerhalb ganzer Dokumentationen zwecks Publikation. Als nützlich erweisen sich auch die interaktiven Kooperationsmöglichkeiten mit dem Web und Microsoft-Anwendungen wie beispielsweise PowerPoint, Excel oder Access. Alle Funktionen lassen sich dabei per Knopfdruck starten.



Seit Mai 2002 kann die neue Version 2.5 Pro von MuPAD erworben werden. Ausgestattet mit verbesserten Bedienungsfunktionen in Form zusätzlicher interaktiver Schalter, Buttons und Hilfen sowie erweiterten Grafiktools wendet sich das Programm auch an die Klientel der Lehrenden und Lernenden. Was speziell die verbesserten grafischen Hilfsmittel betrifft, mögen Hinweise auf den 3D-Viewer VCam und auf ein auf OpenGL basierendes grafisches Darstellungswerkzeug reichen. Letzteres garantiert auch hochauflösende 3D-Grafiken und bietet Funktionalitäten hinsichtlich Zoom, Animationsmöglichkeiten, Beleuchtungseffekten und Daten im Grafikraum. Um den Grafiktransfer zu anderen Anwendungen zu erleichtern, sind weitere Austauschmöglichkeiten integriert worden. Dazu gehören neu aufgenommene Dateiformate inklusive Postscript, die Übertragung als OLE-Objekt oder der HTML-Export zur Verbesserung der Web-Tauglichkeit.

Andere Programmbereiche haben ebenfalls dazu gewonnen. So bietet der weiter verbesserte Debugger jetzt z. B. auch so genannte conditional-breakpoints. Ein überarbeiteter Kernel mit zusätzlichen und besseren Algorithmen, ein neues Solver-Konzept und die Integration von mehr als 100 neuen Funktionen in das bestehende Funktionendepot haben das mathematische Potenzial nochmals angehoben. Zu den gut 60 neuen Funktionen aus dem Bereich Statistik gehören u. a. Erweiterungen in Bezug auf Chi-Quadrat-Tests oder die Box-Plot-Analyse. Die Abteilung Kombinatorik verfügt über neu strukturierte Bibliotheken u. a. zu Partitions- und Permutationsfunktionen, zu Young-Tableaus- und Dyck-Worten-Berechnungen. Auch der neue sehr effiziente Datentyp „sparsematrix" für dünn besetzte Matrizen sowie „Dom::Interval" für Gleitpunktintervallarithmetik dürfen an dieser Stelle nicht unerwähnt bleiben. Falls die numerische Rechenkapazität nicht ausreichen sollte, gibt es eine zusätzliche Möglichkeit, das Programm aufzurüsten. Dazu wird das Add-On Scilab installiert und lizensiert. Scilab baut sich im Zuge der Installation in die numerische MuPAD Pro 2.5 Rechenbibliothek ein. Der Vorteil besteht im Berechnen mit Hardware-Gleitpunktzahlen und in der zusätzlichen Integration von sehr schnellen Algorithmen. In der Summe verkürzt sich die Berechnungsdauer bei komplexen mathematischen Operationen. Für manche Anwender könnte auch die Kooperationsmöglichkeit mit dem DUBBEL, gewissermaßen der Bibel für die Maschinenbauer, von Interesse sein, da dieses Werkzeug inzwischen auf den MuPAD-Kernel direkt zugreift. Erwähnt werden sollte noch der MuPAD Computing Server (MCS), mit dem MuPAD per Internet als E-Learning-Medium nutzbar wird. Für potenzielle Anwender empfiehlt es sich also, einmal die 30-Tage-Demo-Vollversion aus dem Internet zu laden, um einen persönlichen Eindruck zu erhalten, insbesondere da das Programm nicht nur eine preisliche Alternative zu Konkurrenzprodukten darstellt. MuPAD Pro 2.5 existiert für verschiedene Betriebssysteme wie Windows 95/98/ME/2000/XP und NT4.0, Linux 2.x, Sun Solaris 5.9 und MacOSX. Sind mehr als 40 MB auf der Festplatte und 64 MB im RAM vorhanden, kann das Programm installiert und genutzt werden. Je nach Anwender und Bestellmengen sind die Lizenzen preislich gestaffelt und liegen etwa zwischen 135,- für Studenten und etwa 725,- für einen Einzelplatz in der Industrie. Mengenrabatte werden ab 5 Lizenzen und mehr nach Rücksprache gegeben.

Für weitere Nachfragen steht das Team des deutschen Vertreibers ADDITIVE GmbH, Rohrwiesenstr. 2, D-61381 Friedrichsdorf zur Verfügung (Tel: +49 (0)6172 5905-30 [Zentrale: -0], Fax: +49 (0)6172 77613, e-mail: `mupad@additive-net.de`, Internet: `http://www.mupad.de`).

Computeralgebra in der Schule

In Hannover haben sich Vertreter der Universität, der Bezirksregierung und der Gymnasien an einen runden Tisch gesetzt, um das Problem der Schnittstelle Mathematik zwischen Schule und Universität zu diskutieren. Hierbei war ein auslösendes Moment die Überzeugung, dass grafikfähige Taschenrechner und Taschenrechner mit integriertem Computeralgebrasystem in zunehmendem Maß den Unterricht in der Schule prägen. Nach langen Diskussionen ist eine Beschreibung der Schnittstelle entstanden, die die Voraussetzungen im Fach Mathematik für den Übergang von Schule auf Hochschule beschreibt. Diese Schnittstellenvereinbarung soll im nächsten Computeralgebrarundbrief in wesentlichen Teilen veröffentlicht werden.

In diesem Heft widmet sich Herr Werner Burkhardt (Mannheim) in seinem Beitrag „Wie viel CAS braucht der Mensch?" noch einmal grundsätzlich dem Thema Computeralgebra im Mathematikunterricht und fokussiert das Thema auf die Gleichungslösekompetenz unter dem Aspekt der Heymannschen Thesen zum Beitrag der Mathematik zur Allgemeinbildung. Diesem wichtigen Thema wird in den neuen Rahmenrichtlinien Mathematik Klasse 7-10 (Niedersachsen), die sich z. Zt. in der Anhörung befinden, ein eigenes Kapitel gewidmet. Dort wird gefordert, dass Schülerinnen und Schüler neben rein algebraischen Verfahren auch gleichwertig numerische und grafische Verfahren zur Lösung von Gleichungen lernen. Dies soll neben der Erweiterung der zu bearbeitenden Problemklasse auch dazu beitragen, die in Rechnern implementierten Gleichungslöser in Grundzügen zu verstehen und ihre Ergebnisse kritisch zu würdigen. *(Heiko Knechtel)*

Wie viel CAS braucht der Mensch?

Werner Burkhardt (Mannheim)

In dem Artikel „Welche handwerklichen Rechenkompetenzen sind im CAS-Zeitalter unverzichtbar?" [1] versuchen die Autoren, Eckpunkte für grundlegende Rechentechniken, die von Schülern erwartet werden müssen, zu fixieren. Die teilweise heftigen Reaktionen auf diesen Artikel zeigen, wie brisant die dort vertretenen Thesen sind. Betrachtet man die derzeit vertretenen Argumente zum CAS-Einsatz an Schulen, ist von der euphorischen – und bisweilen kritiklosen – Befürwortung bis hin zur völligen Ablehnung alles zu finden.

Die Diskussion all dieser Argumente findet häufig unter Mathematikern und unter denen, die intensiv Mathematik anwenden müssen, statt. Nur werden an unseren Schulen nicht nur Mathematiker und Natur- und Ingenieurwissenschaftler ausgebildet, sondern auch Philologen, Theologen, Juristen etc.. Daher muss Mathematikunterricht an Schulen allgemeinbildende Aspekte berücksichtigen. In [2] nennt Heymann Ideen, die allgemeinbildender Mathematikunterricht berücksichtigen sollte.

Die Heymannschen Ideen sind sicherlich nicht unumstritten. Die Unterrichtsziele Lebensvorbereitung und Denkerziehung sind für den Mathematikunterricht anerkannt. Wie diese Ziele im realen Mathematikunterricht – und nicht in der in manchen Fällen utopischen methodisch didaktischen Diskussion – berücksichtigt werden können, möchte ich am Beispiel des Lösens von Gleichungen näher beleuchten.

Befragt man Oberstufenschüler oder Abiturienten, was denn die Lösung einer Gleichung sei, erhält man häufig fragmentarische Ausführungen zu Gleichungsumformungen, aber selten den Satz „Die Lösung einer Gleichung ist der Wert, der beim Einsetzen in die Gleichung eine wahre Aussage liefert". Diese jungen Menschen wurden sicherlich gemäß der aktuellen Lehr-/Bildungspläne unterrichtet; entsprechen die Äußerungen der Schüler aber den angestrebten Zielen dieser Pläne?

Betrachtet man die Lehr-/Bildungspläne der Schulen, die zum Abitur führen, findet man überall Verfahren zum exakten Lösen quadratischer Gleichungen, zum Auffinden der Nullstellen von Polynomen und u. U. zu Näherungsverfahren. Wie werden diese Inhalte unterrichtlich umgesetzt und was bleibt nachhaltig bei den Schülern haften? Ein Blick in die aktuellen Schulbücher zeigt, dass zum Lösen gleichartiger Gleichungen eine Vielzahl von Übungen angeboten wird. Diese Übungen trainieren fast immer das gleiche Verfahren an Beispielen unterschiedlicher Schwierigkeit. Was dabei haften bleibt, wurde bereits geschildert. Untersuchungen zeigen, dass gerade heute Schüler viele gleichartige Übungen als monoton und ohne Realitätsbezug empfinden.

Auf dieses Schülerverhalten kann mit realitätsbezogenen Aufgaben reagiert werden, wobei die Schüler sich ihre Lösungsverfahren teilweise selbst erarbeiten müssen. Der Strategievorrat zum Lösen von Gleichungen muss im Laufe der Zeit wachsen und sollte u. a. folgende Punkte enthalten:

- Lösen mit Äquivalenzumformungen
- Lösen mit Umkehrfunktion
- Zeichnerische Lösung
- Problemreduktion durch Substitution
- Beachtung von Symmetrie und Periodizität
- Raten und Prüfen
- Problemreduktion durch Faktorisierung
- Lösungsformeln

Der Aufbau eines solchen Katalogs von Lösungsmöglichkeiten – an alltäglichen Beispielen orientiert – unterstützt sicherlich die Unterrichtsziele Lebensvorbereitung und Denkerziehung. Fordert man die Aufnahme dieses oder eines erweiterten Katalogs in Lehr-/Bildungspläne, wird sofort die Frage gestellt, ob hierfür andere Inhalte gestrichen werden oder mehr Unterrichtszeit zur Verfügung steht. Mit mehr Unterrichtszeit – gleichgültig für welches Fach – ist bei der derzeitigen Lage der öffentlichen Haushalte nicht zu rechnen. Streichen von Inhalten ist mehr als problematisch, wenn man den allgemeinbildenden Charakter des Faches Mathematik erhalten möchte.

Welche Aufgabe kann CAS in dieser Situation übernehmen? Für den schwächeren oder wenig an Mathematik interessierten Schüler könnte CAS ein Hilfsmittel sein, um Standardgleichungen sicher und fehlerfrei zu lösen. Hier stellt sich natürlich die Frage nach dem Bildungswert eines derartigen Vorgehens. Provokativ könnte man antworten, dass das fehlerfreie Lösen von Gleichungen mit CAS für den Anwender nach der Schule immer noch besser sei, als das Hantieren mit einem unsicheren Regelwerk.

Das Vorgehen bietet auch eine Chance für den Mathematikunterricht. Durch das sichere Lösen von Gleichungen mit CAS wird die Unterrichtszeit, die zum ausführlichen Üben von Standardverfahren eingesetzt wurde, frei. Diese Zeit kann für die Festigung und Wiederholung des Gleichungsbegriffs so eingesetzt werden, dass Schulabgänger sicherer mit Gleichungen in alltäglichen Situationen umgehen können als heute.

Ferner können durch den Einsatz von CAS schwierigere Gleichungen unterrichtlich behandelt werden. CAS liefert z. B. bei transzendenten Gleichungen häufig nur einen Teil der gesuchten Lösungen. Durch Symmetrie-und Periodizitätsbetrachtungen können weitere Lösungen erschlossen werden. Durch solche Überlegungen können dann auch leistungsfähigere Schüler gefordert und gefördert werden.

