Graduate Texts in Mathematics **141**

Springer Science+Business Media, LLC

Graduate Texts in Mathematics

1. Takeuti/Zaring. Introduction to Axiomatic Set Theory. 2nd ed.
2. Oxtoby. Measure and Category. 2nd ed.
3. Schaefer. Topological Vector Spaces.
4. Hilton/Stammbach. A Course in Homological Algebra. 2nd ed.
5. Mac Lane. Categories for the Working Mathematician. 2nd ed.
6. Hughes/Piper. Projective Planes.
7. Serre. A Course in Arithmetic.
8. Takeuti/Zaring. Axiomatic Set Theory.
9. Humphreys. Introduction to Lie Algebras and Representation Theory.
10. Cohen. A Course in Simple Homotopy Theory.
11. Conway. Functions of One Complex Variable I. 2nd ed.
12. Beals. Advanced Mathematical Analysis.
13. Anderson/Fuller. Rings and Categories of Modules. 2nd ed.
14. Golubitsky/Guillemin. Stable Mappings and Their Singularities.
15. Berberian. Lectures in Functional Analysis and Operator Theory.
16. Winter. The Structure of Fields.
17. Rosenblatt. Random Processes. 2nd ed.
18. Halmos. Measure Theory.
19. Halmos. A Hilbert Space Problem Book. 2nd ed.
20. Husemoller. Fibre Bundles. 3rd ed.
21. Humphreys. Linear Algebraic Groups.
22. Barnes/Mack. An Algebraic Introduction to Mathematical Logic.
23. Greub. Linear Algebra. 4th ed.
24. Holmes. Geometric Functional Analysis and Its Applications.
25. Hewitt/Stromberg. Real and Abstract Analysis.
26. Manes. Algebraic Theories.
27. Kelley. General Topology.
28. Zariski/Samuel. Commutative Algebra. Vol.I.
29. Zariski/Samuel. Commutative Algebra. Vol.II.
30. Jacobson. Lectures in Abstract Algebra I. Basic Concepts.
31. Jacobson. Lectures in Abstract Algebra II. Linear Algebra.
32. Jacobson. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33. Hirsch. Differential Topology.
34. Spitzer. Principles of Random Walk. 2nd ed.
35. Alexander/Wermer. Several Complex Variables and Banach Algebras. 3rd ed.
36. Kelley/Namioka et al. Linear Topological Spaces.
37. Monk. Mathematical Logic.
38. Grauert/Fritzsche. Several Complex Variables.
39. Arveson. An Invitation to C^*-Algebras.
40. Kemeny/Snell/Knapp. Denumerable Markov Chains. 2nd ed.
41. Apostol. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42. Serre. Linear Representations of Finite Groups.
43. Gillman/Jerison. Rings of Continuous Functions.
44. Kendig. Elementary Algebraic Geometry.
45. Loève. Probability Theory I. 4th ed.
46. Loève. Probability Theory II. 4th ed.
47. Moise. Geometric Topology in Dimensions 2 and 3.
48. Sachs/Wu. General Relativity for Mathematicians.
49. Gruenberg/Weir. Linear Geometry. 2nd ed.
50. Edwards. Fermat's Last Theorem.
51. Klingenberg. A Course in Differential Geometry.
52. Hartshorne. Algebraic Geometry.
53. Manin. A Course in Mathematical Logic.
54. Graver/Watkins. Combinatorics with Emphasis on the Theory of Graphs.
55. Brown/Pearcy. Introduction to Operator Theory I: Elements of Functional Analysis.
56. Massey. Algebraic Topology: An Introduction.
57. Crowell/Fox. Introduction to Knot Theory.
58. Koblitz. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59. Lang. Cyclotomic Fields.
60. Arnold. Mathematical Methods in Classical Mechanics. 2nd ed.

continued after index

Thomas Becker Volker Weispfenning
In Cooperation with Heinz Kredel

Gröbner Bases

A Computational Approach to Commutative Algebra

Springer

Thomas Becker
Fakultät für Mathematik
und Informatik
Universität Passau
Postfach 2540
8390 Passau
Germany

Volker Weispfenning
Fakultät für Mathematik
und Informatik
Universität Passau
Postfach 2540
8390 Passau
Germany

