Programm der 3. Jahrestagung des Schwerpunktprogrammes Algorithmische und experimentelle Methoden in Algebra, Geometrie und Zahlentheorie, SPP 1489

Alle Vorträge finden in A704 (d. h. Gebäude A, Ebene 7, Raum 4) statt .

Montag, 18.03.2013:

14:20 – 14:30	Begrüßung in A 704
14:30 – 15:15	Michael Bogner (Universität Mainz): Geometric aspects of differential operators

Kaffeepause in Raum A 701

15:45 – 16:15	Michael Adam (TU Kaiserslautern): The Cohen-Lenstra heuristic and the distribution of eigenspaces in classical groups
16:30 – 17:00	Markus Lange-Hegermann (RWTH Aachen) / Max Horn (Universität Gießen): libsing: A new interface between GAP and Singular
17:15 – 17:45	Saied Emam Mohamed (TU Darmstadt): Algebraic Cryptanalysis

Dienstag, 19.03.2013:

9:15 – 10:00	Janko Böhm (TU Kaiserslautern): Decomposition of Semigroup Algebras
10:15 – 10:45	Dima Grigoriev (MPI Bonn): Universal Stratifications

Kaffeepause in Raum A 701

11:15 – 11:45	Michael Cuntz (TU Kaiserslautern): Free but not recursively free arrangements
12:00 – 12:30	Andreas Distler (TU Braunschweig): Koklassentheorie für nilpotente Halbgruppen

Mittagspause auf Ebene K 7

14:00 – 14:45	Andreas Enge (INRIA Bordeaux - Sud-Ouest): Berechnung von Klassenpolynomen für hyperelliptische Kurven vom Geschlecht 2
14:50 – 15:00	Informationen zum Ausflug

Kaffeepause in Raum A 701

15:30 – 16:00	Julia Bartsch (Universität Göttingen): Algorithmic Aspects of Branch Groups
16:15 – 16:45	Simon Keicher (Universität Tübingen): Computing Cox rings
17:15 – 17:45	Armin Shalile (Universität Stuttgart): Decomposition numbers of Brauer algebras via Jucys-Murphy elements
18:00 – 18:30	Grischa Studzinski (RWTH Aachen): Development, implementation and applications of fundamental algorithms, relying on Gröbner bases in free associative algebras

Mittwoch, 20.03.2013:

9:15 – 10:00	Simon Hampe (Universität Saarbrücken): Algebraic and tropical Hurwitz cycles
10:15 – 10:45	Andreas Paffenholz (TU Darmstadt): Structure and Classifications of Fano Polytopes

Kaffeepause in Raum A 701

11:15 – 11:45 Simon King (Universität Jena):
An F5-algorithm for path algebra quotients and the computation of Loewy layers

11:50 – 12:20 Michael Joswig (TU Darmstadt):
Wronski Polynomial Systems with polymake and Singular

Mittagspause auf Ebene K 7

14:15 – 15:45 Stadtführung, Treffpunkt „Imperia“
Bus 1 (→ Staad/Autofähre) oder Bus 4 (→ Allmannsdorf)

16:35 – 16:50 Überfahrt, Treffpunkt zwischen Yachthafen und Fähre, 16:30

19:00 – 20:45 Abendessen in Meersburg/Haltnau

21:35 – 21:50 Überfahrt, Treffpunkt 21:30, links der Zufahrt zur Fähre

Donnerstag, 21.03.2013:

9:15 – 9:45 Mathias Schulze (TU Kaiserslautern):
Partial normalizations of Coxeter arrangements and discriminants

10:00 – 10:30 Mohamed Barakat (TU Kaiserslautern):
The search for equivariant vector bundles using computer algebra in algebraic geometry and group theory

Kaffeepause in Raum A 701

11:15 – 11:45 Ishai Dan-Cohen (Universität Duisburg-Essen):
Explicit Chabauty-Kim theory for the thrice punctured line