Nun zu der Frage: Wieviel CAS braucht der Mensch? Ich glaube, dass diese Frage einfacher zu beantworten ist als die Frage aus [1]. Betrachtet man den fiktiven Menschen, der nur Gleichungen lösen möchte, genügt diesem ein CAS mit einem ordentlichen Befehl zum Lösen von Gleichungen, wie dies der Befehl *solve* der meisten Systeme leistet. Ein Ingenieur braucht sicherlich ein CAS, das integriert, differenziert und Differentialgleichungen löst. Mathematiker, die mathematische Sätze automatisch beweisen wollen, benötigen spezielle Systeme wie z. B. Theorema. Zusammenfassend kann man sagen, die Frage wieviel CAS ein Mensch braucht, lässt sich nur beantworten, wenn man weiß, in welchem Umfeld CAS eingesetzt werden soll.

Für Schüler würde ich ein vor allem leicht bedienbares CAS bevorzugen, das Befehle zum Lösen von Gleichungen und Gleichungssystemen, zum Zeichnen, zum Integrieren und Differenzieren und u. U. zum Lösen von Differentialgleichungen bereitstellt. Dies und viel mehr leisten die am häufigsten verbreiteten Systeme wie z. B. Derive, Maple, Mathematica und MuPAD. Daher wird die Auswahl für den unterrichtlichen Einsatz von Kriterien wie Bedienbarkeit, Handhabung und Preis bestimmt.

CAS kann den Mathematikunterricht nicht verkürzen oder gar ersetzen, wie sich das manche Bildungspolitiker vielleicht wünschen. Seit TIMSS und PISA gibt es neue Forderungen an einen zeitgemäßen Mathematikunterricht in Deutschland. CAS kann bei der Realisierung dieser Forderungen im alltäglichen Mathematikunterricht seinen Beitrag leisten, aber niemals einen guten Mathematiklehrer ersetzen.

Literatur

[1] W. Herget, H. Heugl, B. Kutzler, E. Lehmann, *Welche handwerklichen Rechenkompetenzen sind im CAS-Zeitalter unverzichtbar?*, Computeralgebra Rundbrief Nr. 27, 2000.

[2] H.W. Heymann, *Allgemeinbildung und Mathematik*, Weinheim: Beltz, 1996.

Computeralgebra in der Lehre

Algebraisches Praktikum

Frank Lübeck (Aachen)

Ich möchte hier über eine Veranstaltung berichten, die wir in jedem Sommersemester am Lehrstuhl D für Mathematik, RWTH Aachen, anbieten. (Ich betreue diese regelmäßig und habe viele der Aufgaben entworfen.)

Die Veranstaltung heißt *Algebraisches Praktikum* und richtet sich an Studierende, die mindestens die Vorlesung *Algebra I* schon gehört haben. Grundkenntnisse eines Computeralgebra-Systems sind nicht vorausgesetzt, aber sehr nützlich. Die meisten Teilnehmerinnen und Teilnehmer sind im vierten bis sechsten Semester und haben neben der Algebra-Vorlesung einen Einführungskurs in Maple (`http://www.maplesoft.com`) besucht.

Ein Ziel des Praktikums ist es, Kenntnisse aus der Algebra-Vorlesung unter praktisch-rechnerischen Aspekten zu verfestigen. Die Intuition für abstrakte algebraische Strukturen und Konzepte soll durch die Realisierung in konkreten Datenstrukturen verbessert werden. Weiter sollen die Studierenden einige grundlegende Algorithmen aus der Computeralgebra kennen lernen. Und schließlich soll die Beschäftigung mit den Aufgaben zur Einarbeitung ins Programmieren mit einem Computeralgebra-System führen.

Den Studierenden ist freigestellt, welches System sie benutzen möchten. Die meisten Aufgaben lassen sich mit jedem der verbreiteten Computeralgebra-Systeme vernünftig lösen. Wir schlagen die Verwendung von Maple oder GAP (`http://www.gap-system.org`) vor, da diese auf vielen Hochschulrechnern und privaten Rechnern zur Verfügung stehen oder leicht zu installieren sind.

Ablauf Am Anfang des Semesters bekommen die Studierenden eine Sammlung von etwa 15 Aufgaben. Dieses sind jeweils Mini-Projekte, zu deren Lösung einige Programme zu schreiben und in vernünftiger Weise kommentiert abzugeben sind. Ein Aufgabenteil ist jeweils eine kleine Anwendung des zu schreibenden Hauptprogramms. Für einen Schein, der die erfolgreiche Teilnahme bestätigt, sind mindestens 5 der Aufgaben teilweise zu bearbeiten und eine gewisse Mindestanzahl an Punkten zu erreichen. Hierbei ist es erlaubt und sogar empfohlen, die Aufgaben in Zweiergruppen zu bearbeiten.

Während des Semesters gibt es eine Doppelstunde pro Woche, während der in einem Rechnerraum Fragen gestellt werden können. Üblicherweise sind die Fragen zu Beginn des Semesters eher technischer Natur, zum Beispiel zu: Aufruf von Programmen, Editieren von Dateien, Grundbefehlen in Maple, Benutzung der eingebauten Hilfe der Programme. Später gibt es mehr Fragen zum mathematischen Hintergrund der Aufgaben, zu weitergehenden technischen Fragen und zur Fehlersuche in Lösungsansätzen. Auch außerhalb dieser Fragestunde versuchen wir bei der Lösung von Problemen behilflich zu sein.

Zu den Aufgaben Die Aufgaben sind unterschiedlich schwierig und aufwändig. Es gibt etwa Aufgaben zur Berechnung größter gemeinsamer Teiler (Euklidischer Algorithmus für $\mathbb{Z}$ und Polynomringe und heuristischer ggT in $\mathbb{Q}[X]$), zur Polynom-Interpolation, zum Chinesischen Restsatz oder zu Pseudoprimzahlen, die zum Einstieg ins Programmieren gedacht sind.

Dann gibt es Aufgaben, die eher abstrakte Themen der Algebra-Vorlesung aufgreifen: Implementierung algebraischer Körpererweiterungen oder endlicher Körper, die Untersuchung von Galoisgruppen von Polynomen.

Andere Aufgaben behandeln kombinatorische Algorithmen: Auflisten und Abzählen von Partitionen, n-Damen-Problem, Aufzählen von Graphen, Bahnen und Stabilisatorkette in Permutationsgruppen. Diese Aufgaben enthalten auch eine Wettbewerbskomponente (Wie große Beispiele können Sie mit Ihrem Programm behandeln?). Es zeigt sich, dass viele im Prinzip korrekte Lösungen nicht sehr effizient sind, dann werden Verbesserungen diskutiert.

Als weitere Gruppe gibt es schließlich Aufgaben, die zu etwas längeren Programmen führen, deren Algorithmen aber recht detailliert erklärt werden: Smith- und Hermite-Normalform von Matrizen, symmetrische Polynome und verschiedene Algorithmen zur Faktorisierung von Polynomen (quadratfreie Faktorisierung, Kronecker-Verfahren und Berlekamp-Algorithmus).

Bei den meisten Aufgaben gibt es keine Hinweise zu technischen Details möglicher Lösungen. Wichtiger Teil der Lösungen ist es, geeignete Datenstrukturen für die zu behandelnden Objekte zu finden. Die Aufgaben sind für die meisten Studierenden recht anspruchsvoll und deren Bearbeitung ist aufwändig.

Erfahrungen Zu Beginn der Veranstaltung melden sich meist etwa 20 interessierte Studierende. Viele davon haben aber nur geringe Vorkenntnisse im Programmieren und stellen nach einiger Zeit fest, dass ihnen die Einarbeitung zu zeitaufwändig ist. Am Ende der Veranstaltung haben bisher zwischen 4 und 9 Studierende einen Schein für die erfolgreiche Teilnahme bekommen.

Die meisten Lösungen werden in Form von xmaple-Worksheets eingereicht, da viele xmaple schon aus einer Einführungsveranstaltung kennen. Die wenigen Teilnehmer, die sich auch GAP angesehen haben, geben meist alle Lösungen als GAP-Programme ab.

Leider fördert die Veranstaltung nicht regelmäßig gute Talente für die Computeralgebra-Programmierung zu Tage. Eine Teilnehmerin hat aber mittlerweile ihr Diplom an unserem Lehrstuhl erhalten mit einer Arbeit mit Programmieranteil. Und einmal konnten wir einen Teilnehmer mit hervorragenden GAP-Lösungen hinterher als Wissenschaftliche Hilfskraft für Programmieraufgaben gewinnen.

Mehr Informationen Die Aufgaben für das Sommersemester 2003 können Sie auf der Webseite `http://www.math.rwth-aachen.de/~Frank.Luebeck/AlgPrakSS03` finden. Die Aufgaben sind „Open Source“, sie dürfen als Anregung für Aufgaben anderer Veranstaltungen benutzt werden. Umgekehrt würde ich mich über Anmerkungen und Tipps für weitere Aufgaben freuen.

Konkrete Aufgabe Als Beispiel sei hier die oben erwähnte Aufgabe zu algebraischen Körpererweiterungen wiedergegeben.

Hintergrund: Algebraische Körpererweiterungen lassen sich etwa durch Restklassenringe von Polynomringen realisieren. Informationen hierzu finden Sie in jedem Textbuch zur Algebra.

Hauptaufgabe: Sei K ein Körper, in dem wir bereits Elemente hinschreiben und mit diesen rechnen können, Sie dürfen der Einfachheit halber etwa $K = \mathbb{Q}$ annehmen. Sei $f(X)$ ein nicht-konstantes Polynom über K und $(f(X))$ das davon erzeugte Ideal im Polynomring $K[X]$.

(a) Überlegen Sie sich, wie Sie mit dem Computer Elemente im Restklassenring $R = K[X]/(f(X))$ darstellen können.

(b) Programmieren Sie eine Arithmetik zum Rechnen in R. Diese sollte Addition, Subtraktion, Multiplikation und den Test auf Gleichheit für je zwei Elemente aus R einschließen. (Das Polynom f können Sie entweder jeder Operation als Argument mitgeben, oder sie speichern es in der Datenstruktur für die Elemente aus dem Restklassenring.)

(c) Welche Elemente aus R haben ein Inverses bezüglich der Multiplikation? Schreiben Sie ein Programm, das von einem Element feststellt, ob es invertierbar ist, und gegebenenfalls das Inverse berechnet. Unter welcher Bedingung an f ist R ein Körper?

(d) Sei R ein Körper. Wie bestimmen Sie für ein beliebiges Element $x \in R$ sein Minimalpolynom über K?

Anwendungen: (a) Sei ζ_5 eine primitive 5-te Einheitswurzel über $\mathbb{Q}$. Wie können Sie mit Ihrem Programm im Körper $L := \mathbb{Q}(\zeta_5)$ rechnen?

(b) Der Körper L enthält die Quadratwurzeln $\pm\sqrt{5}$. Wie schreiben Sie in Ihrem Programm die Elemente ζ_5 und $\pm\sqrt{5}$, und können Sie entscheiden, welches Element $+\sqrt{5}$ ist?

(c) Wie lautet das Minimalpolynom von $\zeta_5+\zeta_5^4$ über $\mathbb{Q}$?

(d) Sei $L(i)$ eine minimale Körpererweiterung von L, in der das Polynom $X^2+1 \in \mathbb{Q}[X]$ eine Nullstelle hat. Bestimmen Sie ein primitives Element der Erweiterung $L(i)/\mathbb{Q}$ und sein Minimalpolynom über $\mathbb{Q}$.

Hinweise: Wenn Sie die Programmierung in Maple ausführen möchten, könnten folgende Hilfeseiten nützlich sein: `polynomials`, `array`, `list`.

Entsprechende Informationen in GAP-4 sind unter `lists` und `polynomials and rational functions` zu finden.

Wenn Sie eine vorhandene Polynomarithmetik verwenden, dürfen Sie auch die darin vorhandenen Funktionen für größte gemeinsame Teiler und Division mit Rest benutzen.

Berichte über Arbeitsgruppen

Lehrstuhl „Algorithmische Algebra“ an der TU München

Gregor Kemper (München)

Am Zentrum Mathematik der Technischen Universität München wurde zum Wintersemester 2002/03 ein neuer Lehrstuhl „Algorithmische Algebra“ eingerichtet. Dies ist in erster Linie ein Algebra-Lehrstuhl, der die Algebra auf möglichst großer Breite vertreten will. Zugleich hat der Lehrstuhl aber eine spezielle algorithmische und computerorientierte Ausrichtung. Die Arbeitsgruppe befindet sich derzeit im Aufbau und hofft, bald Diplomanden und Doktoranden gewinnen zu können.