Heinz Kredel
Fakultät für Mathematik
und Informatik
Universität Passau
Postfach 2540
8390 Passau
Germany

Mathematics Subjects Classifications (1991): 13P10, 68Q40, 12Y05

Library of Congress Cataloging-in-Publication Data
Becker, Thomas.
Gröbner bases: a computational approach to commutative algebra/
Thomas Becker, Volker Weispfenning, in cooperation with Heinz
Kredel.
p. cm. – (Graduate texts in mathematics)
Includes bibliographical references and index.
ISBN 978-1-4612-6944-1 ISBN 978-1-4612-0913-3 (eBook)
DOI 10.1007/978-1-4612-0913-3
1. Gröbner bases. 2. Algebra – Data processing. I. Weispfenning,
Volker. II. Kredel, Heinz. III. Title. IV. Series.
QA251.3.B43 1993
512′.24 – dc20 92-37955
CIP

Printed on acid-free paper.

Production managed by Natalie Johnson; manufacturing supervised by Vincent Scelta.
Photocomposed using the authors' LaTeX Files.

9 8 7 6 5 4 3 2 (Corrected second printing, 1998)

ISBN 978-1-4612-6944-1

Preface

The origins of the mathematics in this book date back more than two thousand years, as can be seen from the fact that one of the most important algorithms presented here bears the name of the Greek mathematician Euclid. The word "algorithm" as well as the key word "algebra" in the title of this book come from the name and the work of the ninth-century scientist Mohammed ibn Mûsâ al-Khowârizmî, who was born in what is now Uzbekistan and worked in Baghdad at the court of Harun al-Rashid's son. The word "algorithm" is actually a westernization of al-Khowârizmî's name, while "algebra" derives from "al-jabr," a term that appears in the title of his book *Kitab al-jabr wa'l muqabala*, where he discusses symbolic methods for the solution of equations. This close connection between algebra and algorithms lasted roughly up to the beginning of this century; until then, the primary goal of algebra was the design of constructive methods for solving equations by means of symbolic transformations.

During the second half of the nineteenth century, a new line of thought began to enter algebra from the realm of geometry, where it had been successful since Euclid's time, namely, the *axiomatic method.* The starting point of the axiomatic approach to algebra is the question, What kind of object is a symbolic solution to an algebraic equation? To use a simple example, the question would be not only, What is a solution of $ax + b = 0$, but also, What are the properties of the objects a and b that allow us to form the object $-b/a$? The axiomatic point of view is that these are objects in a surrounding algebraic structure which determines their behavior. The algebraic structure in turn is described and determined by properties that are laid down in a set of axioms.

The foundations of this approach were laid by Richard Dedekind, Ernst Steinitz, David Hilbert, Emmy Noether, and many others. The axiomatic method favors abstract, non-constructive arguments over concrete algorithmic constructions. The former tend to be considerably shorter and more elegant than the latter. Before the arrival of computers, this advantage more or less settled the question of which one of the two approaches was to be preferred: the algorithmic results of mathematicians like Leopold Kronecker and Paul Gordan were way beyond the scope of what could be done with pencil and paper, and so they had little to offer except being more tedious than their non-constructive counterparts.

On the other hand, it would be a mistake to construe the axiomatic and the algorithmic method as being irreconcilably opposed to each other. As a matter of fact, significant algorithmical results in algebra were proved by the very proponents of axiomatic thinking such as David Hilbert and Emmy Noether. Moreover, mathematical logic—a field that centers around the axiomatic method—made fundamental contributions to algorithmic mathematics in the 1930s. Alan Turing and Alonzo Church for the first time made precise the concept of computability in what is known as Church's thesis, or also as the Church-Turing thesis. Kurt Gödel proved that certain problems inherently elude computability and decidability. This triggered a wave of new results by Alfred Tarski and other members of the Polish school of logicians on the algorithmic solvability or unsolvability of algebraic problems. Again, because of their enormous complexity, these algorithms were of no practical significance whatsoever. As a result, the beginning second half of this century saw an axiomatic and largely non-constructive approach to algebra firmly established in both research and teaching.

