

Johannes Grabmeier
Erich Kaltofen
Volker Weispfenning
Editors

Computer Algebra Handbook



FOUNDATIONS
APPLICATIONS
SYSTEMS



Springer

Table of Contents

Foreword	v
Editorial Remarks	vii
Table of Contents	ix
List of Contributing Authors	xv
1 Development, Characterization, Prospects	1
1.1 Historical Remarks	1
1.2 General Characterization	1
1.3 Impact on Education	2
1.4 Impact on Research	4
1.5 Computer Algebra – Today and Tomorrow	6
1.5.1 Today	6
1.5.2 Outlook	7
2 Topics of Computer Algebra	11
2.1 Exact Arithmetic	11
2.1.1 Long Integer Arithmetic	11
2.1.2 Arithmetic with Polynomials, Rational Functions and Power Series	13
2.1.3 Euclid’s Algorithm and Continued Fractions	16
2.1.4 Modular Arithmetic and the Chinese Remainder Theorem ..	17
2.1.5 Computations with Algebraic Numbers	18
2.1.6 Real Algebraic Numbers	19
2.1.7 p -adic Numbers and Approximations	20
2.1.8 Finite Fields	21
2.2 Algorithms for Polynomials and Power Series	23
2.2.1 The Division Algorithm	23
2.2.2 Factorization of Polynomials	24
2.2.3 Absolute Factorization of Polynomials	26
2.2.4 Polynomial Decomposition	26
2.2.5 Gröbner Bases	28
2.2.6 Standard Bases	32
2.2.7 Characteristic Sets	32
2.2.8 Algorithmic Invariant Theory	33
2.3 Linear Algebra	36
2.3.1 Linear Systems	36
2.3.2 Algorithms for Matrix Canonical Forms	38
2.4 Constructive Methods of Number Theory	41
2.4.1 Primality Tests	41
2.4.2 Integer Factorization	44
2.4.3 Algebraic Number Fields and Algebraic Function Fields ...	45
2.4.4 Galois Groups	47
2.4.5 Rational Points on Elliptic Curves	48
2.4.6 Geometry of Numbers	50
2.5 Algorithms of Commutative Algebra and Algebraic Geometry	51
2.5.1 Algorithms for Polynomial Ideals and Their Varieties	51

2.5.2	Singularities of Varieties	54
2.5.3	Real Algebraic Geometry	55
2.6	Algorithmic Aspects of the Theory of Algebras	57
2.6.1	Structure Constants	58
2.6.2	Generators and Relations, Swapping and G-Algebras	58
2.6.3	Monad Algebras, Path Algebras and Generalizations	59
2.6.4	Finite-Dimensional Lie Algebras	60
2.6.5	Non-commutative Gröbner Bases	60
2.6.6	Structural Issues and Classification	63
2.6.7	Identities	63
2.6.8	Computational Aspects in the Representation Theory of Quivers and Path Algebras	64
2.7	Computational Group Theory	65
2.7.1	A Crash Course in Group Theory	66
2.7.2	Describing Groups	67
2.7.3	A Brief History	69
2.7.4	Permutation Groups	71
2.7.5	Matrix Groups	74
2.7.6	Black Box Groups	75
2.7.7	Abelian Groups	76
2.7.8	Polycyclic Groups	76
2.7.9	Finitely Presented Groups	78
2.7.10	Group-Theoretic Software	83
2.7.11	Another Perspective	83
2.8	Algorithms of Representation Theory	84
2.8.1	Ordinary Representation Theory	84
2.8.2	Modular Representation Theory	85
2.8.3	Generic Character Tables	87
2.8.4	Summary of Systems	88
2.9	Algebraic Methods for Constructing Discrete Structures	89
2.10	Summation and Integration	91
2.10.1	Definite Summation and Hypergeometric Identities	91
2.10.2	Symbolic Integration	94
2.11	Symbolic Methods for Differential Equations	96
2.11.1	Introduction	96
2.11.2	Differential Galois Theory	97
2.11.3	Lie Symmetries	98
2.11.4	Painlevé Theory	99
2.11.5	Completion	102
2.11.6	Differential Ideal Theory	104
2.11.7	Dynamical Systems	105
2.11.8	Numerical Analysis	108
2.12	Symbolic/Numeric Methods	109
2.12.1	Computer Analysis	109
2.12.2	Algorithms for Computing Validated Results	110

