ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

FOUNDED BY G.-C. ROTA

Volume 88

Solving Polynomial Equation Systems I

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

4 W. Miller, Jr. *Symmetry and separation of variables*
6 H. Minc *Permanents*
11 W. B. Jones and W. J. Thron *Continued fractions*
12 N. F. G. Martin and J. W. England *Mathematical theory of entropy*
18 H. O. Fattorini *The Cauchy problem*
19 G. G. Lorentz, K. Jetter and S. D. Riemenschneider *Birkhoff interpolation*
21 W. T. Tutte *Graph theory*
22 J. R. Bastida *Field extensions and Galois theory*
23 J. R. Cannon *The one-dimensional heat equation*
25 A. Salomaa *Computation and automata*
26 N. White (ed.) *Theory of matroids*
27 N. H. Bingham, C. M. Goldie and J. L. Teugels *Regular variation*
28 P. P. Petrushev and V. A. Popov *Rational approximation of real functions*
29 N. White (ed.) *Combinatorial geometrics*
30 M. Pohst and H. Zassenhaus *Algorithmic algebraic number theory*
31 J. Aczel and J. Dhombres *Functional equations containing several variables*
32 M. Kuczma, B. Chozewski and R. Ger *Iterative functional equations*
33 R. V. Ambartzumian *Factorization calculus and geometric probability*
34 G. Gripenberg, S.-O. Londen and O. Staffans *Volterra integral and functional equations*
35 G. Gasper and M. Rahman *Basic hypergeometric series*
36 E. Torgersen *Comparison of statistical experiments*
37 A Neumaier *Intervals methods for systems of equations*
38 N. Korneichuk *Exact constants in approximation theory*
39 R. A. Brualdi and H. J. Ryser *Combinatorial matrix theory*
40 N. White (ed.) *Matroid applications*
41 S. Sakai *Operator algebras in dynamical systems*
42 W. Hodges *Model theory*
43 H. Stahl and V. Totik *General orthogonal polynomials*
44 R. Schneider *Convex bodies*
45 G. Da Prato and J. Zabczyk *Stochastic equations in infinite dimensions*
46 A Bjorner, M. Las Vergnas, B. Sturmfels, N. White and G. Ziegler *Oriented matroids*
47 E. A. Edgar and L. Sucheston *Stopping times and directed processes*
48 C. Sims *Computation with finitely presented groups*
49 T. Palmer *Banach algebras and the general theory of *-algebras*
50 F. Borceux *Handbook of categorical algebra I*
51 F. Borceux *Handbook of categorical algebra II*
52 F. Borceux *Handbook of categorical algebra III*
54 A. Katok and B. Hassleblatt *Introduction to the modern theory of dynamical systems*
55 V. N. Sachkov *Combinatorial methods in discrete mathematics*
56 V. N. Sachkov *Probabilistic methods in discrete mathematics*
57 P. M. Cohn *Skew fields*
58 Richard J. Gardner *Geometric tomography*
59 George A. Baker, Jr. and Peter Graves-Morris *Padé approximants*
60 Jan Krajicek *Bounded arithmetic, propositional logic, and complex theory*
61 H. Gromer *Geometric applications of Fourier series and spherical harmonics*
62 H. O. Fattorini *Infinite dimensional optimization and control theory*
63 A. C. Thompson *Minkowski geometry*
64 R. B. Bapat and T. E. S. Raghavan *Nonnegative matrices and applications*
65 K. Engel *Sperner theory*
66 D. Cvetkovic, P. Rowlinson and S. Simic *Eigenspaces of graphs*
67 F. Bergeron, G. Labelle and P. Leroux *Combinatorial species and tree-like structures*
68 R. Goodman and N. Wallach *Representations of the classical groups*
69 T. Beth, D. Jungnickel and H. Lenz *Design theory I 2 ed.*
70 A Pietsch and J. Wenzel *Orthonormal systems and Banach space geometry*
71 George E. Andrews, Richard Askey and Ranjan Roy *Special Functions*
72 R. Ticciati *Quantum field theory for mathematicians*
76 A. A. Ivanov *Geometry of sporadic groups I*
78 T. Beth, D. Jungnickel and H. Lenz *Design theory II 2 ed.*
80 O. Stormark *Lie's structural approach to PDE systems*
88 T. Mora *Solving polynomial equation systems I*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Solving Polynomial Equation Systems I