The arrival of computers and their breathtaking development in the last three decades then prompted a renewed interest in the problem of effective constructions in algebra. Many constructive results from the past were unearthed, often after having been rediscovered independently. Moreover, the development of new concepts and results in the area has now established *computer algebra* as an independent discipline that extends deeply into both mathematics and computer science.

There are many good reasons for viewing computer algebra as an independent field. However, the fact that the mathematical part of it is somewhat separated from the work of pure algebraists is, in our opinion, rather unfortunate and not at all justified. We feel that this situation must and will change in the near future. As a matter of fact, computational aspects are beginning to show up more and more in undergraduate-level textbooks on abstract algebra. There is, however, one particular contribution made by computational algebra that is in most dire need of being introduced in the mathematical mainstream, namely, the theory of *Gröbner bases.*

Gröbner bases were introduced by Bruno Buchberger in 1965. The terminology acknowledges the influence of Wolfgang Gröbner on Buchberger's work. To the reader who has any background in abstract algebra at all, the basic idea behind the theory is easily explained. Suppose you are given a finite set of polynomials in one variable over a field and you wish to decide membership in the ideal generated by these polynomials in the polynomial ring. What you must do is compute the greatest common divisor of the given polynomials by means of the Euclidean algorithm. Any given polynomial then lies in the ideal in question if and only if its remainder upon division by this gcd equals zero. Gröbner basis theory is the successful attempt to imitate this procedure for polynomials in several variables. Given a finite set of multivariate polynomials over a field, the *Buchberger algorithm* computes a new set of polynomials, called a Gröbner basis, which generates the same ideal as the original one and is an analogue to the gcd of the unvariate case in the following sense. A given polynomial lies in the ideal generated by the Gröbner basis if and only if a suitably defined normal form of the polynomial with respect to the Gröbner basis equals zero. The computation of this normal form is a rather straightforward generalization of long division of polynomials, except that we are looking at the division of one polynomial by a set of finitely many polynomials.

Considering both the outstanding importance of the Euclidean algorithm for the computation of gcd's of univariate polynomials and the scope of its implications in pure and computational algebra, it should come as no surprise that its multivariate analogue, the Buchberger algorithm for the computation of Gröbner bases, is of similar relevance. It leads to solutions to a large number of algorithmic problems that are related to polynomials in several variables. Most notably, algorithms that involve Gröbner basis computations allow exact conclusions on the solutions of systems of nonlinear equations, such as the (geometric) dimension of the solution set, the exact number of solutions in case there are finitely many, and their actual computation with arbitrary precision.

Most of the problems for which Gröbner bases provide algortihmic solutions were already known to be solvable in principle. Gröbner bases are a giant step forward insofar as actual implementations have become feasible and have actually provided answers to physicists and engineers. On the other hand, many problems of no more than moderate input size still defy computation. The mathematics behind the algorithms as well as the hardware that performs them have a long way to go before these problems can be considered solved to the satisfaction of the user.

The purpose of this book is to give a self-contained, mathematically sound introduction to the theory of Gröbner bases and to some of its applications, stressing both theoretical and computational aspects.

A book that would start out with Gröbner basis theory would have to direct its readers to a source for a large number of elementary results on commutative rings and, more specifically, on polynomials in several variables. These are of course all available somewhere, and certainly known to the mature mathematician. However, we found ourselves unable to name a reasonably small number of books that would enable the beginning graduate student or the non-mathematician with an interest in Gröbner bases to aquire this background within a reasonable amount of time. *We have therefore decided to write a book that requires no prerequisites other than the mathematical maturity of an advanced undergraduate student.* In particular, no prior knowledge of abstract algebra whatsoever is assumed. Under the European system, this means that the book can be used after the second semester of mathematics or computer science. People with different backgrounds will enter such a book at different points; for more details, we refer the reader to the comments on "How to Use This Book" on p. xi.

As for the overall concept, the book traverses three stages. Chapters 0–3 provide pre-Gröbner-bases results on commutative rings with an emphasis on polynomial rings, as well as the basics on vector spaces and modules. Chapters 4 and 5 then develop Gröbner basis theory. The definition of a Gröbner basis does not show up until Section 5.2, but the material of Chapter 4 and Section 5.1 is rather specific to Gröbner bases already. Chapters 6–10 cover a wide range of applications, intertwined with a development of post-Gröbner-bases algebra. Algorithms are presented using a semi-formalism that is self-explanatory even to those with no background in computer programming. Strong emphasis is placed on a mathematically sound verification of the algorithms. Each chapter closes with a "Notes" section that puts the material in a larger mathematical perspective by tracing its historical development and providing references to the literature.