12:00 – 12:30 Jürgen Müller (Universität Hannover):
Iwahori-Hecke algebras of exceptional type as cellular algebras

Mittagspause auf Ebene K 7

14:00 – 14:45 Charles Leedham-Green (University of London):
Calculating with matrix groups

Kaffeepause in Raum A 701

15:15 – 15:45 Max Horn (Universität Gießen):
Constructing extensions of finite solvable groups

16:00 – 16:30 Tobias Roßmann (Universität Bielefeld):
Toroidal methods for computing zeta functions of groups and rings

Freitag, 22.03.2013:

9:30 – 10:00 Markus Kirschmer (RWTH Aachen):
One-class genera of definite ternary forms

10:15 – 10:45 Claus Fieker (TU Kaiserslautern):
Computations in the multiplicative group

Kaffeepause in Raum A 701

11:15 – 11:45 Christof Söger (Universität Osnabrück):
Normaliz: Algorithms for rational cones and affine monoids

Montag

Michael Bogner: ***Geometric aspects of differential operators***

Abstract: The study of differential equations related to geometric objects is an old but still very active subject which reaches back to studies of Euler, Gaußand Riemann.

In this talk, I discuss algebraic and arithmetic properties of differential equations which are satisfied by periods related to families of compact complex manifolds over $\mathbb{P}^1$ minus a finite set of points - so called Picard-Fuchs equations - with emphasis on families of Calabi-Yau manifolds. Moreover, I present a method to construct potential differential equations of this type and a strategy to find related families using tools from computer-algebra. This is joint work with D. van Straten and M. Dettweiler.

- - -

Michael Adam: ***The Cohen-Lenstra heuristic and the distribution of eigenspaces in classical groups***

Abstract: In 1984, Henri Cohen and Hendrik W. Lenstra introduced a probability distribution on the space of finite abelian p-groups based on the heuristic that the probability for a group to occur should be inversely proportional to the order of its automorphism group and conjectured that the sequence of class groups of quadratic number fields follows this distribution. H. Cohen and Jacques Martinet extended these ideas to more general number fields. In doing so, they noticed the existence of a set of "bad prime", which do not agree with the predicted formulas, but they could explain this by genus theory. Gunter Malle upgraded the set of "bad prime" by the primes p satisfying the property that the base field contains the pth roots of unity and phrased a new conjecture, supported by numerical data, for them, too. Jeffrey D. Achter establishes a connection between the distribution of class groups of function fields and the distribution of the eigenspaces corresponding to the eigenvalue one in symplectic groups. G. Malle relates this idea to the number field case. Motivated by these texts we compute here for a finite abelian p-group H the limit

$$P_{\infty,p,f}(H) := \lim_{n\to\infty} P_{n,p,f}(H) := \lim_{n\to\infty} \frac{|\{g \in G_n(\mathbb{Z}/p^f\mathbb{Z}) \,|\, \ker(g-1) \cong H\}|}{|G_n(\mathbb{Z}/p^f\mathbb{Z})|}$$

for certain classical groups Gn of increasing dimension n and relate the results to the distribution of class groups of number fields. In doing so we yield a reasonable backup for Malle's conjecture.

- - -

Markus Lange-Hegermann/Max Horn: ***libsing: A new interface between GAP and Singular***

Abstract: Modern applications of computer algebra necessitate the use different computer algebra systems.

We present a new work-in-progress GAP package dubbed llibsingffor connecting GAP and Singular on the kernel level. In particular, libsing allows code written in the GAP4 language to efficiently access functionality from the Singular C kernel. Additionally, libsing provides access to the interpreter level of Singular, including full use of existing Singular libraries. In the talk, we will describe the architecture of libsing and the low, middle and high level interfaces it provides to all parts of Singular.

We envision that the GAP4 programming environment (including features like garbage collection) plus libsing will become a full-fledged substitute for the Singular interpreter for efficiently accessing all capabilities of the Singular kernel.