Mitglieder der Arbeitsgruppe: Prof. Dr. W. Heise, Dr. F. Himstedt, Priv.-Doz. Dr. T. Honold, Akad. Dir. Dr. M. Kaplan, Dr. C. Karpfinger, Prof. Dr. G. Kemper (Lehrstuhlinhaber), Prof. Dr. H. Wähling.

Arbeitsgebiete: Die vertretenen Forschungsrichtungen sind:

Codierungstheorie (Heise, Honold, Kaplan): quadratische Restcodes, Decodierung für Codes mit hochtransitiver Automorphismengruppe, Fortsetzbarkeit von Isometrien.

Computeralgebra (Kaplan, Kemper): schnelle Polynomarithmetik (Programm-Projekt „Spock“), algorithmische kommutative Algebra.

Darstellungstheorie (Himstedt, Kemper): Berechnung von Zerlegungsmatrizen, Darstellungen endlicher Gruppen vom Lie-Typ, symmetrische Potenzen.

Invariantentheorie (Kemper): Algorithmische Invariantentheorie, modulare Invariantentheorie, Anwendungen der Invariantentheorie (z. B. in der Bildverarbeitung).

Fastkörper, mehrfach transitive Gruppen (Karpfinger, Wähling): Automorphismen endlicher Fastkörper, bewertete Fastkörper.

Homepage: `http://www-m11.mathematik.tu-muench`

Literatur:

- H. Derksen, G. Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin 2002.
- W. Heise, P. Quattrocchi, *Informations- und Codierungstheorie*, Springer-Verlag, Berlin 1995.
- H. Wähling, *Theorie der Fastkörper*, Thales Verlag, Essen 1987.

- Brylinski, R.K., Chen, G., *Mathematics of Quantum Computation*, Chapman & Hall/CRC, London, Boca Raton, 2002, 448 Seiten, ISBN 1-58488-282-4, $ 89,95.
- Enss, R., Hrsg., *Computer Algebra Recipes for Classical Mechanics*, Birkhäuser Verlag, Basel, Boston, 2002, 264 Seiten, ISBN 0-8176-4291-9, € 75,-. *
- Garvan, F., *The Maple Book*, Chapman & Hall/CRC, London, Boca Raton, 2002, 496 Seiten, ISBN 1-5848-8232-8, $ 49,95.
- Gaál, I., Hrsg., *Diophantine Equations and Power Integral Bases*, Birkhäuser Verlag, Basel, Boston, 2002, 184 Seiten, ISBN 0-8176-4271-4, € 59,-. *
- Grabmeier, J., Kaltofen, E., Weispfenning, V., *Computer Algebra Handbook*, Springer Verlag, Berlin, Heidelberg, New York, 2003, 638 Seiten, ISBN 3-540-65466-6, € 74,85. (Besprechung dieses Buches auf Seite 29 in diesem Rundbrief.)
- Grätzer, G., *General Lattice Theory*, Birkhäuser Verlag, Basel, Boston, 2002, 662+xix Seiten, ISBN 3-7643-6996-5, € 78,-. *
- Stojanovic, S., Hrsg., *Computational Financial Mathematics using MATHEMATICA*, Birkhäuser Verlag, Basel, Boston, 2002, 320 Seiten, ISBN 0-8176-4197-1, € 88,-. *
- Szabo, F., *Linear Algebra: An Introduction Using Maple*, Academic Press, , 2002, 768 Seiten, ISBN 0-12-680144-4, € 92,69.
- Wright, F., *Computing with Maple*, Chapman & Hall/CRC, London, Boca Raton, 2001, 552 Seiten, ISBN 1-5848-8236-0, $ 64,95.

* Diese Bücher können auf der Seite `http://www.fachgruppe-computeralgebra.de/Buecher/` zur Besprechung angefordert werden.

J. H. Davis
Differential Equations with Maple – An interactive Approach

Birkhäuser Verlag, Basel, Boston, 2001, ISBN 0-8176-4181-5, 250 Seiten, € 90,-.

Das Buch ist gedacht als eine erste Einführung in die Theorie gewöhnlicher Differentialgleichungen mit starker Betonung konkreter Rechnungen mit MAPLE. Kenntnisse in MAPLE werden nicht vorausgesetzt; im Gegenteil: stellenweise liest sich das Buch mehr als „Maple with Differential Equations“. Es besteht im Wesentlichen aus zwei Teilen, *Differential Equations* und *Maple Application Topics*, die durch zahlreiche Querverweise miteinander verzahnt sind. Der erste Teil enthält die Theorie; der zweite Teil diskutiert einige längere MAPLE-Rechnungen bis hin zu kompletten Anwendungspaketen.

Der Text wendet sich eher an Naturwissenschaftlicher und Ingenieure als an Mathematiker. Das sieht man schon daran, dass der Existenztheorie ganze zwei Seiten gewidmet sind, während die Impedanzanalyse von Schaltkreisen ein eigenes Kapitel erhalten hat. Nichtlineare Gleichungen werden kaum behandelt; wichtigstes Hilfsmittel ist die Laplace-Transformation. Wie bei den meisten amerikanischen Lehrbüchern liegt das Niveau deutlich unter dem entsprechender deutscher Vorlesungen; so sind praktisch keine Beweise zu finden. Zum Vergleich: Das bekannte Lehrbuch von Walter enthält weit mehr Stoff (insbesondere zur nichtlinearen Theorie) und geht viel tiefer. Dafür diskutiert Davis auch kurz die numerische Integration mit Runge-Kutta-Methoden.

Da ich relativ wenig Erfahrung mit der Programmierung von MAPLE habe, will ich keine Aussagen über die Qualität der angegebenen Programme wagen. Wiederholte Kommentare der Form *“It goes without saying that many of these [Maple hacks] emerged by interactive experimentation after a first code pass went down in flames”* (S. 358) erwecken aber gewisse Zweifel. Das MAPLE-Programmieren wird im wesentlichen als die Suche nach trickreichen „Hacks“ dargestellt. Ich halte auch wenig vom Abdruck zwanzigseitiger Listings, vor allem, wenn dem Buch eine CD beiliegt.

Etwas verblüfft haben mich die beiden größten MAPLE-Projekte. Bei dem ersten geht es um die Aufstellung der Ordnungsbedingungen für Runge-Kutta-Methoden. Dieses Thema ist nicht nur für die meisten Anwender von geringem Interesse (eine ausführlichere Diskussion der Methoden wäre sicherlich nützlicher gewesen), Davis benutzt auch noch den veralteten und ineffizienten „brute force“ Ansatz über Taylor-Reihen statt der Butcher-Theorie, was das Paket schnell unbrauchbar macht. Bei dem zweiten Projekt geht es um den Entwurf eines einfachen Pakets zur Kontrolltheorie. Das ist sicherlich ein interessantes Thema, nur wird es leider nirgendwo im Buch behandelt, so dass der/die Leser/in über keinerlei Grundlagen verfügt und überhaupt nicht weiß, was er/sie mit dem Paket machen soll.

Jemand, dem eine kurze Einführung in die wichtigsten Kochrezepte zum Arbeiten mit gewöhnlichen Differentialgleichungen und MAPLE reicht, ist mit dem Buch nicht schlecht bedient. Es ist in einem flüssigen, freundlichen Stil geschrieben und eignet sich auch gut zum Selbststudium. Wer tiefer gehen will, wird sich aber schnell einen anderen Text suchen.

Werner M. Seiler (Heidelberg)

R. H. Enns, G. C. McGuire
Nonlinear Physics with Mathematica for Scientists and Engineers

Birkhäuser Verlag, Basel, Boston, 2001, ISBN 0-8176-4223-4, 704 Seiten, € 120,-.

Bei dem Buch handelt es sich um die *Mathematica*-Version einer früheren MAPLE-Ausgabe. Auch wenn die Autoren betonen, dass sie nicht nur die MAPLE-durch *Mathematica*-Programme ersetzt hätten, fanden sich bei meinen Stichproben nur minimale Änderungen. Der wichtigste Unterschied scheint zu sein, dass bei der

MAPLE-Version der zweite Teil des Buchs (siehe unten) als eigenständiges *Laboratory Manual* verkauft wurde, während es jetzt nur noch ein Buch mit über 700 Seiten Umfang gibt.

Laut Klappentext wurde die MAPLE-Ausgabe in einer Reihe von Besprechungen sehr positiv beurteilt. Bei mir hat das Buch eher gemischte Gefühle hervorgerufen, was aber auch daran liegen mag, dass ich mittlerweile mehr Mathematiker als Physiker bin. Denn die Zielgruppe sind (wie schon aus dem Titel klar hervorgeht) eher Naturwissenschaftler und Ingenieure als Mathematiker. Dies wird schon dadurch deutlich, dass in dem zweiten Teil des Buchs unter der Überschrift *Experimental Activities* auf über 150 Seiten reale Experimente zur nichtlinearen Physik vorgeschlagen werden. Bei den meisten geht es darum, konkrete physikalische Systeme zu bauen, die durch die im ersten Teil diskutieren Gleichungen beschrieben werden können. Für Leser mit entsprechenden Experimentiermöglichkeiten eine sehr interessante Ergänzung.

Die Stärke des Buchs ist eindeutig seine Breite. Ein/e Student/in, der/die es ganz durcharbeitet, hat praktisch alle klassischen Beispiele nichtlinearen Verhaltens gesehen. Zumindest gilt dies im Bereich endlichdimensionaler Systeme, auf dem der Schwerpunkt des Textes liegt; bei partiellen Differentialgleichungen sieht es aus verständlichen Gründen etwas anders aus. Leider kommen wir damit auch sofort zur größten Schwäche des Buchs: Es geht nicht über das Zeigen der Beispiele hinaus. Irgendwie erinnert es an einen Reiseführer. Man findet zwar eine lange Liste mit Sehenswürdigkeiten; über deren Hintergründe lernt man aber wenig bis nichts.

Als ein konkretes Beispiel sei erwähnt, dass der Begriff eines Eigenwerts erst auf Seite 494 auftaucht und zwar in einem Kapitel über die inverse Streumethode, das (wie auch im Vorwort erwähnt) mathematisch deutlich anspruchsvoller ist als der Rest des Buchs. Die gesamte Diskussion von singulären Punkten erfolgt ohne diesen Begriff! Die verschiedenen Typen werden ausschließlich anhand von Phasendiagrammen vorgeführt. Lediglich für den Fall zweidimensionaler Systeme wird ein klein wenig gerechnet. Dabei wird sogar der *Mathematica*-Befehl `Eigenvalues` benutzt, ohne auf die Bedeutung des Namens hinzuweisen.

Natürlich darf man die Zielgruppe nicht vergessen: amerikanische Undergraduates mit Schwerpunkten in Fächern wie Physik, Chemie, Biologie oder einer Ingenieurswissenschaft. Trotzdem wird man oft den Eindruck nicht los, dass hier Masse wichtiger war als Klasse. Ein paar Beispiele weniger, diese dafür ausführlicher diskutiert, wäre vielleicht mehr gewesen.

Ärgerlich sind auch eine Vielzahl kleinerer Punkte, wobei ich mich nur auf einige besonders typische Beispiele beschränken will. In dem Buch werden eine ganze Reihe von Lotka-Volterra-Systeme behandelt. Weder wird darauf hingewiesen, dass all diese Systeme in eine gemeinsame Klasse gehören und in vielerlei Hinsicht gemeinsam behandelt werden können, noch taucht der Begriff im Index auf. Das SIR-Modell für Epidemien wird zweimal behandelt (Problem 2-30 bzw. 4-41), ohne dass es einen Querverweis gibt.

In den Problemen 5-5 und 5-6 wird unter unterschiedlichem Namen zweimal dasselbe Beispiel (lineare Verfolgung) diskutiert. Anstatt darauf hinzuweisen, wird durch eine unterschiedliche Wahl des Ursprungs und durch ein Wurzelziehen in der zugehörigen Differentialgleichung der Eindruck erweckt, dass es sich um zwei ganz verschiedene Aufgaben handelt.

Das Literaturverzeichnis wurde relativ schlampig zusammengestellt. Bei einigen Artikeln fehlen die Titel ganz, was man als ein Indiz dafür sehen könnte, dass eine Referenz einfach abgeschrieben wurde, ohne jemals die zugehörige Arbeit zu lesen. Die Schreibweise deutscher Titel ist mitunter recht interessant. Bei einem Lehrbuch auf elementarem Niveau ist es auch nicht so entscheidend, möglichst viele Originalarbeiten zu zitieren, sondern eher wichtig auf didaktisch gelungene Aufbereitungen zu verweisen. Ich habe Mühe, mir vorzustellen, wie ein amerikanischer Undergraduate 50–100 Jahre alte deutsche Arbeiten liest. Auch hier war wohl Masse wichtiger als Klasse.