Needless to say, the list of omissions is tremendous. If it is possible at all to write the definitive book on computational algebra, then this is not it.

More specifically, the choice of the material and the reasons for making it are as follows. The introductory chapters 0–3 are written mainly for the purpose of providing the necessary background for Gröbner bases and their applications. The solutions to algorithmic problems such as factorization of polynomials given there are strictly "in principle" solutions; implementations of any practical value involve considerably more mathematics. Our treatment is thus incomplete in a sense; on the other hand, we are laying firm mathematical foundations which can also be helpful for the reader who wishes to proceed to the advanced literature on topics in computational algebra other than Gröbner bases.

Chapters 4 and 5, the main chapters on Gröbner bases, are fairly complete both theoretically and algorithmically. The theory of orders and reduction relations of Chapter 4 is rather well-rounded. In Chapter 5, the theoretical aspects of Gröbner bases are explored extensively. The Buchberger algorithm for their computation is presented first in an "in principle" version and then in two real-life versions. The only major omission in these two chapters—and it is one that actually pervades the entire book—is the absence of any *complexity theory*, that is, the discussion of the time and space that an algorithm requires as a function of the size of its input. This omission is clearly a serious one. It was not made because we consider the issue to be of minor importance. On the contrary, we feel that complexitiy theory is too important an issue to be dealt with lightly. We hope that our effort will motivate others to treat these problems comprehensively in some kind of book format. A brief overview of complexity results for Gröbner basis constructions is given in the appendix "Outlook on Advanced and Related Topics" at the end of the book.

Once Gröbner bases have been introduced, there is an almost limitless choice of topics that one could cover. Our focus in Chapters 6–10 is on the theory of polynomial ideals. A large number of ready-to-use algorithms is presented. Furthermore, we demonstrate how Gröbner bases can often be used to give elegant an enlightening proofs of classical results, for example, in the area of algebraic field extensions. This shows that Gröbner bases are not only a powerful tool for actual computations, but also a cornerstone of commutative algebra.

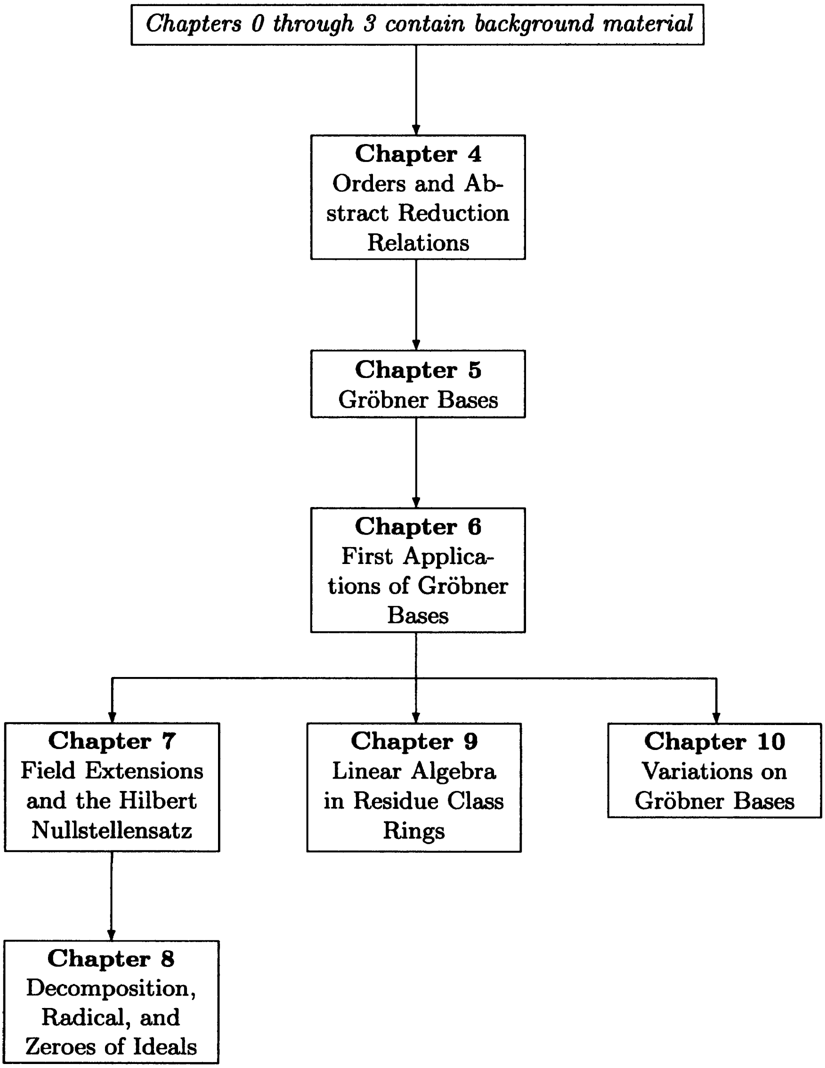
The book closes with an appendix that tries to at least partly make up for the incompleteness of this book. Here, we have given brief summaries of a number of recent results that surround or extend Gröbner basis theory. Each section explains a problem, outlines the solution, and provides a guide to the original literature.