Finally we will demonstrate the homalg project as an example of a mathematical software project relying both on the high level programming capabilities of GAP4 and the efficient commutative and noncommutative Gröbner bases implementation in Singular's kernel. The emerging package libsing has been successfully used to replace the IO-based GAP-Singular interface used by homalg. Once stable, libsing will provide the most convenient and robust interface between GAP and Singular.

- - -

Saied Emam Mohamed: ***Algebraic Cryptanalysis: Solving Multivariate Polynomial Equation Systems over Finite Fields***

Abstract: The discipline of algebraic cryptanalysis uses a range of algebraic tools and techniques to assess the security of cryptosystems, which are essential for trusted communications over open networks. Algebraic cryptanalysis is a young and largely heuristic discipline, and the exact complexity of algebraic attacks is often hard to measure. However, it has proven to be a remarkably successful practical method of attacking cryptosystems, both symmetric and asymmetric, and provides a strong measure for the overall security of a scheme.

The first step in algebraic cryptanalysis is to model a given cipher as a system of polynomial equations. The challenge is then to find a solution to the system, which corresponds to secret information used in the cipher (e. g. plaintext or secret key). In general, finding a solution to a set of polynomial equations is NP-hard. But equations generated by a cipher (from e. g. plaintext/ciphertext pairs) often have structural properties which may be exploited to find a solution significantly faster than a brute force search for the key.

In this talk we discuss some techniques of solving multivariate polynomial equation systems over finite fields and explaining how algebraic attacks work. Moreover, we present an algebraic attack on the AES block cipher together with additional side-channel information.

Dienstag

Janko Böhm: ***Decomposition of Semigroup Algebras***

Abstract: Considering finite extensions $K[A] \subseteq K[B]$ of positive affine semigroup rings over a field K, we develop an algorithm to decompose K[B] as a direct sum of monomial ideals in K[A]. This allows us to describe an algorithm for computing the regularity of homogeneous semigroup rings which outperforms the standard methods by far. In the case of simplicial semigroup rings, we show how to determine ring theoretic properties like Buchsbaum, Cohen-Macaulay, Gorenstein, normal, and seminormal in terms of the decomposition. We discuss applications in the context of the Eisenbud-Goto conjecture. This is joint work with David Eisenbud and Max J. Nitsche.

- - -

Dima Grigoriev: ***Universal Stratifications***

- - -

Michael Cuntz: ***Free but not recursively free arrangements***

Abstract: We enumerate small arrangements over finite fields with nontrivial symmetry groups which are not inductively free. It turns out that some of them have an intersection lattice which is realizable over the complex numbers. This technique even produces an example of an arrangement which is free but not recursively free in characteristic zero.

- - -

Andreas Distler: ***Koklassentheorie für nilpotente Halbgruppen***

Abstract: Die Koklassentheorie ist ein erfolgreicher Ansatz zur Untersuchung und Klassifikation endlicher, nilpotenter Gruppen. In Zusammenarbeit mit Bettina Eick studiere ich endliche, nilpotente Halbgruppen unter Verwendung eines ähnlichen Ansatzes. Ein bedeutender Unterschied ist, dass wir zusätzlich mit gewissen Algebren arbeiten, die zu den Halbgruppen korrespondieren.

Eine Halbgruppe S ist nilpotent, wenn eine natürliche Zahl c existiert, so dass die Menge aller Produkte der Länge $c+1$ aus nur einem Element besteht. In diesem Fall ist das kleinste c mit dieser Eigenschaft die Klasse von S und $|S|-1-c$ die Koklasse von S.

Die Gesamtheit der Halbgruppen gegebener Koklasse kann mit Hilfe eines Koklassengraphen veranschaulicht werden. Diese Graphen und ihre Eigenschaften zu verstehen ist vorrangiges Ziel der Untersuchungen. Als Basis dienen zunächst die Halbgruppen der Koklassen 0, 1 und 2, deren Klassfikation mit kombinatorischen Methoden erfolgte. Halbgruppen höherer Koklasse können für kleine Ordnungen mit Computerhilfe erzeugt werden. Die untersuchten Koklassengraphen lassen vermuten, dass stets periodische Strukturen in den Graphen auftauchen. Eine genaue Kenntnis der Periodizität führt direkt zu einer vollständigen Klassifikation.