The Kronecker–Duval Philosophy

TEO MORA

University of Genoa

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2003

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 10/13 pt *System* LaTeX 2ε [TB]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

Mora, Teo.
Solving polynomial equation systems : the Kronecker-Duval philosophy / Teo Mora.
p. cm. – (Encyclopedia of mathematics and its applications; v. 88)
Includes bibliographical references and index.
ISBN 0 521 81154 6
1. Equations–Numerical solutions. 2. Polynomials. 3. Iterative methods (Mathematics)
I. Title. II. Series.
QA218 .M64 2002
512.9′4–dc21 2001043132

ISBN 0 521 81154 6 hardback

In the beginning God created the heaven and the earth.
Genesis

Quapropter bono christiano, sive mathematici, sive quilibet impie divinatium, maxime dicentes vera, cavendi sunt.
St Augustine, *De genesis ad literam*

The most effective way for solving polynomial equation systems is just to interpret such a system as a tool for solving itself, by building programs which use this tool to manipulate its own roots.

Therefore, the best way for solving is to return the equations (well, perhaps after some massaging) shouting sufficiently loudly that *that* is the solution.

This really means that instead of working hard to build programs which *compute* the solutions, one should work hard to build programs which use the given equations in order to *manipulate* the solutions, without even computing them.

That is the Kronecker–Duval Philosophy.
R.F. Ree, *The foundational crisis, a crisis of computability?*

Since the desperate cry of Galois, 'I have no time', but even since the scribbled note of Fermat, 'I have no space', Mathematics has been forced to investigate Complexity.
E.B. Gebstadter, *Copper, Silver, Gold: an Indestructible Metallic Alloy*

Contents

Preface *page* xi

Part one: The Kronecker – Duval Philosophy 1

1 Euclid 3
- 1.1 The Division Algorithm 4
- 1.2 Euclidean Algorithm 6
- 1.3 Bezout's Identity and Extended Euclidean Algorithm 8
- 1.4 Roots of Polynomials 9
- 1.5 Factorization of Polynomials 10
- 1.6* *Computing a gcd* 12
  - 1.6.1* *Coefficient explosion* 12
  - 1.6.2* *Modular Algorithm* 16
  - 1.6.3* *Hensel Lifting Algorithm* 16
  - 1.6.4* *Heuristic gcd* 18

2 Intermezzo: Chinese Remainder Theorems 23
- 2.1 Chinese Remainder Theorems 24
- 2.2 Chinese Remainder Theorem for a Principal Ideal Domain 26
- 2.3 A Structure Theorem (1) 29
- 2.4 Nilpotents 32
- 2.5 Idempotents 35
- 2.6 A Structure Theorem (2) 39
- 2.7 Lagrange Formula 41