The authors wish to thank Johannes Grabmeier, Alexander Knapp, Frank Lippold, Wolfgang Mark, Christian Münch, Michael Pesch, Gernot Schreib, and Thomas Sturm for reading parts of the manuscript. Gerlinde Kollmer kept us organized and did a lot of work in LaTeX along the way. The typesetting of the final manuscript was done by the first author in LaTeX—with the additional use of several AMSFonts—on an Atari Mega 2. Special thanks is due to Michael Pesch for his superb software consulting, and to Thomas Sturm for his competence and dedication.

Passau, Germany T.B., V.W., H.K.

How to Use This Book

Interdependence of Chapters



Chapters 0 through 3 contain background material
Chapter 4 Orders and Abstract Reduction Relations
Chapter 5 Gröbner Bases
Chapter 6 First Applications of Gröbner Bases
Chapter 7 Field Extensions and the Hilbert Nullstellensatz
Chapter 9 Linear Algebra in Residue Class Rings
Chapter 10 Variations on Gröbner Bases
Chapter 8 Decomposition, Radical, and Zeroes of Ideals

Sections 6.1, 6.4, and 7.5–7.7 are exempt from this flow diagram. They can be postponed or dropped altogether; details are to be found at the beginning of each of these sections.

Prerequisites

Chapters 0–3 of this book are written for the reader with very little or no background in abstract algebra. The prerequisite for this part is the mathematical maturity of an advanced undergraduate student. You may skip these chapters if you can answer the following questions.

> What is a commutative ring with unity, and when is it a field?
>
> What is an ideal, and what is a residue class ring?
>
> What does the Euclidean algorithm do with two univariate polynomials over a field, and how does it do it?
>
> What is a vector space?

If you failed the test, then you must read Chapters 0 and 1 and the first two sections of Chapter 2 to be able to understand the main part on Gröbner bases (Chapters 4 and 5). If you decide to continue on past Chapter 5 into the applications, you will soon feel the need to read the rest of Chapter 2 as well as Chapter 3.

If you passed the test or know you could, then for you, the book begins with Chapter 4. If you need to go back to one of the first four chapters for some specific definition or result that you have trouble with, then the index and the extensive cross-referencing of this book should make it easy for you to do so.

Exercises

There are two types of exercises: those printed in normal size, and those in small print. Normal size indicates that these exercises have the status of lemmas whose proof is left to the reader. Their statements will be used later on. None of them are hard; working them is also a good way of making sure that you are ready to grasp the material that is being presented next. Small print indicates exercises in the usual sense of application and extension of what has just been covered. The difficulty ranges from easy to moderate.

Use of Computer Algebra Systems

It is possible to view this as a mathematics textbook that can be read without the use of a computer. On the other hand, most of the mathematics presented here is application-oriented, and seeing things happen or making things happen on the screen will greatly enhance the experience of studying the material.