Selbst wenn dies Kleinigkeiten sind, schmälern sie durch ihre große Zahl doch erheblich die Freude an dem Buch. Zusammenfassend kann man sagen, dass eine derart umfassende Sammlung von Beispielen sicherlich ihren Wert hat. Ein nicht zu unterschätzender Faktor ist, dass die intensive praktische Beschäftigung mit dem Thema vielleicht manche/n Student/in zum tiefergehenden Studium motiviert. Deshalb kann ich mir bei aller Kritik durchaus vorstellen, das Buch in einem Praktikum zur nichtlinearen Dynamik einzusetzen – allerdings nur als Ergänzung zu einem anspruchsvolleren Text.

Werner M. Seiler (Heidelberg)

W. Forst, D. Hoffmann
Funktionentheorie erkunden mit Maple

Springer Verlag, Berlin, Heidelberg, New York, 2002, ISBN 3-540-42543-8, 328 Seiten, € 24,95.

Das vorliegende Buch schließt eine Lücke im Lehrbuchangebot. Während es bereits einige Bücher gibt, die die Anfängervorlesungen unter Zuhilfenahme von Computeralgebrasystemen wie DERIVE, Maple oder Mathematica vermitteln, ist das Buch von Forst und Hoffmann meines Wissens das erste, bei welchem ein Computeralgebrasystem zur Darstellung der Funktionentheorie benutzt wird. Dies mag mehrere Gründe haben. Einer davon ist bestimmt die Tatsache, dass sich „General Purpose Computeralgebrasysteme“ wie Maple beim Rechnen mit komplexen Zahlen und Funktionen manchmal schwertun. Es lässt sich vorneweg sagen, dass die Einbindung von Maple im vorliegenden Text ausgezeichnet gelungen ist: Die Autoren benutzen Maple in eleganter Weise zur grafischen Darstellung komplexer Zahlen und Funktionen und zu vielem mehr. Dabei leidet keineswegs das übliche Curriculum. Die Autoren setzen nämlich ein zweigeteiltes Konzept um: Jedes Kapitel besteht aus einem konventionellen Teil, in welchem die funktionentheoretischen Sachverhalte mit ausführlichen Beweisen eingeführt werden, und einem zweiten Teil, in welchem Maple benutzt wird, um die besprochenen Themen zu erläutern und zu vertiefen. Auch wenn mir diese Trennung etwas zu starr erscheint, so ist doch das Gesamtergebnis sehr zufriedenstellend. Es werden die üblichen Themengebiete behandelt: Die komplexen Zahlen, Riemannsche Zahlenkugel, Stetigkeit, Potenzreihen, komplexe Differenzierbarkeit, Cauchy-Riemannsche Differentialgleichungen, die elementaren Funktionen, Kurvenintegrale, Cauchyscher Intergralsatz, Cauchysche Integralformel, Satz von Morera, Residuensatz, Laurentreihen, Argumentprinzip und Folgerungen. Zusätzlich werden spezielle konforme Abbildungen (insbesondere die Joukowski-Transformation) sowie die Γ-Funktion behandelt.

Einige Kleinigkeiten, die den ansonsten sehr guten Eindruck nur unwesentlich trüben, könnten in einer Neuauflage vielleicht besser gemacht werden:

- Ich halte die Schreibweise Sin und Cos für die hyperbolischen Funktionen für groben Unfug. In *Mathematica* ist dies z. B. die einzige korrekte Schreibweise für die trigonometrischen Funktionen.
- Das mitgelieferte Dienstleistungspaket „verdi“ sollte lieber als Textdatei geladen werden. Will man sie mit *with* als package laden, so muss Maples libname geändert werden. Das ist für den Gelegenheitsbenutzer zu kompliziert und wird auch nicht beschrieben.
- Die Autoren erwarten auf S. 153 eine Fehlermeldung des Maple-Kommandos *series*. Zurecht wäre die Erwartung einer Fehlermeldung bei *taylor*, welche bei dem betrachteten Beispiel auch eintritt. Die Funktionalität von *series* geht allerdings weit über Potenzreihen hinaus und umfasst verallgemeinerte Reihen, u. a. Laurent- und Puiseuxreihen, was die Autoren auf S. 215 sowie S. 294 ja auch nutzen.

Ich werde das Buch bei meiner nächsten Funktionentheorievorlesung einsetzen.

Wolfram Koepf (Kassel)

J. Grabmeier, E. Kaltofen, V. Weispfenning
Computer Algebra Handbook

Springer Verlag, Berlin, Heidelberg, New York, 2003, ISBN 3-540-65466-6, 638 Seiten, € 74,85.

Mit dieser kurzen Besprechung möchte ich auf ein eindrucksvolles Gemeinschaftswerk hinweisen, zu welchem ein wesentlicher Teil der internationalen Computer Algebra Community beigetragen hat und dessen Zustandebringen den Editoren einiges an (zum Glück nicht mehr ersichtlicher) Mühe abgefordert haben muss. Mit welchen mathematischen Objekten zu rechnen sei, war historisch stets der Gegenstand der Algebra; anhand deren Aufzählung ließe sich eine Geschichte der Mathematik schreiben. Mit welchen Hilfsmitteln zu rechnen sei: Auf diesem Gebiet ist nach vereinzelten Anfängen eigentlich erst etwas in Bewegung gekommen, seitdem sich die Mathematiker des Computers bemächtigt haben. Es ist damit zu rechnen, dass sowohl die Objekte wie die Methoden der Computer Algebra noch erstaunliche Ausweitungen erfahren werden. Es ist meines Erachtens auch abzusehen, dass deshalb in der Algebra einmal ein Paradigmenwechsel eintritt, ähnlich wie seinerzeit der Schritt hin zur axiomatisch-, strukturell-, mengentheoretischen modernen Algebra, nun weiterhin zur Computeralgebra. Und eines Tages wird man diese auch nur wieder einfach Algebra nennen: Die Lehre von dem, womit zu rechnen ist.

Das Ziel dieses Buches ist glücklicherweise weniger utopisch. Auf Seite 2 wird eine operable Definition des Gegenstandes der Computeralgebra vorgeschlagen, gemäß derer dann auch das Handbuch aufgebaut ist: Die exakte endliche Darstellung von konkreten und abstrakten mathematischen Objekten zwecks Lösung von mathematisch formulierten Problemen mit programmierbaren Algorithmen. Angesichts der ungeheuren Breite des mathematischen Objektbereiches mussten die Editoren gewisse Auswahlen treffen; erfreulicherweise nicht vor allem durch Ausschlüsse von Gebieten, aber in einer Graduierung der Darstellung. Einige Gebiete, die bereits Eingang in die Lehrbuchliteratur gefunden haben, erhalten eine annotierte Übersicht mit aktuellen Verweisen auf Publikationen, URLs und Software. Andere Gebiete werden ausführlicher abgehandelt, z. T. durch die entsprechenden Pioniere. Der Verweisapparat (Seiten 485-637) ist demgemäß einer der hervorstechendsten Aspekte dieses Buches und ist geschickterweise auch in die CD integriert. Wenn alles nichts hilft, so sind da immer noch die e-mail-Adressen der rund 200 Autoren.

Besondere Aufmerksamkeit wird auch den pragmatischen Fragen der Computeralgebra zuteil: Vorhandensein und Qualität der Dokumentationen, Grenzen der Zuverlässigkeit von Algorithmen, Maßnahmen zur Hebung der Interoperabilität von Programmen etc. Diese Aspekte sind insbesondere im Zusammenhang mit zwei weiteren Themen des Handbuches relevant: mit dem immer wichtiger werdenden Einfluss von Computeralgebra in der Lehre auf allen Stufen und mit der inzwischen selbstverständlichen Integration der Methodologie in die natur- und ingenieurwissenschaftliche Forschung und Praxis. Beide Bereiche, die sowohl für Anwendungen wie für Forschungsanregungen bedeutungsvoll sind, treten hier mit durchaus repräsentativen und anschaulich beschriebenen Beispielen auf.

Die Computeralgebra, und dies wird in diesem Werk deutlich, ist nicht mehr nur eine Hilfs- oder Ergänzungsdisziplin zur „eigentlichen“ Algebra, ihre Forschungsgegenstände, Darstellungsstil und Methodik haben Substanz. Es war mir persönlich eine große Genugtuung, so vielem und vielen (nicht allem und allen, wer wollte das verlangen) in so erfreulicher Weise wieder zu begegnen.

Erwin Engeler (Zürich)

J. Hromkovic
Algorithmische Konzepte der Informatik – Berechenbarkeit, Komplexitätstheorie, Algorithmik, Kryptographie

B.G. Teubner Stuttgart, Leipzig, Wiesbaden, 2001, ISBN 3-519-00332-5, 286 Seiten, € 28,-.

In den letzten Jahren ist die Zahl der auf dem Büchermarkt verfügbaren Bücher zum Gegenstand der Theoretischen Informatik erfreulich angewachsen. Allen ist das Ziel gemeinsam, in die Hauptthemen der Theoretischen Informatik einzuführen und für die zum festen Bestandteil eines jeden Informatikcurriculums gehörenden Lehrveranstaltungen zur Theoretischen Informatik die notwendige Literaturbasis zu schaffen. Dabei fällt auf, dass in jüngster Zeit einige Autoren neue Wege gehen, den nicht leicht zu vermittelnden Stoff in einer Weise aufzubereiten, die es den im allgemeinen nicht sonderlich an theoretischen Konzepten interessierten Studierenden leichter macht, Sinn, Zweck und Nutzen theoretischer Konzepte zu erfassen, Aussagen und Beweisgänge auch ohne allzu tiefes vorausgehendes Studium der Mathematik zu verstehen und sich für wissenschaftlich exaktes Arbeiten und Anwenden zu motivieren.

Mit seinem Buch „Algorithmische Konzepte der Informatik“ gelingt J. Hromkovic ein ausgezeichneter Beitrag zum Erreichen dieser Ziele. Während sich andere bewährte Einführungen in die Theoretische Informatik dominierend auf den klassischen Stoff der Berechenbarkeit, der Theorie der formalen Sprachen und der abstrakten Komplexitätstheorie orientieren, trägt Hromkovic verstärkt der Tatsache Rechnung, dass in den letzten Jahrzehnten die Theorie immer stärker auf die Bedürfnisse der Praxis eingegangen ist und über die Fülle neuer faszinierender Anwendungen auch neue Möglichkeiten entstanden sind, die Erkenntnisse der Theoretischen Informatik anschaulich zu vermitteln und bei den Studierenden die Motivation für dieses Studienfach zu erhöhen.

Wie der Titel des Buches richtig verspricht, bilden die algorithmischen Aspekte der Theoretischen Informatik den Hauptinhalt dieser Einführung. In einem einleitenden Kapitel unternimmt der Autor den interessanten Versuch, Studierenden das Beschäftigen mit dem Gegenstand der Theoretischen Informatik schmackhaft zu machen. Acht Kapitel sind den Themen Sprachen, Endliche Automaten, Turingmaschinen, Berechenbarkeit, Komplexitätstheorie, Algorithmik für schwere Probleme, Randomisierung und Kommunikation/Kryptographie gewidmet. Die Darstellung des Stoffes ist übersichtlich und gut verständlich. Dabei wird ein ausgewogenes Verhältnis zwischen der Prägung des intuitiven informalen Verständnisses und der präzisen Formalisierung und Beweisführung erreicht. Die Anzahl an benutzten Begriffen und Definitionen wird bewusst minimal gehalten. Jedes Kapitel ist mit einer relativ umfangreichen Zahl didaktisch gut ausgewählter Übungsaufgaben angereichert. Die am Schluss eines jeden Kapitels in einem gesonderten Abschnitt vorgenommene Zusammenfassung reflektiert den Studierenden noch einmal übersichtlich den besprochenen Stoff in seinem Zusammenhang.

Bleibt zu hoffen und zu wünschen, dass dieses Buch unter den Studierenden eine große Verbreitung findet und dann den erhofften leichteren und verständlicheren Zugang zum anspruchsvollen Lehrstoff der Theoretischen Informatik bringt.

Karl Hantzschmann (Rostock)

S. F. Singer
Symmetry in Mechanics – A Gentle, Modern Introduction

Birkhäuser Verlag, Basel, Boston, 2001, ISBN 0-8176-4145-9, 224 Seiten, € 45,-.