3 Cardano 47
- 3.1 A Tautology? 47
- 3.2 The Imaginary Number 48
- 3.3 An Impasse 51
- 3.4 A Tautology! 52

4 Intermezzo: Multiplicity of Roots 53
4.1 Characteristic of a Field 54
4.2 Finite Fields 55
4.3 Derivatives 57
4.4 Multiplicity 58
4.5 Separability 62
4.6 Perfect Fields 64
4.7 Squarefree Decomposition 68
5 Kronecker I: Kronecker's Philosophy 74
5.1 Quotients of Polynomial Rings 75
5.2 The Invention of the Roots 76
5.3 Transcendental and Algebraic Field Extensions 81
5.4 Finite Algebraic Extensions 84
5.5 Splitting Fields 86
6 Intermezzo: Sylvester 91
6.1 Gauss Lemma 92
6.2 Symmetric Functions 96
6.3* Newton's Theorem 100
6.4 The Method of Indeterminate Coefficients 106
6.5 Discriminant 108
6.6 Resultants 112
6.7 Resultants and Roots 115
7 Galois I: Finite Fields 119
7.1 Galois Fields 120
7.2 Roots of Polynomials over Finite Fields 123
7.3 Distinct Degree Factorization 125
7.4 Roots of Unity and Primitive Roots 127
7.5 Representation and Arithmetics of Finite Fields 133
7.6* Cyclotomic Polynomials 135
7.7* Cycles, Roots and Idempotents 141
7.8 Deterministic Polynomial-time Primality Test 148
8 Kronecker II: Kronecker's Model 156
8.1 Kronecker's Philosophy 156
8.2 Explicitly Given Fields 159
8.3 Representation and Arithmetics 164
8.3.1 *Representation* 164
8.3.2 *Vector space arithmetics* 165
8.3.3 *Canonical representation* 165
8.3.4 *Multiplication* 167
8.3.5 *Inverse and division* 167

8.3.6 *Polynomial factorization* 168
8.3.7 *Solving polynomial equations* 169
8.3.8 *Monic polynomials* 169
8.4 Primitive Element Theorems 170
9 Steinitz 175
9.1 Algebraic Closure 176
9.2 Algebraic Dependence and Transcendency Degree 180
9.3 The Structure of Field Extensions 184
9.4 Universal Field 186
9.5* Lüroth's Theorem 187
10 Lagrange 191
10.1 Conjugates 192
10.2 Normal Extension Fields 193
10.3 Isomorphisms 196
10.4 Splitting Fields 203
10.5 Trace and Norm 206
10.6 Discriminant 212
10.7* Normal Bases 216
11 Duval 221
11.1 Explicit Representation of Rings 221
11.2 Ring Operations in a Non-unique Representation 223
11.3 Duval Representation 224
11.4 Duval's Model 228
12 Gauss 232
12.1 The Fundamental Theorem of Algebra 232
12.2 Cyclotomic Equations 237
13 Sturm 263
13.1* Real Closed Fields 264
13.2 Definitions 272
13.3 Sturm 275
13.4 Sturm Representation of Algebraic Reals 280
13.5 Hermite's Method 284
13.6 Thom Codification of Algebraic Reals (1) 288
13.7 Ben-Or, Kozen and Reif Algorithm 290
13.8 Thom Codification of Algebraic Reals (2) 294
14 Galois II 297
14.1 Galois Extension 298
14.2 Galois Correspondence 300
14.3 Solvability by Radicals 305
14.4 Abel–Ruffini Theorem 314

14.5* Constructions with Ruler and Compass 318

Part two: Factorization 327

15 Prelude 329
15.1 A Computation 329
15.2 An Exercise 338

16 Kronecker III: factorization 346
16.1 Von Schubert Factorization Algorithm over the Integers 347
16.2 Factorization of Multivariate Polynomials 350
16.3 Factorization over a Simple Algebraic Extension 352

17 Berlekamp 361
17.1 Berlekamp's Algorithm 361
17.2 The Cantor–Zassenhaus Algorithm 369

18 Zassenhaus 380
18.1 Hensel's Lemma 381
18.2 The Zassenhaus Algorithm 389
18.3 Factorization Over a Simple Transcendental Extension 391
18.4 Cauchy Bounds 395
18.5 Factorization over the Rationals 398
18.6 Swinnerton-Dyer Polynomials 402
18.7 L^3 Algorithm 405

19 Finale 415
19.1 Kronecker's Dream 415
19.2 Van der Waerden's Example 415

Bibliography 420

Index 422

Preface

If you HOPE too much from this SPES book, you will probably be disappointed: in fact not only is it nothing more than an extension of some notes of my undergraduate course, but also my *horror vacui* compelled me to fill it with irrelevant information.