2.12.3	Hybrid Methods	112
2.13	Algebraic Complexity Theory	125
2.14	Coding Theory and Cryptography	128
2.14.1	Coding Theory	128
2.14.2	Quantum Coding Theory	130
2.14.3	Cryptography	131
2.15	Algorithmic Methods in Universal Algebra and Logic	132
2.15.1	Term Rewriting Systems	132
2.15.2	Decision Procedures and Quantifier Elimination Methods for Algebraic Theories	137
2.16	Knowledge Representation and Abstract Data Types	140
2.16.1	Mathematical Knowledge Representation and Expert Systems	140
2.16.2	Abstract Data Types	142
2.17	On the Design of Computer Algebra Systems	143
2.17.1	Memory Management	143
2.17.2	Program Verification and Abstract Data Types	144
2.17.3	The Concept of Types	144
2.17.4	Genericity	145
2.17.5	Modularization	145
2.17.6	Parallel Implementation	145
2.17.7	Continuing Development of Computer Algebra Systems	146
2.18	Parallel Computer Algebra Systems	146
2.18.1	Parallel Architectures and Operating Systems Supports	146
2.18.2	Parallel Execution: Mapping and Scheduling	147
2.18.3	Parallelism Expression and Languages	149
2.19	Interfaces and Standardization	150
2.19.1	Interfaces to Word Processors	150
2.19.2	Graphics	150
2.19.3	Interfaces to Numerical Software	150
2.19.4	User Interfaces	152
2.19.5	General Problem-Solving Environments	152
2.19.6	Standardisation	153
2.19.7	MathML	154
2.20	Hardware Implementation of Computer Algebra Algorithms	161
3	Applications of Computer Algebra	163
3.1	Physics	163
3.1.1	Elementary Particle Physics	164
3.1.2	Gravity	172
3.1.3	'Central Configurations' in the Newtonian N-Body Problem of Celestial Mechanics	176
3.1.4	CA-Systems for Differential Geometry and Applications	180
3.1.5	Differential Equations in Physics	187
3.2	Mathematics	195
3.2.1	Computer Algebra in Group Theory	196

3.2.2	The Tangent Cone Algorithm and Applications in the Theory of Singularities	197
3.2.3	Automatic Theorem Proving in Geometry	201
3.2.4	Homological Algebra	207
3.2.5	Study of Differential Structures on Quantum Groups	212
3.2.6	Orthogonal Polynomials and Computer Algebra	214
3.2.7	Computer Algebra in Symmetric Bifurcation Theory	215
3.2.8	Symbolic-Numeric Treatment of Equivariant Systems of Equations	216
3.3	Computer Science	217
3.3.1	Computer Algebra in Computer Science	217
3.3.2	Decomposable Structures, Generating Functions and Average-Case of Algorithms	219
3.3.3	Telecommunication Management Networks	221
3.4	Engineering	221
3.4.1	Computer Algebra, a Modern Research Tool for Engineering	221
3.4.2	Critical Load Computations for Jet Engines	226
3.4.3	Audio Signal Processing	227
3.4.4	Robotics	229
3.4.5	Computer Aided Design and Modelling	234
3.5	Chemistry	242
3.5.1	Computer Algebra in Chemistry and Crystallography	242
3.5.2	Chemical Reaction Systems	243
3.6	Computer Algebra in Education	244
3.6.1	New Hand-Held Computer Symbolic Algebra Tools in Mathematics Education	245
3.6.2	The Dutch Perspective	247
3.6.3	Computer Algebra in Teaching and Learning Mathematics: Experiences at the University of Plymouth, England	250
3.6.4	The Educational Use of Computer Algebra Systems at the University of Illinois	253
3.6.5	Mathematics Education from a MATHEMATICA Perspective	254
3.6.6	Visualization: Courseware for Mathematics Education	256
4	Computer Algebra Systems	261
4.1	General Purpose Systems	261
4.1.1	AXIOM	261
4.1.2	Aldor	265
4.1.3	DERIVE and the TI-92	271
4.1.4	Macsyma	283
4.1.5	MAGMA	295
4.1.6	Maple	308
4.1.7	<i>Mathematica</i>	314