Dieses ungewöhnliche Buch ist eine kleine Perle. Wie der Untertitel verspricht, enthält es eine „gentle“ Einführung in die moderne geometrische Mechanik. Die Mechanik ist eine sehr alte Wissenschaft, und die meisten Physiker oder Ingenieure lernen sie aus den klassischen Lehrbüchern wie Goldstein oder Landau/Lifschitz. Diese Bücher sind alle koordinatenorientiert und entstanden lange vor der Renaissance der geometrischen Mechanik in den letzten circa 30 Jahren. Es gibt durchaus auch eine Reihe von Lehrbüchern über geometrische Mechanik, allen voran immer noch der bekannte Text von Abraham/Marsden, der mit zu dieser Renaissance führte. Allerdings setzen diese Bücher profunde Kenntnisse in moderner Differentialgeometrie voraus bzw. führen diese zunächst ein. Gerade Ingenieure klagen immer wieder, dass das für sie eine (zu) hohe Hürde darstellt.

Genau an dieser Stelle setzt das vorliegende Buch an. Es versucht zum einen, immer wieder zwischen den oft unterschiedlichen Denk- und Ausdrucksweisen von Physikern und Mathematikern zu vermitteln. Zum anderen versucht es, mit möglichst wenig technischem Aufwand die wesentlichen *Ideen* der Differentialgeometrie zu vermitteln. Ziel ist es, den/die Leser/in in die Lage zu versetzen, anspruchsvollere Texte wie eben z. B. Abraham/Marsden zu lesen. Dieser Versuch ist meiner Meinung nach ausgezeichnet gelungen. Es ist schon vom Umfang des Buchs her klar, dass es keine tiefgehende Einführung in die moderne Differentialgeometrie und Mechanik sein kann. Wer aber das Buch durchgearbeitet hat, ist bestens präpariert, solche Einführungen zu lesen und vor allem zu verstehen!

Zwei Beispiele mögen den Stil des Buchs demonstrieren. Bei der Definition einer Mannigfaltigkeit wird das Schwergewicht auf die Idee gelegt, dass sie lokal wie ein $\mathbb{R}^n$ aussieht; das technisch wesentlich anspruchsvollere topologische Konzept eines Hausdorff-Raums wird dabei ignoriert. Für die beabsichtigten Anwendungen reicht dies völlig aus. Außerdem verschweigt Singer solche Auslassungen nicht, sondern gibt detaillierte Referenzen zu klassischen Lehrbüchern. Lie-Gruppen sind durchgehend Matrixgruppen; abstrakte Gruppen werden nur kurz in einem optionalen Abschnitt eingeführt.

Das Ziel des Buchs ist eine Einführung in die berühmte (Meyer)-Marsden-Weinstein-Reduktion Hamiltonscher Systeme mit einer Symmetrie. Allerdings wird nicht die allgemeine Theorie dargestellt, sondern durchgehend der Spezialfall des Zweikörperproblems behandelt. Auf dem Weg dorthin werden alle wesentlichen Konzepte wie symplektische Strukturen, Differentialformen und Vektorfelder, Lie-Gruppen und -Algebren, Gruppenoperationen und Impulsabbildungen etc. in ihrer modernen intrinsischen Form eingeführt. Insbesondere die Veranschaulichung dualer Objekte wie z. B. Differentialformen, die erfahrungsgemäß Anfängern besondere Schwierigkeiten bereiten, ist gut gelungen. So fehlt auch nicht eine Diskussion, dass der Gradient eigentlich eine Einsform und eben kein Vektorfeld ist.

Zahlreiche explizite Beispiele und Aufgaben (mit Lösungen im Anhang) sowie eine kommentierte Liste weiterführender Texte runden das wirklich gut gemachte Buch ab.

Werner M. Seiler (Heidelberg)

Die folgende Besprechung ist bereits in den Mitteilungen der Deutschen Mathematiker-Vereinigung, Heft 4-2002, 14–21 erschienen. Für die Erlaubnis, sie auch hier abdrucken zu dürfen, bedanken wir uns herzlich.

S. Wagon
The Mathematical Explorer

Wolfram Research, 2001, € 162,40.

Es gibt einige Bücher, in denen ausgewählte Themen der Mathematik des 20. Jahrhunderts für Nichtmathematiker aufbereitet werden; zum Beispiel Ian Stewarts *The Problems of Mathematics* oder Keith Devlins *Mathematics: The New Golden Age*. Stan Wagon hat etwas Neues ausprobiert: Er hat ein auf Mathematica basierendes elektronisches und interaktives „Buch" geschrieben, das auf einer CD-ROM vertrieben wird, den *Mathematical Explorer*.

Der *Mathematical Explorer* besteht aus zwei Teilen. Da ist zum einen der Mathematica-Kern, der zwar nicht die Funktionalität der Vollversion von Mathematica besitzt, aber für den Hausgebrauch ausreicht. Außer den für den *Explorer* maßgeschneiderten Befehlen kann man die üblichen Anwendungen wie Differenzieren, Integrieren, Lösen von Gleichungen (alles sowohl numerisch als auch symbolisch), Termvereinfachungen, Plotten von Funktionsgraphen usw. ausführen und hat also ein Computeralgebraprogramm für die meisten mathematischen Operationen vor sich.

Aber das ist nicht der eigentliche Kern dieser CD. Der verbirgt sich etwas schamhaft unter `Help` und dort unter dem Stichwort `Help...`, nämlich Stan Wagons *Mathematical Explorer* mit 15 Kapiteln aus verschiedenen Bereichen der Mathematik. Im Einzelnen geht es um folgende Themen: Primzahlen, Differential- und Integralrechnung, Berechnung von π, ebene Kurven, Prüfziffern, Kryptographie, Escher-Pflasterungen, mathematische Rätsel, noch mehr ebene Kurven, Fraktale, Muster im Chaos, den großen Fermatschen Satz, die Riemannsche Vermutung, ungewöhnliche Zahlensysteme und den Vierfarbensatz.

Soweit das nackte Inhaltsverzeichnis – was hat es nun mit dem Interaktiven auf sich? Der *Explorer* enthält außer dem erklärenden Text nämlich Zeilen mit Mathematica-Befehlen, die man mit `Shift-Enter` ausführen kann (und sollte). Zum Beispiel findet man im Kapitel über Primzahlen die Zeile
`In[1]:= PrimePi[100]`,
mit der man die Anzahl der Primzahlen ≤ 100 berechnen kann. Hier steht die Antwort gleich darunter:
`Out[1]= 25`,
aber man kann nun mit diesen Dingen fast beliebig herumspielen. Zum Beispiel kann ich die Eingabe zu
`In[2]:= PrimePi[32578]`
verändern, und ich erfahre aus
`Out[2]= 3496`,
dass es 3496 Primzahlen ≤ 32578 gibt.

Und im π-Kapitel habe ich herausgefunden, dass unter den ersten 5000 Ziffern von π auch mein Geburtstag vorkommt, nicht aber meine Telefonnummer.

Dies sind nur zwei (absolut nichtssagende, weil kaum erkenntnisfördernde) Beispiele, wie man den *Mathematical Explorer* benutzen kann. Die Mathematica-Befehle kann jeder Leser nach Belieben abändern, um weiter auszuprobieren oder zu variieren, und es gibt viele Gelegenheiten, interessantere Dinge zu finden als den eigenen Geburtstag in der Ziffernfolge von π. Man kann sich Details zur Primzahlverteilung zeigen lassen, sich auf Feigenbaums Spuren begeben und quadratische Funktionen iterieren, parametrisierte Kurven aufzeichnen etc. An den besten Stellen gelingt es, auf diese Weise sogar so etwas wie mathematisches Verständnis zu generieren. Es ist jedoch zu betonen, dass Mathematica hier in erster Linie hilft, mathematische Sachverhalte zu illustrieren; ob der *Mathematical Explorer* vermag, den Lesern zu eigenständigen Entdeckungen zu verhelfen, bleibe fürs erste dahingestellt.

Wie jedes herkömmliche gedruckte Buch hat auch der *Mathematical Explorer* seine Stärken und Schwächen. Ich persönlich fand das Kapitel zur Differential- und Integralrechnung etwas dröge, auch wenn es dort als Zuckerl das Weierstraßsche Beispiel einer stetigen, nirgends differenzierbaren Funktion zu besichtigen gibt. Am anderen Ende der Skala hat mich das Kapitel zum Vierfarbensatz besonders fasziniert. Hier wird zuerst das Problem beschrieben, danach graphentheoretisch umformuliert und dann im Detail die (lückenhafte) Lösung von Kempe aus dem Jahr 1879 vorgestellt, dessen Algorithmus manchmal funktioniert, manchmal jedoch auch nicht. Jetzt zahlt sich die Interaktivität wirklich aus. Dank der von Wagon entwickelten Mathematica-Befehle kann sich jeder Leser Graphen erzeugen und mit der Kempeschen Methode färben lassen – und in der Animation genau nachvollziehen, ob und wann der Algorithmus versagt. Und noch etwas sieht man: Lässt man den Algorithmus statt deterministischer Wahlen wo statthaft zufällige Wahlen treffen, so steigt seine Erfolgsquote erheblich. Hier ist das elektronische Medium dem gedruckten meilenweit überlegen.

Im Großen und Ganzen halte ich den *Mathematical Explorer* für gelungen, auch wenn manche Details verbesserungswürdig sind. Die Verlinkungen sind gewiss nicht optimal, und es gibt Formulierungen, die eher in die Rubrik unfreiwilliger Humor gehören („The limit [of $\sum_{n=1}^{\infty}(-1)^{n+1}/\sqrt{n}$] is $0.604899\ldots$ which we can see by computing the sum to infinity.“). Auch auf der technischen Ebene sind nicht alle Probleme gelöst. Der Text wird in einer Art Browser dargestellt, aber im Gegensatz zu einem richtigen Browser sind die Möglichkeiten, vor und zurück zu springen, sehr begrenzt. Und führt ein Link auf eines der mitgelieferten Mathematica-Demo-Notebooks, folgt man ihm und kehrt wieder in den *Explorer* zurück, so funktioniert (zumindest auf meinem Rechner) Mathematica nicht mehr; es heißt dann *Explorer* schließen, Hilfe schließen, Hilfe wieder öffnen, *Explorer* wieder öffnen und suchen, wo man vor zwei Minuten war.

Wie der Inhaltsüberblick zeigt, sind fast alle Kapitel mit dem heutigen Abiturwissen zugänglich; mögliche Ausnahmen sind der große Fermatsche Satz und die Riemannsche Vermutung. Das Fermat-Kapitel behandelt jedoch nur die Periode vor Wiles und diskutiert diverse diophantische Gleichungen – sicher eine gute Entscheidung des Autors. Wirklich etwas härtere Kost wird zur Riemannschen Vermutung serviert.

Bei der Auswahl des Materials hat sich Wagon meines Erachtens zwei Chancen entgehen lassen. Zum einen hätte es sich angeboten, etwas zur Fourier-Analyse zu schreiben. Hier könnte man die Konvergenz einer Reihe nicht nur sehen, sondern auch hören – das wäre doch ein ideales Multimediathema! Und da ist die ganze Welt des Zufalls, der hier außer bei Randomisierungen im Hintergrund fast vollständig außen vor bleibt. Wahrscheinlichkeitstheoretische Effekte im eigentlichen Sinn werden nur einmal angesprochen, nämlich mit dem Buffonschen Nadelexperiment im Kapitel Integralrechnung (das aber auf sehr gelungene Weise). Übrigens: Im Anhang des *Explorers* sind Kurzbiographien vieler Mathematiker gesammelt, und über den Comte de Buffon, auf den dieses Experiment zurückgeht, wird dort berichtet, er habe im Jahre 1777 Brote auf den mit parallelen Linien versehenen Fußboden fallen lassen, um die Wahrscheinlichkeit zu ermitteln, dass dabei eine Linie getroffen wird. Bei aller Dekadenz des ancien régime, ganz so war es nicht: *baguette* heißt auf deutsch zunächst schlicht (dünner) Stab.

Wenn Sie nun neugierig auf den *Mathematical Explorer* geworden sind, beachten Sie bitte, dass es nur eine Version für Windows und Macintosh gibt, nicht aber für Linux, und dass der Spaß 140 Euro (netto) kostet.