If, notwithstanding this *incipit*, you are not yet disinterested by SPES, I will now provide a quick résumé of this volume.

In the first part, *The Kronecker–Duval Philosophy*, my aim is to discuss recent approaches to **S**olving **P**olynomial **E**quation **S**ystems endorsed by the Project **PoSSo**[1] through the most elementary case: the solution of a single univariate polynomial $f(X) \in \mathbb{Q}[X]$.

It requires an introduction to Kronecker's theory (finitely generated field extensions, algebraic extensions, splitting fields) and allows us to stress the importance of the revolutionary approach introduced by Kronecker: before him, the notion of 'solving' meant producing techniques for computing the roots of the equation $f(X) = 0$; Kronecker interpreted 'solving' as producing techniques for computing **with** the roots: this in a nutshell is the rôle of algebraic extensions.

This change of perspective about 'solving', stressing more the manipulation than the computations of roots, is now central to the approaches for solving polynomial equation systems: in this volume I will sketch the significantly of the Duval model and of the Thom codification of real algebraic numbers.

Such an introduction of Kronecker's theory forced me to orient the volume toward a presentation of the theory of algebraic field extensions: in this task my *livre de chevet* was naturally van der Waerden's *Algebra*[2].

---

[1] **Po**lynomial **S**ystem **So**lving, ESPRIT-BRA 6846.

[2] B. L. van der Waerden, *Algebra*, vol. I, Ungar, New York.
I mainly used the 1950 translation more than the 1970 one; the choice is 'political'.

A discussion of Kronecker's theory requires a discussion of polynomial factorization which is the content of the second part, *Factorization*[3], which is devoted to a discussion of factorization over extension fields of prime fields, in particular the Berlekamp–Hensel–Zassenhaus factorization algorithm – but I have also included a sketch of the L^3 one.

This volume should be seen as a part of a more general survey of solving polynomial equation systems; while I already have a plan of the structure[4] and of the content of that survey, I would prefer not to bind myself too much discussing it here.

As any writer knows, the number of hidden mistakes in a draft is always larger than the number of the found ones; this text is no different. I am very grateful to Mariemi Alonso, Domenico Arezzo, Miguel Anger Borges Trenard and Maria Grazia Marinari who saved me from making some mathematical mistakes and, at the same time, detected many misspellings. I want to apologize to the reader for any errors (both misspellings and mathematical) which may still lurk.

I am grateful to the ISSAC'96 Conference in Zurich, where I was an invited tutorial speaker. This book grew out of the notes of my talks there. I am also grateful to Mika Seppala and the Mathematics Department of Florida State University in Tallahassee for inviting me to be a visiting professor in 1999. That semester in Tallahassee gave me an opportunity to test these notes in the course I offered there.

It is my firm belief that the best way of understanding a theory and an algorithm is to verify it through computation; therefore the book contains many examples which have been mainly developed via paper-and-pencil computations[5] – an approach which naturally is strongly prone to further mistakes; the readers are encouraged to follow them and, better, to test their own examples.

In order to help the readers to plan their journey through this book, some sections, containing only some interesting digressions, are indicated by asterisks in the table of contents.

---

[3] In the preparation of this part, I was mainly dependent on E. Kaltofen, Factorization of polynomials in B. Buchberger, G.E. Collins, R. Loos (Eds.) *Computer Algebra, System and Algebraic Computation*, Springer, 1982 and J.H. Davenport, Y. Siret, E. Tournier, *Computer Algebra*, Academic Press, (1988) where the reader can also find a vast bibliography.

[4] The reader can guess it from the quotations.

[5] I used computer algebra systems only to perform the four operations with polynomials.

A possible short cut which allows the readers to appreciate the discussion, without being too bored by the details (and which I usually employ in my lessons) is Chapters 1–5, 8, 11 to which I strongly suggest adding, according to the reader's interest, one of the two short tours devoted to real numbers (Section 12.1 and Chapter 13) and to Galois theory (Section 12.2, Chapter 14).

Well, good reading!