Andreas Enge: ***Berechnung von Klassenpolynomen für hyperelliptische Kurven***

- - -

Julia Bartsch: ***Algorithmic Aspects of Branch Groups***
Abstract: Self-similar groups, in particular branch groups, contain interesting examples and counterexamples for classical group theoretical questions, like the Grigorchuk group. This talk gives a brief introduction to the theory of branch groups and some recently developed algorithms. The investigation of branch groups is closely related to the study of recursive group presentations. We will present a procedure for computing recursive presentations for branch groups algorithmically.

- - -

Simon Keicher: ***Computing Cox Rings***

- - -

Armin Shalile: ***Decomposition numbers of Brauer algebras via Jucys-Murphy elements***
Abstract: Brauer algebras were introduced by Richard Brauer in 1937 and are closely related to the representation theory of orthogonal, symplectic and symmetric groups. They are also a prototypical example of a cellular algebra in the sense of Graham and Lehrer. In this talk, we will introduce Brauer algebras with a focus on exhibiting their connection to symmetric groups. We will also outline how methods proposed by Okounkov and Vershik for the symmetric groups can be used to study decomposition numbers of Brauer algebras.

- - -

Grischa Studzinski: ***Development, implementation and applications of fundamental algorithms, relying on Gröbner bases in free associative algebras***
Viele Fragen, welche sich mit endlich präsentieren Algebren beschäftigen, kann man mit Hilfe von Gröbner Basen oder Berechnungen, welche auf Gröbner Basen basieren, beantworten, zum Beispiel Trivialität einer solchen Algebra, Bestimmung der Vektorraum- oder Gelfand-Kirillov Dimension oder wenn man einen Gruppenring studiert und das Problem der Konjugatorsuche lösen möchte. Eines der Ziele dieses Projektes ist es, ein Subsystem für das bekannte Computeralgebra System Singular mit dem Titel Letterplace zu erweitern, welches eine von La Scala und Levandovskyy entwickelte Methode nutzt, um Berechnungen von Gröbner Basen in der freien Algebra durchzuführen.

In einem kürzlich veröffentlichtem Paper diskutiert Roberto La Scala die Möglichkeit, nichthomogene Erzeugendensysteme zu homogenisieren und präsentiert eine verallgemeinerte Letterplace Korrespondenz, welche es erlaubt Gröbner Basen zu berechnen. Für praktische Anwedung haben homogenisierte Erzeugendensysteme häufig schwerwiegende Nachteile, allerdings bietet dieser Ansatz die Möglichkeit die Korrektheit der rein nichthomogenen Letterplace Methode theoretisch zu zeigen. Dafür kann man die natürlich auftretende Struktur des Letterplace Ringes ausnutzen und Erkennen, dass eine zusätzliche Homogenisierungsvariable nicht von Nöten ist.

Wendet man nun die bereits bekannte trennende Invariante für die Bahnen der shift-Operation des Monoids N an, erhält man eine effektive Methode zur Berechnung von nichthomogenen Gröbner Basen.

Zum Abschluß des Vortrages werden Anwendungen der neuen Methoden, sowie die neueste Version des Symbolic Data Projektes vorgestellt, welches den Prozess des Benchmarking verschiedener Computeralgebrasysteme noch weiter vereinfacht und die Verwaltung der Beispieldatenbank nicht nur benutzerfreundlicher, sondern auch übersichtlicher und strukturierter macht.

Mittwoch

Simon Hampe: ***Algebraic and tropical Hurwitz cycles***

- - -

Andreas Paffenholz: ***Structure and Classifications of Fano Polytopes***

Abstract: Lattice polytopes, i.e. polytopes whose vertices are contained in the integer lattice, are an important subclass of polytopes with applications in number theory, optimization, and algebraic geometry, among others. Lattice polytopes naturally correspond to toric varieties, and many properties of the polytope or variety are reflected on the other side.