Dirk Werner (Berlin)

Berichte von Konferenzen

1. **Summer School on Computational applications of commutative algebra**

Otzenhausen, 29.09 – 04.10.2002

The summer school took place in the framework of the Graduiertenkolleg “Hierarchie und Symmetrie in mathematischen Modellen” at the RWTH Aachen. The audience mainly consisted of the members of the Graduiertenkolleg, i. e. graduate students and professional mathematicians, working in different areas of both pure and applied mathematics. The overall aim of the summer school was to introduce the participants to some of the notions of commutative algebra as well as to the related algorithms, and to show by means of examples how these techniques can be applied to questions arising in other mathematical areas, here to dynamical systems with symmetry and to algebraic control theory.

The recent books by K. GATERMANN: “Computer algebra methods for equivariant dynamical systems” (Lecture Notes in Mathematics 1728, Springer, 2000) and E. ZERZ: “Topics in multidimensional linear systems theory” (Lecture Notes in Control and Information Sciences 256, Springer, 2000) have been chosen as basic references, supplemented by additional literature.

Gatermann’s book provides an overview over a whole variety of topics both from theoretical and computational commutative algebra, e. g. commutative rings, algebraic varieties, solving polynomial systems of equations, gradings, Hilbert-Poincaré series, Molien’s formula, Weyl’s integral formula, monomial orders, Gröbner bases, the Buchberger algorithm and refinements thereof, ideal membership tests, dimension theory of ideals, computational Noether normalisation, Cohen-Macaulay rings, Stanley decomposition, invariant rings and modules of equivariants of finite groups, compact Lie groups and algebraic groups, linear reductivity, computation of fundamental, primary and secondary invariants. As an application, it is shown how symmetry groups influence the behaviour of dynamical systems, such as bifurcation of steady states, and how invariant theory can be used to find generic polynomial vector fields having a prescribed symmetry group and to perform orbit space reduction.

Zerz’s book introduces the central notions of algebraic control theory, e. g. controllability, observability, autonomy, parametrizability and stabilizability, in terms of the behavioural approach, relates this to the standard input-output approach, and interprets these notions in terms of finitely presented modules over polynomial rings in several variables. This is where both theoretical and computational commutative algebra come into play.

For the summer school, every participant has been asked to read through some appropriate section of one of the abovementioned books and to give a talk on it. Hence all the participants have been well-prepared in advance, and it has been possible to discuss large parts of these books within the summer school week. Additionally, K. Gatermann (Berlin), S. Walcher (Aachen) and E. Zerz (Kaiserslautern) have been on location all the time, giving valuable advice and complementary remarks, as well as three expert talks each, reporting on more advanced topics and related recent research.

J. Müller (Aachen)

2. **Summer School on D-modules**

Kaiserslautern, 21. – 25.10.2002

The intention of the summer school was to introduce PhD students and young postdocs to the theory of D-modules. The course comprised lectures in the morning and example sessions and contributed talks in the afternoon. The morning lectures were given by Philippe Maisonobe and Claude Sabbah and covered basic D-module theory, direct images of D-modules, and effective computations on D-modules. The lecturers presented the intrinsic side and the explicit and computational side of D-module theory. Example sessions in the afternoon and lecture notes helped to gain insight into the subject.

There were 27 participants from 8 european countries. Financial support was provided by the UKL Graduate School from DAAD resources and the DFG Forschungsschwerpunkt “Globale Methoden in der komplexen Geometrie”.

In addition to the course, there were the following contributed talks: Ignacio de Gregorio: Deformations of functions on space curves and Frobenius manifolds, Luisa Fiorot: Localization of categories with differential operators, Francisco Leon Trujillo: Global Brieskorn modules and Hodge cycles, Hossein Movasati: Global Brieskorn modules and Hodge cycles, Mathias Schulze: The differential structure of the Brieskorn lattice, Christian Sevenheck: Lagrangian singularities, Lie algebroids and D-modules, Jose Maria Ucha-Enriquez: Applications of Gröbner bases to D-modules.

Further information can be found on the summer school homepage `http://www.mathematik.uni-kl.de/~wwwagag/workshops/dmod-02`.

Mathias Schulze (Kaiserslautern)

3. **Symposium on Logic, Mathematics, and Computer Science: Interactions**

Hagenberg, Austria, 22. – 24.10.2002

The symposium LMCS’02 took place in Hagenberg, Austria, on October 20-22, 2002, in honor of Prof. Bruno Buchberger’s 60th birthday, chaired by Hoon Hong (University of North Carolina) and Franz Winkler (RISC-Linz). The event consisted of a two-day workshop featuring contributed talks on topics related to Bruno Buchberger’s research interests over the past almost fourty years.

There were 20 presentations covering topics ranging from pure logic to applied computer science. The subjects of the workshop presentations emphasize the seemingly most important contribution of Buchberger to the field of mathematics, namely the invention of the Groebner Bases method, often called Buchberger algorithm, an algorithmic method in polynomial ideal theory.

Accepted workshop papers are collected and published in proceedings available in the RISC Report series (number 02-60). Extended versions of some of the papers will appear in a special issue of the Journal of Symbolic Computation to appear in fall 2003, edited by Deepak Kapur.

The last day of the symposium consisted of 6 invited talks by Henk Barendregt (University of Nijmegen), Manfred Broy (TU Munich), Dana Scott (Carnegie Mellon University), Stephen Wolfram (Wolfram Inc., by video conference), Doron Zeilberger (Rutgers University), and Bruno Buchberger himself. The invited talks will be published in the RISC book series (Springer Heidelberg), guest editor: Peter Paule.

Bruno Buchberger

The event was concluded by a birthday banquet with many of the 60 participants present. For more information, such as the detailed program and pictures taken during the conference, please visit the conference web-site at `www.risc.uni-linz.ac.at/conferences/LMCS2002`.

Wolfgang Windsteiger (Linz)

4. **Informationsaustausch zwischen FH-Professoren und Lehrern Beruflicher Schulen in Baden-Württemberg**

Stuttgart, 03.12.2002

Die Schulen haben nur ein unvollständiges und teilweise falsches Bild von der Arbeit an Fachhochschulen. Es herrscht immer noch das Bild vor, dass an den Hochschulen in anonymen Vorlesungen der Stoff ausschlielich im Vortragsstil präsentiert wird und moderne Hilfsmittel wie Computeralgebrasysteme oder Taschenrechner nicht verwendet werden dürfen. Umgekehrt beklagen sich die Hochschulen, dass die Studienanfänger nicht mehr über die elementaren Rechentechniken verfügen, relativ unselbständig sind und über kein Durchhaltevermögen verfügen. Aufgrund der Unkenntnis über die Arbeit der jeweils anderen Seite entsteht häufig eine undifferenzierte Schuldzuweisung.

Um die Vorurteile abzubauen, fand am 3. Dezember an der Fachhochschule Stuttgart - Hochschule für Technik ein Informationsaustausch zwischen Mathematikprofessoren und Lehrern an Beruflichen Schulen in Baden-Württemberg statt. Ziel war es, sich über die Arbeitsweisen und Zielsetzungen zu informieren und weitere Möglichkeiten der Kommunikation anzudiskutieren. In Vorträgen von Prof. Dr. Rainer Roos (FH Karlsruhe) und Prof. Dr. Wilhelm Werner (FH Heilbronn) wurde das Mathematik-Curriculum an Fachhochschulen, die benötigten Eingangsvoraussetzungen und der Einsatz von Computeralgebrasystemen an Fachhochschulen vorgestellt. Die Vertreter des LEU (Landesinstitut für Erziehung und Unterricht) SD Dr. Gerhard Keller und SD Bruno Weber sowie SD Dr. Jörg Heuß vom Staatlichen Seminar für Schulpädagogik berichteten über die Weiterentwicklung des Unterrichts in Mathematik nach TIMSS und PISA sowie über die daraus resultierenden veränderten Lehrpläne. Die Studierenden Christian Haag (FHT Esslingen) und Thorsten Schwing (FH Karlsruhe) kamen ebenfalls zu Wort, um über allgemeine und ihre persönlichen Eingangsprobleme an der

Fachhochschule im Umfeld der Mathematik zu berichten. In Arbeitskreisen wurde über erweiterte Möglichkeiten von Kooperation von Schule und Hochschule diskutiert. So wird insbesondere an weitere gemeinsame Tagungen mit zentralen Themenstellungen wie die Definition eines gemeinsamen Anforderungsprofils für die Schnittstelle Schule-Hochschule oder den Einsatz von Computeralgebrasystemen in Schule und Hochschule gedacht.

Die Ergebnisse der Tagung sind auf der WWW-Site der Geschäftsstelle der Studienkommission für Hochschuldidaktik Baden-Württemberg (`www.fh-karlsruhe.de/ghd`) verfügbar.

Klaus Dürrschnabel (Karlsruhe)

Hinweise auf Konferenzen

1. GAMM Jahrestagung

Padua, Italien, 24. – 28.03.2003

Sektion: Computeralgebra und Computeranalysis

Die Gesellschaft für Angewandte Mathematik und Mechanik e. V. (GAMM e. V.) lädt Sie ein zur Teilnahme an der Wissenschaftlichen Jahreskonferenz 2003 in Abano Terme, Padua, Italien, vom 24. bis zum 28. März. Eine von 24 Sektionen ist der Computeralgebra und Computeranalysis gewidmet.

Mitten im Stadtzentrum bietet das große Kongresszentrum mit seinen Tagungsräumen und den weitläufigen Räumlichkeiten für Ausstellungen und informale Treffen eine der modernsten Strukturen, die im Moment zu finden sind.

Abano Terme und die Städte, die in seiner näheren Umgebung liegen, Padua, Venedig, Vicenza und Verona, sind Attraktionen und Ausgangspunkte für eine große Anzahl von Rundfahrten, von denen jede einzelne eine faszinierende Fahrt in die Geschichte, die Kunst, die Folklore, die Gastronomie und die Weinkultur darstellt.

In der Sektion Computeralgebra und Computeranalysis werden neue Entwicklungen in vielen Gebieten diskutiert, in denen Computeralgebramethoden eine Rolle spielen, darunter etwa Lösen von Polynomsystemen, Integrationstheorie oder formales Lösen von Differentialgleichungen.

Leitung der Sektion:
Walter Krämer (Wuppertal), Franz Winkler (Linz).

Vortragende:
Franz Winkler, E. Miletics, Erik Hillgarter, Werner M. Seiler, Wolfgang Küchlin, Carsten Sinz, Franz Pauer, Thomas Bayer, Tomasz Strek.

Further Information:
`http://www.gamm2003.it/versione_tedesco/default_tedesco.html`

2. ASCM 2003 – The Asian Symposium on Computer Mathematics

Peking, China, 17. – 19.04.2003

The Asian Symposium on Computer Mathematics (ASCM) is a series of conferences which offers an opportunity for participants to present original research, to learn of research progress and new developments, and to exchange ideas and views on doing mathematics using computers. ASCM 2003 will provide an international forum for active researchers to review the current state of the art and trends on computer mathematics. The symposium will consist of plenary sessions by invited speakers, regular sessions of contributed papers, and software demonstrations. ASCM 2003 is the sixth in this series. The previous symposia ASCM 1995, 1996, 1998, 2000, 2001 in the series were held in Beijing (China), Kobe (Japan), Lanzhou (China), Chiang Mai, (Thailand), and Matsuyama (Japan), respectively.

Topics:
Research papers on all aspects of the interaction between computers and mathematics are solicited for the symposium. Specific topics include but are not limited to symbolic, algebraic, and geometric computation, computer-aided problem solving and instruction, computational algebra and geometry and computational methods for differential equation.

Further Information:
`http://www.mmrc.iss.ac.cn/~ascm/ascm03`

3. Fq7 – Seventh International Conference on Finite Fields and Applications

Toulouse, 05. – 09.05.2003

The conference will be held at Pierre Baudis congress center, the same place as for AAECC-15 conference (see below). Both conferences are in sequel, and registration to both ones will save money.

Invited Speakers:
C. Bachoc: Codes and designs in Grassmannian spaces, S.D. Cohen: Primitive polynomials over small fields, a p-adic method, Ding Cunsheng: Cyclotomy and codes, I. Duursma: Combinatorics of the two-variable zeta function, P. Gaudry: Linear recurrence with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves, J.D. Key: Recent results on permutation decoding, D. Panario: What do random polynomials over finite fieds look like, M. Zieve: Exceptional polynomials over finite fields.

Organizers:
Alain Poli, Claude Carlet, Dieter Jungnickel, Gary Mullen, Harald Niederreiter, Henning Stichtenoth, Horacio Tapia-Recillas.

Further Information:
`http://www.irit.fr/ACTIVITES/AAECC/Fq7.shtml`

4. **AAECC15 – the 15th Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes**

Toulouse, 12. – 16.05.2003

AAECC 15th Symposium will be held at Pierre Baudis congress center, the week just after Fq7 conference, organised by AAECC/IRIT. Both conferences are in sequel, and registration to both ones will save money.

