Matzat · Greuel · Hiss (Eds.)
Algorithmic Algebra and Number Theory

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Singapore
Tokyo

B. Heinrich Matzat Gert-Martin Greuel
Gerhard Hiss (Eds.)

Algorithmic Algebra and Number Theory

Selected Papers from a Conference
Held at the University of Heidelberg
in October 1997

Springer

B. Heinrich Matzat
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
der Universität Heidelberg
Im Neuenheimer Feld 368
D-69120 Heidelberg, Germany
e-mail: matzat@iwr.uni-heidelberg.de

Gert-Martin Greuel
Fachbereich Mathematik
Universität Kaiserslautern
Postfach 3049
D-67653 Kaiserslautern Germany
e-mail: greuel@mathematik.uni-kl.de

Gerhard Hiss
RWTH Aachen
Lehrstuhl D für Mathematik
Templergraben 64
D-52062 Aachen, Germany
e-mail: gerhard.hiss@math.rwth-aachen.de

Mathematics Subject Classification (1991): 11-06, 12-06, 13-06, 14-06, 20-06, 11Y40, 12Y05, 13P10, 14QXX, 20B40, 20C40, 68Q40

Cataloging-in-Publication Data applied for

Algorithmic algebra and number theory: selected papers from a conference, held at the University of Heidelberg in October 1997 / B. Heinrich Matzat ...(ed.).- Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999

ISBN-13: 978-3-540-64670-9 e-ISBN-13: 978-3-642-59932-3
DOI: 10.1007/978-3-642-59932-3

ISBN-13: 978-3-540-64670-9 Springer-Verlag Berlin Heidelberg New York

Typesetting: By the authors using a Springer LaTeX Macro Package
Cover design: *design & production* GmbH, Heidelberg

SPIN: 10654649 46/3143 - 5 4 3 2 1 0 – Printed on acid-free paper

Preface

This book contains 22 lectures presented at the final conference of the German research program (Schwerpunktprogramm) *Algorithmic Number Theory and Algebra* 1991-1997, sponsored by the Deutsche Forschungsgemeinschaft.

The purpose of this research program and of the meeting was to bring together developers of computer algebra software and researchers using computational methods to gain insight into experimental problems and theoretical questions in algebra and number theory.

The book gives an overview on algorithmic methods and on results obtained during this period. This includes survey articles on the main research projects within the program:

- algorithmic number theory emphasizing class field theory, constructive Galois theory, computational aspects of modular forms and of Drinfeld modules
- computational algebraic geometry including real quantifier elimination and real algebraic geometry, and invariant theory of finite groups
- computational aspects of presentations and representations of groups, especially finite groups of Lie type and their Hecke algebras, and of the isomorphism problem in group theory.

Some of the articles illustrate the current state of computer algebra systems and program packages developed with support by the research program, such as KANT and LiDIA for algebraic number theory, SINGULAR, REDLOG and INVAR for commutative algebra and invariant theory respectively, and GAP, SYSYPHOS and CHEVIE for group theory and representation theory.

According to the three main research directions, the book is divided into three parts representing algorithmic aspects of algebraic number theory, commutative algebra and algebraic geometry, and group theory and representation theory, edited by B. H. Matzat, G.-M. Greuel and G. Hiss, respectively.

The editors thank the contributors to this volume and the Deutsche Forschungsgemeinschaft for its support of the research program and the conference held in Heidelberg.

G.-M. Greuel, G. Hiss and B. H. Matzat

Heidelberg, May 1998

Table of Contents

Part A: Algorithmic Algebraic Number Theory

Sieving Methods for Class Group Computation
J. Buchmann, M. J. Jacobson, Jr., S. Neis, P. Theobald and D. Weber..... 3

Arithmetic of Modular Curves and Applications
G. Frey and M. Müller..... 11

Local and Global Ramification Properties of Elliptic Curves
in Characteristics Two and Three
E.-U. Gekeler..... 49

Techniques for the Computation of Galois Groups
A. Hulpke 65

Fortschritte in der inversen Galoistheorie
B. H. Matzat 79

From Class Groups to Class Fields
M. E. Pohst 103

A Gross-Zagier Formula for Function Fields
H.-G. Rück and U. Tipp 121

Extremal Lattices
R. Scharlau and R. Schulze-Pillot.....139

Part B: Algorithmic Commutative Algebra and Algebraic Geometry

On the Real Nullstellensatz
E. Becker and J. Schmid 173

Primary Decomposition: Algorithms and Comparisons
W. Decker, G.-M. Greuel and G. Pfister 187

Real Quantifier Elimination in Practice
A. Dolzmann, T. Sturm and V. Weispfenning 221

Hilbert Series and Degree Bounds in Invariant Theory
G. Kemper 249

Invariant Rings and Fields of Finite Groups
G. Kemper and G. Malle 265

Computing Versal Deformations with SINGULAR
B. Martin 283

Algorithms for the Computation of Free Resolutions
T. Siebert 295

Part C: Algorithmic Group and Representation Theory

Computational Aspects of the Isomorphism Problem
F. M. Bleher, W. Kimmerle, K. W. Roggenkamp and M. Wursthorn 313

Representations of Hecke Algebras and Finite Groups of Lie Type
R. Dipper, M. Geck, G. Hiss and G. Malle 331

The Groups of Order 512
B. Eick and E. A. O'Brien 379

Computational Aspects of Representation Theory of Finite Groups II
K. Lux and H. Pahlings 381

High Performance Computations in Group Representation Theory
G. O. Michler 399

The Structure of Maximal Finite Primitive Matrix Groups
G. Nebe 417

Presentations and Representations of Groups
W. Plesken 423