If a computer algebra system is at hand, then there are basically two things that you can do along with reading this book. Firstly, if an algorithm that you have just learned about is available on your system, you can simply run it on examples that you make up, get from the exercises, or find somewhere else. Although this is somewhat less than creative, you will be surprised how much it helps your understanding and motivation. The other thing is to implement algorithms from the book. Doing so from scratch will in general be a major endeavor. However, many algorithms in computational algebra are such that they allow a top-down approach, where good results can be obtained by tying together lower-level algorithms with relatively little effort. In order to do this, you need a system that provides a library of polynomial algorithms and the possibility to use them in your own programs. If you implement an algorithm that was already part of your system, then you have worked a useful exercise; if it was not, then you have extended the capabilities of your system.

Commercially available computer algebra systems that are suited to be used along with this book include Axiom, Macsyma, Maple, Mathematica, and Reduce. A system that the authors of this book recommend is MAS by Heinz Kredel. MAS makes available for interactive and programming use an extensive library of polynomial algorithms, including those that were developed for the system ALDES/SAC-2. In addition to such classics as greatest common divisors, factorization, and real root isolation, you will find the Buchberger algorithm for the computation of Gröbner bases as well as applications thereof such as ideal decomposition and real roots of polynomial systems. Of the more recent variants of the Buchberger algorithm, the non-commutative case (polynomial rings of solvable type), comprehensive Gröbner bases, and Gröbner bases over principal ideal domains and Euclidean domains are implemented. Programming in MAS is in a language that is based on MODULA-2. User-defined programs can be run interactively; if a MODULA-2 compiler is available, they can also be compiled, thus allowing a fair comparison between existing and user-defined versions of algorithms. MAS is available free of charge per anonymous ftp from alice.fmi.uni-passau.de and via World Wide Web from http://alice.fmi.uni-passau.de/mas.htm. Currently available is version 1.0 for UN*X workstations (e.g. IBM RS6000/AIX, HP 9000/HP-UX, NextStep, Sun Sparc with a Modula-2 to C translator) and PCs 386, 486, 586 (DOS, OS2 and Linux).

Use as a Textbook

It should be clear from the above discussion of prerequisites that this book allows a variety of uses as a textbook on the advanced undergraduate as well as the graduate level. There is at present no established way of including Gröbner bases in the mathematics/computer science curriculum. The fact that this book requires practically no specific prior knowledge should make it possible to experiment in this regard.

One conceivable situation that deserves perhaps some comment is the following. Suppose you are at a point where the basic theory of commutative rings and polynomial rings is available. Now you wish to cover Gröbner bases, but you do not have the time and/or the desire to get into the theory of orders and reduction relations to the extent that they are treated in Chapter 4. You may then essentially start with Section 4.5, which deals with reduction relations and Newman's lemma. This requires only a moderate amount of material from the earlier sections of Chapter 4, and you should have no trouble providing this material. You then jump ahead to Section 5.1. You will need some more material from Chapter 4, most of which is obvious and easily provided, such as the definition of a quasi-order. The only deeper results that you will need are Dickson's lemma, whose proof you lift from the proof of Proposition 4.49, the well-foundedness of term orders, which you prove using the comments in Exercise 4.63, and the properties of the induced quasi-order on the polynomial ring, which you transfer from Lemma 4.67 and Theorem 4.69.

Abbreviations

The following abbreviations will be used throughout this book.

cf., (Latin *confer*) compare
e.g., (Latin *exempli gratia*) for example
etc., (Latin *et cetera*) and so on
i.e., (Latin *id est*) that is
iff, if and only if
w.l.o.g., without loss of generality
w.r.t., with respect to

Moreover, a □ will indicate the end of a proof.

Numberings

Chapters and sections are numbered in the obvious way: Chapter 5, for example, consists of Sections 5.1–5.6. Definitions, lemmas, propositions, theorems, corollaries, and exercises are treated as one type of item and numbered consecutively within each chapter: Chapter 5 contains Exercise 5.1, Theorem 5.2, etc. Due to the fact that there is such an item on virtually every page, this should make it easy to locate referenced items. Algorithms are given in tables in order to prevent them from running across a page-break; these tables are also numbered within each chapter.

Contents

List of Algorithms