Invited Speakers :
D. Costello: Graph-based convolutional LDPC codes, I. Shparlinsky: Dynamical systems generated by rational functions, A. Lauder: not known , S. Lin: Combinatoric Low Density Parity Check Codes, P. Sol: Public key cryptosystems based on rings, J. Stern: Cryptography and the methodology of provable security.

Organizers:
Alain Poli (Toulouse, General Chair), Tom Hoeholdt (Technical University of Denmark, Co-Chair).

Further Information:
`http://www.irit.fr/ACTIVITES/AAECC/A15.shtml`

5. **Tagung der Fachgruppe Computeralgebra**

Kassel, 15. – 17.05.2003

Diese Tagung der Fachgruppe Computeralgebra wurde bereits auf Seite 6 angekündigt. Die Abstracts der Hauptvorträge finden sich ebenfalls dort. Wir wollen auf dieser Tagung vor allem Nachwuchswissenschaftlern die Vorstellung ihrer Ergebnisse ermöglichen. Auf der anderen Seite wird in verschiedenen Übersichtsvorträgen auch zum aktuellen Stand in einigen wichtigen Gebieten der Computeralgebra berichtet sowie über in Deutschland mitentwickelte Computeralgebra-Software informiert.

Als Hauptvortragende konnten wir gewinnen:

- Prof. Dr. Wolfram Decker (Saarbrücken): *Computeralgebramethoden in der algebraischen Geometrie*
- Prof. Dr. Bettina Eick (Braunschweig): *Algorithmische Gruppentheorie mit dem Computeralgebrasystem GAP*
- Dr. Claus Fieker (Sydney): *Konstruktive Klassenkörpertheorie in globalen Körpern*
- Prof. Dr. Martin Kreuzer (Dortmund): *Effiziente Berechnung von Gröbner-Basen*
- Prof. Dr. Tsuyoshi Takagi (Darmstadt): *Cryptographical Algorithms*

Die Anmeldung zur Tagung ist noch bis zum 15. April möglich. Wir hoffen auf zahlreiche Beteiligung. Ein Anmeldeformular finden Sie auf der Seite `http://www.mathematik.uni-kassel.de/compmath/ca.htm`. Dort wird demnächst auch das Tagungsprogramm zu finden sein.

Organisation:
Gunter Malle (Kassel)

Weitere Informationen:
`http://www.mathematik.uni-kassel.de/compmath/ca.htm`

6. **MEGA 2003 – The Seventh International Symposium on Effective Methods in Algebraic Geometry**

Kaiserslautern, 10. – 14.06.2003

MEGA is the acronym for Effective Methods in Algebraic Geometry, a series of roughly biennial conferences on computational aspects of Algebraic Geometry with very high standards. It has taken place in 1990 (Castiglioncello, Italy), 1992 (Nice, France), 1994 (Santander, Spain),1996 (Eindhoven, Nederlands), 1998 (St. Malo, France) and 2000 (Bath, United Kingdom). Proceedings of the papers and invited talks presented at the conference have been published by Birkhauser in the series Progress in Mathematics (volumes no. 94, 109 and 143) and by the Journal of Pure and Applied Algebra (volumes no. 117 and 118, 139 and 164).

The conference topics include: Effective Methods and Theoretical and Practical Complexity Issues in: Commutative Algebra, Geometry, Real Geometry, Algebraic Number Theory, Algebraic Geometry and related fields as well as applications.

Invited speakers are David Eisenbud, Willem de Graaf, Janos Kollar, Kristin Lauter, Yuri Nesterov, Marius van der Put, Martin Sombra, Bernd Sturmfels and Orlando Villamayor.

Further Information:
`http://www.mathematik.uni-kl.de/~mega2003`

7. **Computing in Algebra and Geometry**

Kaiserslautern, 16. – 20.06.2003

The workshop will follow the conference MEGA 2003 which is to be held in Kaiserslautern from June 10 to June 14, but is otherwise completely independent. One of its goals, however, is to help PhD students and young postdocs from neighbouring fields to improve their knowledge of Groebner Basis and and Resultant methods and thus to increase their personal benefit of the MEGA conference.

During the workshop, the following topics will be covered: symbolic/numerical solving, primary decomposition, radical computation, normalization, computing in local rings (singularity theory), resultants and application. The schedule will be organized with lectures in the morning and example sessions in the early afternoon, in a way to have enough time for participants to give contributed talks.

Organizers:
D. Ilsen, C. Lossen, G. Pfister (Kaiserslautern)

Further Information:
`http://www.mathematik.uni-kl.de/~wwwagag/workshops/compag-03/`

8. **Explicit Methods in Number Theory**

Oberwolfach, 20. – 26.07.2003

The goal of this meeting is to present new methods and results on concrete aspects of number theory. In many cases this includes computational and experimental work.

Organizers:
Henry Cohen (Talence), Hendrik W. Lenstra jr. (Berkeley/Leiden), Don B. Zagier (Bonn).

Further Information:
`http://www.mfo.de/Meetings/Meeting_Program_2003.html`

9. **USACAS 2003**

Glenview, 21. – 22.06.2003

Computer algebra systems have the potential to revolutionize mathematics education at the secondary level. They do for algebra and calculus what calculators do for arithmetic: simplifying expressions, solving equations, factoring, taking derivatives, and much more. Yet, they are currently not widely used in the U.S. The conference takes place at the Glenbrock South Highschool in Glenview, Illinois.

Invited Speakers:
Bengt Ahlander (Sweden), Josef Böhm (Austria), Hongguang Fu (China), Gloria Stillman (Australia), Marlene Torres-Skoumal (Austria).

Organizers:
James E. Schultz, Robert L. Morton (Ohio University), Natalie Jakucyn (Mathematics Department Glenbrock South Highschool).

Further Information:

`http://www4.glenbrook.k12.il.us/USACAS/2003.html`

10. **ACA 2003 – The 9th International Conference on Applications of Computer Algebra**

Raleigh, North Carolina, 28. – 31.07.2003

ACA'2003 will be held from July 28 to July 31, 2003 at North Carolina State University in Raleigh, North Carolina, USA. The Scientific Committee is soliciting proposals to organize sessions at the conference. Session chairs are expected to organize 4 or more speakers on a theme consistent with that of the conference. Proposals for organizing a session should be directed to the Program Chair (Mark Giesbrecht: mwg@uwaterloo.ca).

While there is a target date of March 1 for session proposals, organizing earlier will help guarantee your choice of session date and time in the ACA schedule.

Scientific Committee:
Alkiviadis G. Akritas, Jacques Calmet, Victor Edneral, Victor Ganzha, Vladimir Gerdt, Mark Giesbrecht, Hoon Hong, Erich Kaltofen, Ilias S. Kotsireas, Bernard Kutzler, Richard Liska, Bill Pletsch, Eugenio Roanes-Lozano, Stanly Steinberg, Quoc-Nam Tran, Nikolay Vassiliev, Michael Wester.

Important Dates:
May 1, 2003: Target date for submission of speaker list and abstracts
May 15, 2003: Deadline to submit an application for financial support
June 15, 2003: Notification of decisions for financial support
June 15, 2003: Deadline for early registration
July 15, 2003: Deadline for regular registration

Organizers:
Hoon Hong, Erich Kaltofen, Agnes Szanto (General Chairs), Mark Giesbrecht (Program Chair) Stanly Steinberg, Michael Wester (Organizing Committee).

Further Information:

`http://math.unm.edu/ACA/2003`

11. **ISSAC 2003 – International Symposium on Symbolic and Algebraic Computation**

Philadelphia, Pennsylvania, 03. – 06.08.2003

ISSAC is the yearly premier international symposium in Symbolic and Algebraic Computation that provides an opportunity to learn of new developments and to present original research results in all areas of symbolic mathematical computation. ISSAC 2003 will take place at Drexel University in Philadelphia, Pennsylvania, USA, August 3-6.

Organizers:
Hoon Hong (General Chair), Robert Corless (SIGSAM Chair).

Important Dates:
March 25, 2003: Notification of acceptance/rejection
April 14, 2003: Camera-ready copies due

Poster Abstracts:
April 21, 2003: Submission deadline
May 21, 2003: Notification of acceptance/rejection
June 16, 2003: Camera-ready copies due

Further Information:

`http://knave3.mcs.drexel.edu/~issac2003/index.html`

12. **CCCG 2003 – The 15th Canadian Conference on Computational Geometry**

Halifax, 11.08. – 13.08.2003

The Canadian Conference on Computational Geometry (CCCG) focuses on the mathematics of discrete geometry from a computational point of view. Abstracting and studying the geometry problems that underly important applications of computing (such as geographic information systems, computer-aided design, simulation, robotics, solid modeling, databases, and graphics) leads not only to new mathematical results, but also to improvements in these application areas. Despite its international following, CCCG maintains the informality of a smaller workshop and attracts a large number of students.

Organizing Committee:
Jit Bose (Carleton University), Michael McAllister (Dalhousie University), Bettina Speckmann (ETH Zürich).

Further Information:

`http://www.cs.dal.ca/~cccg`

13. **NETCA – Instructional Workshop on Computational Algebra**

St. Andrews, 01.09. – 05.09.2003

The Centre for Interdisciplinary Research in Computational Algebra (CIRCA) at the University of St Andrews will be holding an instructional workshop in Computational Algebra. The workshop will feature short courses and individual lectures by invited speakers, linked to hands-on lab sessions, an introduction to the GAP software package and plenty of opportunities to try it out in the labs, and opportunities to describe your own research interests and discuss them with others.

Meals and accommodation will be provided in student residences. Names of speakers and other information will be made available as soon as possible.

The workshop will be aimed primarily at UK graduate students and research staff, although all are welcome. Thanks to generous support from NETCA the EPSRC funded Research Network in Computer Algebra, we expect to be able to offer support with travel and/or accommodation to any UK participants who need it.

Organizers:
Steve Linton, Edmund Robertson, Colin Campbell, Nik Ruskuc.

Further Information:
`http://www-circa.mcs.st-and.ac.uk/WkShop.html`

14. DMV Jahrestagung 2003

Rostock, 14.09. – 20.09.2003

Sektion: Algebra / Computeralgebra / Zahlentheorie

Das Präsidium der Deutschen Mathematiker-Vereinigung und das örtliche Organisationskomitee unter Leitung von Herrn Prof. Günther Wildenhain laden herzlich zur Jahrestagung 2003 ein, die vom 14.-20. September stattfindet. Gastgeberin ist die 1419 gegründete Universität der Hansestadt Rostock. Als Hauptvortragende konnten gewonnen werden: Yuri I. Manin (Eröffnungsvortrag), T. Colding (New York), J. Lang (Darmstadt), D. Kreimer (Boston), H. Matano (Japan), V. Mazya (Linköping), J. Pach (Budapest), S. A.Vanstone (Waterloo).

Die Sektion Algebra/Computeralgebra/Zahlentheorie wird von G. Malle, B. Porst und R. Schulze-Pillot geleitet.

Weitere Informationen:
`http://www.math.uni-rostock.de/DMV2003`

15. CASC 2003 – The Sixth International Workshop on Computer Algebra in Scientific Computing

Passau, 20.09. – 26.09.2003

The methods of Scientific Computing play an important role in research and engineering applications in the natural and the engineering sciences. The significance and impact of computer algebra methods and computer algebra systems for scientific computing has increased considerably in recent times. Nowadays, such general-purpose computer algebra systems as Mathematica, Maple, MuPAD and others enable their users to solve three important tasks within a uniform framework: symbolic manipulation, numerical computation and visualization. The ongoing development of such systems, including their adaptation to parallel environments, puts them to the forefront in scientific computing and enables the practical solution of many complex applied problems in the domains of natural sciences and engineering.

The topics addressed in the workshop cover all the basic areas of scientific computing provided by application of computer algebra methods and software, including computer algebra and approximate computations, computer algebra based simulations, computer algebra in industry and many more.

Organizing Committee:
Werner Meixner (München), lokal: Andreas Dolzmann, Thomas Sturm, Volker Weispfenning (Passau).

Further Information:
`http://wwwmayr.informatik.tu-muenchen.de/CASC2003`

16. ICTMT6 – The 6th International Conference on Technology in Mathematics Teaching

Volos, Greece, 10. – 13.10.2003

The first International Conference on Technology in Mathematics Teaching was organized in 1993 at the University of Birmingham in England. Since then this conference has been organized every two years giving people working on Curriculum Development and Mathematics Education the opportunity to meet and collaborate. The 6th International Conference on Technology in Mathematics Teaching will be organized in parallel with the 6th Panhellenic Conference on the Didactics of Mathematics and Informatics in Education.