4.1.8	MuPAD	321
4.1.9	REDUCE	333
4.2	Special Purpose Systems	345
4.2.1	Algebraic Combinatorics Environment (ACE)	345
4.2.2	Building Nonassociative Algebras With Albert	346
4.2.3	ALGEB	348
4.2.4	AMORE	348
4.2.5	BERGMAN	349
4.2.6	CANNES / PARCAN	351
4.2.7	CARAT	354
4.2.8	CASA	356
4.2.9	CHEVIE	359
4.2.10	C-Meataxe	363
4.2.11	CoCoA	364
4.2.12	CREP	368
4.2.13	The Desir Project and Its Continuation	370
4.2.14	DISCRETA: A Tool for Constructing t -Designs	372
4.2.15	FELIX	375
4.2.16	<i>Fermat</i>	380
4.2.17	FoxBOX and Other Blackbox Systems	383
4.2.18	GAP	385
4.2.19	GiNaC	391
4.2.20	Kan/sm1	392
4.2.21	KANT V4	396
4.2.22	LiDIA	403
4.2.23	Lie	408
4.2.24	LIE	411
4.2.25	A Brief Introduction to Macaulay 2	411
4.2.26	MAS	421
4.2.27	MASYCA	428
4.2.28	MOC	429
4.2.29	NTL: A Library for Doing Number Theory	430
4.2.30	PARI	431
4.2.31	PARSAC	434
4.2.32	QUOTPIC	436
4.2.33	REDUX	437
4.2.34	REPTILES A Program for Interactively Generating Periodic Tilings	438
4.2.35	SAC-1, Aldes/SAC-2, Saclib	439
4.2.36	SciNapse: Software that Writes PDE Software	440
4.2.37	SENAC	441
4.2.38	SIMATH - Algorithms in Number Theory	442
4.2.39	SINGULAR - A Computer Algebra System for Poly- nomial Computations	445
4.2.40	SymbMath	451

4.2.41	SYMMETRICA	452
4.2.42	Theorema: Computation and Deduction in Natural Style ..	453
4.2.43	THEORIST—a User Interface for Symbolic Algebra	454
4.3	Packages	459
4.3.1	ANU Polycyclic Quotient Programs	459
4.3.2	AREP	461
4.3.3	CALI	463
4.3.4	CLN	464
4.3.5	CRACK, LIEPDE, APPLYSYM and CONLAW	465
4.3.6	DIMSYM	468
4.3.7	EinS	469
4.3.8	<i>FeynArts</i> and <i>FormCalc</i>	469
4.3.9	FeynCalc – Tools and Tables for Elementary Particle Physics	471
4.3.10	GRAPE	473
4.3.11	Recognising Matrix Groups over Finite Fields	474
4.3.12	MOLGEN	476
4.3.13	ORME	477
4.3.14	Ratappr	477
4.3.15	TTC: Tools of Tensor Calculus	480
5	Meetings and Publications	485
5.1	Conferences and Proceedings	485
5.2	Books on Computer Algebra	490
	Cited References	493
	Subject Index	623
	Index for Authors' Contributions	635