A lattice polytopes is a Fano polytope if the origin is the unique interior lattice point in the polytope. These polytopes correspond to toric Fano varieties. Their analysis is an important step in the study of general lattice polytopes.

In my talk I will introduce Fano polytopes, discuss their connection to toric varieties, and explain structural results. In particular, I will discuss simplicial, terminal and reflexive d-dimensional Fano polytopes. These polytopes have at most 3d vertices, and I will classify those with at least 3d-2 vertices. This extends previous work of Casagrande, Nill, and Oebro.

This is based on joint work with Benjamin Assarf and Michael Joswig.

- - -

Simon King: ***An F5-algorithm for path algebra quotients and the computation of Loewy layers***

Abstract: We provide a non-commutative version of the F5 algorithm for right-modules over path algebra quotients. It terminates, if the path algebra quotient is a basic algebra. We use the F5 algorithm in negative degree monomial orderings to compute Loewy layers.

- - -

Michael Joswig: ***Wronski Polynominal Systems with polymake and Singular***

Abstract: The number of complex solutions of a generic system of polynomial equations is known by Kushnirenko's Theorem, which relates this number to the volume of the associated Newton polytope. Estimating the number of real solutions is much more difficult. By work of Soprunova and Sottile we can obtain a lower bound for certain systems of polynomial equations using special (foldable) triangulations of their Newton polytope.

In our presentation we will explain how one can define the relevant objects and do computations in the software systems polymake and Singular. The system polymake is a software for combinatorial geometry and related areas, while Singular deals with commutative algebra, algebraic geometry and related fields. A recently introduced interface allows using methods implemented in Singular from within polymake. We start with a brief introduction of the systems, before we show how one can use the new interface to compute lower bounds for the number of real solutions of a system of polynomial equations and experimentally compare this to the true number of solutions.

Donnerstag

Mathias Schulze: ***Partial normalizations of Coxeter arrangements and discriminants***

- - -

Mohamed Barakat: ***The search for equivariant vector bundles using computer algebra in algebraic geometry and group theory***

- - -

Ishai Dan-Cohen: ***Explicit Chabauty-Kim theory for the thrice punctured line***
Abstract: Let $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, and let S denote a finite set of prime numbers. In an article of 2005, Minhyong Kim gave a new proof of Siegel's theorem for X: the set $X(\mathbb{Z}[S^{-1}])$ of S-integral points of X is finite. The proof relies on a'nonabelian' version of the classical Chabauty method. At its heart is a modular interpretation of unipotent p-adic Hodge theory, given by a tower of morphisms h_n between certain $\mathbb{Q}_p$-varieties. We set out to obtain a better understanding of h_2. Its mysterious piece is a polynomial in $2|S|$ variables. Our main theorem states that this polynomial is quadratic, and gives a procedure for writing its coefficients in terms of p-adic logarithms and dilogarithms. This is joint work with Stefan Wewers.

- - -

Jürgen Müller: ***Iwahori-Hecke algebras of exceptional type as cellular algebras***
Abstract: Iwahori-Hecke algebras, which are deformations of group algebras of Coxeter groups, play a prominent role in the theory of finite groups of Lie type. By work of Geck [2008], they carry the structure of cellular algebras. Hence their representation theory is governed by so-called Graham-Lehrer cell modules and their associated invariant bilinear forms.
Neither these cell modules nor their bilinear forms are at all well-understood. We report on computations with Iwahori-Hecke algebras of exceptional type, where we have compiled a database on explicit bilinear forms for so-called W-graph representations, which conjecturally coincide with cell modules.
These computations require the handling of (large) matrices whose entries are polynomials over the rationals or the integers, which is facilitated through variants of so-called IntegralMeatAxe techniques. This is joint work with Meinolf Geck.