The goal of the conference is the exploration of the role of technology in the teaching and learning of mathematics at all educational levels as well as the improvement of the quality of its instruction and learning. The goals of the conference also include applications of technology in other school subjects as well as in industry or trade, in cases where these applications are directly related to mathematics.

More specifically, the central thematic axes around which the conference has been organized are the following: The influence of technology on the teaching and learning of mathematics, Access to mathematics education through technology, Technology and assessment, Future trends in the development of technology in mathematics.

Local Organizing Committee:
Triandafillos A. Triandafillidis, Kostas Hatzikiriakou (co-chairs), Anna Chronaki, Panagiotis Politis (academic program), Kostas Sdrolias, Anastasia Manoli(secretaries), Kiki Lalagianni, Stavroula Korlou (social program), Demetra Anesti, Eleni Andoniadou (exhibitions).

Further Information:
`http://ictmt6.pre.uth.gr`

17. ATCM 2003 – The Asian Technology Conference in Mathematics

Hsin-Chu, Taiwan, 15. – 19.12.2003

The 8th Asian Technology Conference in Mathematics (ATCM2003) aims to provide an interdisciplinary forum for teachers, researchers, educators and decision makers around the world in the fields of mathematics and mathematical sciences. It also provides a venue for researchers and developers of computer technology to present their results in using technology in both basic research and pedagogical research, and to exchange ideas and information in their latest developments. The conference will cover a broad range of topics on the relevancy of technology in mathematical research and teaching.

Topics:
The topics include, but are not limited to: Geometry Using Technology, Computer Algebra, Internet Technology for Mathematics, Graphics Calculators, Mathematical Software and Tools on WWW.

Organizers:
Wei-Chi Yang (Radford University, U.S.A., wyang@radford.edu), Tilak de Alwis (Southeastern Louisiana University, U.S.A., talwis@selu.edu).

Important Dates:
Submission of Abstracts: June 15, 2003
Submission of Full Papers: July 31, 2003
Notification of Full Paper Acceptance: August 31, 2003

Further Information:
http://www.atcminc.com/mConferences/ATCM03

18. Computeralgebra in Lehre, Ausbildung und Weiterbildung III

Kloster Schöntal, 13. – 16.04.2004

Diese Tagung wird von der Fachgruppe Computeralgebra in Kooperation mit der MNU, der Fachgruppe Didaktik der Mathematik der DMV sowie der GDM veranstaltet. Sie setzt die bisherigen Tagungen in Thurnau und Schöntal fort und findet in der Zeit von Dienstag, 13.04.2004 bis Freitag, 16.04.2004 im Bildungshaus des Klosters Schöntal (http://www.kloster-schoental.de) statt.

Klosterkirche Schöntal

Weitere Informationen:
http://www.fachgruppe-computeralgebra.de/CLAW

Lehrveranstaltungen zu Computeralgebra im SS 2003

- **Rheinisch–Westfälische Technische Hochschule Aachen**
  Computeralgebra, H. Pahlings, V4+Ü2
  Algebraisches Praktikum, H. Pahlings, P2
  Fachdidaktisches Seminar: Mathematikunterricht mit Computereinsatz, U. Bettscheider, U. Schoenwaelder, S2+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, E. Görlich, Ü2

- **Technische Universität Berlin**
  Seminar Algorithmische Zahlentheorie, M. Pohst, S2

- **Universität Dortmund**
  Symbolisches und numerisches Lösen von Gleichungssystemen, H.M. Möller, V4+Ü2
  Seminar Computeralgebra, M. Kreuzer, H.M. Möller, G. Rosenberger, S2

- **Fachhochschule Flensburg**
  Mathematische Modelle in der Biologie mit Maple, N. Pavlik, S2
  Lineare Algebra mit Maple, M. Kersken, Ü1
  Applied Logics (V3) mit Maple, P. Thieler, Ü1

- **Technische Universität Hamburg-Harburg**
  Diskrete Mathematik Ib, Karl-Heinz Zimmermann, V3
  Seminar Computeralgebra, Prashant Batra, S2

- **Universität Heidelberg**
  Differential-Galoistheorie, B.H. Matzat, V4+Ü2
  Computeralgebra und Differentialgleichungen, W.M. Seiler, V4
  Seminar Gröbnerbasen und Multivariate Splines, W.M. Seiler, F. Zeilfelder, S2 (gemeinsam mit der Universität Mannheim)

- **Universität Kaiserslautern**
  Computeralgebra, A. Frühbis-Krüger, V4 + Ü2
  Geometric Methods in Cryptography, J. Zintl, V2 + Ü2
  Primzahltests und Kryptographie, A. Guthmann, V4 + Ü2
  Seminar Computeralgebra, G. Pfister, S2
  Seminar über Singularitätentheorie und Computeralgebra, G.-M. Greuel, G. Pfister, S2

- **Pädagogische Hochschule Karlsruhe**
  Informatik II, J. Ziegenbalg, V2

- **Universität Kassel**
  Einführung in Computeralgebrasysteme II (Maple), R. Schaper, P2
  Mathematik mit dem TI 92, M. Brede, V2
  Seminar Computational Mathematics: Summationsalgorithmen, W. Koepf, S2
  Oberseminar Computational Mathematics, W. Koepf, G. Malle. H.-G. Rück, OS2

- **Universität Leipzig**
  Einführung in das Symbolische Rechnen, H.-G. Gräbe, V2+Ü1
  Geometriebeweise mit dem Computer, H.-G. Gräbe, V2
  Gröbnerbasen und deren Anwendungen, H.-G. Gräbe, V2

- **Universität Linz, Research Institute for Symbolic Computation**
  Kommutative Algebra und Algebraische Geometrie, F. Winkler, V4+Ü1
  Programmieren in Mathematica, W. Windsteiger, P2
  Elimination Theory, D. Wang, V2
  Mathematik lernen und lehren mit dem CAS-Rechner TI-89/92, B. Kutzler, V2
  Projektseminar Computeralgebra, F. Winkler, S2
  Projektseminar: Solving Algebraic Equations, J. Schicho, S2

- **Universität Mannheim**
  Seminar Computeralgebra (Algebraische Gleichungssysteme und Anwendungen), W. K. Seiler, M. Schlichenmaier, H. Kredel, S2

- **Technische Universität München**
  Arbeitsgemeinschaft Computeralgebra, W. Heise, T. Honold, M. Kaplan, G. Kemper, S2

- **Universität Oldenburg**
  Seminar Math. Anwendersysteme im Sekundarbereich, W. Schmale und mitwirkende Lehrer, S2

- **Universität Paderborn**
  Computer Algebra, J. von zur Gathen, V4+Ü2
  Selected Topics in Complexity Theory, J. Blömer, P. Bürgisser, F. Meyer auf der Heide, J. von zur Gathen, S2
  Seminar: Computeralgebra , J. von zur Gathen, S2
  Oberseminar: Algorithmische Mathematik, P. Bürgisser, J. von zur Gathen, S2
  Seminar: MuPAD, W. Oevel, S2

- **Universität Rostock**
  Symbolisches Rechnen, K.Hantzschmann, V2
  Elements of Computer Mathematics, V.P. Gerdt, V2

- **Universität Tübingen**
  Algebraische Methoden in der Informatik, P. Hauck, V4
  Finger oder Fäuste – Arithmetische Algorithmen, R. Loos, C. Schwarzweller, V4+Ü2

- **Universität Würzburg**
  Programmierkurs zur Computational Physics, G. Reents, V2
  Mathematisches Praktikum (Mathematica), K. Schaper, Kompaktkurs

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 200___ die Aufnahme als Mitglied in die Fachgruppe

   Computeralgebra (CA) (bei der GI: 0.2.1).

2. Der Jahresbeitrag beträgt €7,50 bzw. €9,00. Ich ordne mich folgender Beitragsklasse zu:

   [ ] **€7,50** 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.

   [ ] **€7,50**. 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.

   [ ] **€9,00** 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, so wird c. angenommen).

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

Ort, Datum: ______________________ Unterschrift: ______________________________

Bitte senden Sie dieses Formular an:

Sprecher der Fachgruppe Computeralgebra
Prof. Dr. Wolfram Koepf
Fachbereich Mathematik/Informatik
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel
0561-804-4207,-4646 (Fax)
koepf@mathematik.uni-kassel.de
http://www.mathematik.uni-kassel.de/~koepf

Fachgruppenleitung Computeralgebra 2002-2005

Fachreferentin Chemie:
PD Dr. Karin Gatermann
Konrad-Zuse-Zentrum Berlin (ZIB)
Takustr. 7
14195 Berlin-Dahlem
030-84185-217, -107 (Fax)
gatermann@zib.de
http://www.zib.de/gatermann

Prof. Dr. Johannes Grabmeier
FH Deggendorf
Edlmairstr. 6+8
D-94469 Deggendorf
0991-3615-141
johannes.grabmeier@fh-deggendorf.de
http://www.fh-deggendorf.de/home/jgrabmeier

Vertreter der GAMM, Fachreferent Computational Engineering:
Prof. Dr. Klaus Hackl
Ruhr-Universität Bochum
Lehrstuhl für Allgemeine Mechanik
Universitätsstr. 150
44780 Bochum
0234-32-26025, -14154 (Fax)
hackl@am.bi.ruhr-uni-bochum.de

Fachexperte Physik:
Dr. Thomas Hahn
Max-Planck-Institut für Physik
Föhringer Ring 6
80805 München
089-32354-300, -304 (Fax)
hahn@feynarts.de
http://wwwth.mppmu.mpg.de/members/hahn/

Vertreter der GI:
Prof. Dr. Karl Hantzschmann
Universität Rostock
Fachbereich Informatik
Albert-Einstein-Straße 21
18059 Rostock
Postanschrift: 18051 Rostock
0381-498-3400,-3399(Fax)
hantzschmann@informatik.uni-rostock.de

Fachreferent Lehre und Didaktik:
Prof. Dr. Hans-Wolfgang Henn
Universität Dortmund
Fachbereich Mathematik
Lehrstuhl für Didaktik der Sekundarstufe I
Vogelpothsweg 87
44227 Dortmund
0231-755-2939, -2948 (Fax)
wolfgang.henn@mathematik.uni-dortmund.de
http://www.mathematik.uni-dortmund.de/didaktik/personelles/people/henn.htm

Prof. Dr. Gerhard Hiß
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen
0241-80-94543, -92108 (Fax)
Gerhard.Hiss@Math.RWTH-Aachen.de
http://www.math.rwth-aachen.de/LDFM/homes/Gerhard.Hiss

Fachreferent Schule:
OStD. Heiko Knechtel
An der Tränke 2a
31675 Bückeburg
05722-23628
HKnechtel@aol.com

Sprecher:
Prof. Dr. Wolfram Koepf
Universität Kassel
Fachbereich Mathematik/Informatik
Heinrich-Plett-Str. 40
34132 Kassel
0561-804-4207,-4646 (Fax)
koepf@mathematik.uni-kassel.de
http://www.mathematik.uni-kassel.de/~koepf

Fachexperte Mathematische Software:
Prof. Dr. Ulrich Kortenkamp
Technische Universität Berlin
Fachbereich Mathematik
Sekr. MA 6-2
Strae des 17. Juni 136
10623 Berlin
030-314-25181, -21269 (Fax)
kortenka@inf.fu-berlin.de
http://www.kortenkamps.net

Vertreter der DMV:
Prof. Dr. B. Heinrich Matzat
IWR, Univ. Heidelberg,
Im Neuenheimer Feld 368
69120 Heidelberg
06221-54-8242,-8318(Sekr.),-8850 (Fax)
matzat@iwr.uni-heidelberg.de

Stellv. Sprecher:
Prof. Dr. H. Michael Möller
Universität Dortmund
Fachbereich Mathematik
Vogelpothsweg 87
44221 Dortmund
0231-755-3077
Moeller@math.uni-dortmund.de

Fachreferent Internet:
Dr. Ulrich Schwardmann
GWDG
Am Fassberg
37077 Göttingen
0551-201-1542
Ulrich.Schwardmann@gwdg.de
http://www.gwdg.de/~uschwar1

Fachreferent Fachhochschulen:
Prof. Dr. Wilhelm Werner
Fachhochschule Heilbronn
Max-Planck-Str
74081 Heilbronn
07131-504387
werner@fh-heilbronn.de

Werbeseite der Fa. TI