Charles Leedham-Green: ***Calculating with matrix groups***

The problem of computing with matrix groups over finite fields is intrinsically hard. We have now reached a point where, from a theoretical standpoint, we can determine a composition series, and much more, in polynomial time, subject to a large number of conditions. Some of these conditions, such as having a discrete logarithm oracle, are of no great practical concern, as such an oracle is available. Other conditions arise from a small number of representations of some classical groups. Other problems arise from the fact that we have not yet programmed significant recent developments.

We aspire to be able to determine a composition series for any matrix group in dimen- sion d over the field with q elements for $d < 240$ and q at most 19^{17}, with the exception of some rather exotic situations, for example when the group has a cyclic composition factor of order some prime that is too big for integer factorisation to find. However, if a quick response is required, these bounds need to be reduced.

When it comes to infinite fields the situation is completely different. This is a new area, and while much has been achieved, we are looking for problems that we can solve, rather than, as with finite fields, worrying about exceptional problems that we cannot solve.

The successes achieved with infinite fields rest, in general, on the back of our success with finite fields.

- - -

Max Horn: ***Constructing extensions of finite solvable groups***

Abstract: We discuss a novel approach for constructing finite extensions E of a solvable group G over a solvable group N such that N embeds as Fitting subgroup of E into G, up to isomorphism. This has various applications. For example, it can be used to construct all isomorphism classes of solvable groups of a given order N supposing that all solvable groups of order dividing N are already known. In the talk, we discuss this construction and the algorithms we developed for it.

Note that these algorithms have been implemented in a package for the GAP computer algebra system as part of our work in the SPP, and are currently being applied to extend the library of Small Groups to most orders up to 10,000.

- - -

Tobias Roßmann: ***Toroidale Methoden zur Berechnung von Zetafunktionen von Gruppen und Ringen***

Abstract: Zetafunktionen von Gruppen und Ringen wurden ursprünglich im Kontext des Untergruppenwachstums eingeführt.

Solche Zetafunktionen gestatten oft eulersche Faktorisierungen indiziert durch Primzahlen. Die hierbei auftretenden lokalen Zetafunktionen sind einer algorithmischen Untersuchung zugänglich. Ziel dieses gemeinsamen Projektes mit Christopher Voll ist, Algorithmen zur Berechnung und Untersuchung lokaler Zetafunktionen zu entwickeln. Im Mittelpunkt steht ein Begriff von Nichtausgeartetheit für eine Klasse p-adischer Integrale bezüglich gewisser assoziierter Polyeder.

Freitag

Markus Kirschmer: ***One-class genera of definite ternary forms***

- - -

Claus Fieker: ***Computations in the multiplicative group***

- - -

Christof Söger: ***Normaliz: Algorithms for rational cones and affine monoids***

Abstract: Normaliz is a software tool for computations in discrete convex geometry and toric algebra. Its main objectives are the computation of Hilbert bases and of Hilbert (or Ehrhart) series of rational cones $C \subset \mathbb{R}^n$. The Hilbert basis of C with respect to a sublattice L of $\mathbb{Z}^n$ is the minimal system of generators of $M = C \cap L$, and the Hilbert series, defined with respect to a grading of M counts the number of lattice points in each degree.

Normaliz combines several algorithms: Fourier-Motzkin elimination, computation of (partial) lexicographic triangulation on connection with pyramid decomposition, lattice operations, reduction in normal monoids and, rational generating functions, as a variant to triangulation based approaches, Pottier's algorithm for Hilbert bases. In our lecture we will explain the basic steps in the computation of Hilbert bases.

Normaliz has been developed in the last 15 years by W. Bruns in cooperation with R. Koch (until 2002), B. Ichim (since 2007) and C. Söger (since 2009). Several other mathematicians have contributed to it. Normaliz has interfaces to CoCoA, Singular, and Macaulay 2, polymake and is accessible from Sage. Normaliz has been written in C++, and is highly parallelized via OpenMP.