

Graduate Texts in Mathematics **185**

Editorial Board

S. Axler F.W. Gehring K.A. Ribet

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

David Cox
John Little
Donal O'Shea

Using Algebraic Geometry

With 22 Illustrations



Springer

David Cox
Department of Mathematics
and Computer Science
Amherst College
Amherst, MA 01002-5000
USA

John Little
Department of Mathematics
College of the Holy Cross
Worcester, MA 01610-2395
USA

Donal O'Shea
Department of Mathematics, Statistics
and Computer Science
Mount Holyoke College
South Hadley, MA 01075-1493
USA

Editorial Board

S. Axler
Mathematics Department
San Francisco State
University
San Francisco, CA 94132
USA

F.W. Gehring
Mathematics Department
University of Michigan
Ann Arbor, MI 48109
USA

K. A. Ribet
Department of Mathematics
East Hall University of
California at Berkeley
Berkeley, CA 94720-3840
USA

Mathematics Subject Classification (1991): 14-01, 13-01, 13Pxx

Library of Congress Cataloging-in-Publication Data

Cox, David A.

Using algebraic geometry / David A. Cox, John B. Little, Donal B. O'Shea.

p. cm. — (Graduate texts in mathematics ; 185)

Includes bibliographical references (p. —) and index.

ISBN 978-0-387-98492-6

ISBN 978-1-4757-6911-1 (eBook)

DOI 10.1007/978-1-4757-6911-1

I. Geometry, Algebraic. I. Little, John B. II. O'Shea, Donal,

III. Title. IV. Series.

QA564.C6883 1998

516.3'5—dc21

98-11964

Printed on acid-free paper.

© 1998 Springer Science+Business Media New York

Originally published by Springer-Verlag New York, Inc. in 1998

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher Springer Science+Business Media, LLC, except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production managed by Timothy Taylor; manufacturing supervised by Jacqui Ashri.

Camera-ready copy prepared from the authors' \LaTeX files.

9 8 7 6 5 4 3 2 1

ISBN 978-0-387-98492-6

*To Elaine,
for her love and support.
D.A.C.*

*To my mother and the memory of my father.
J.B.L.*

*To my parents.
D.O'S.*

Preface

In recent years, the discovery of new algorithms for dealing with polynomial equations, coupled with their implementation on inexpensive yet fast computers, has sparked a minor revolution in the study and practice of algebraic geometry. These algorithmic methods and techniques have also given rise to some exciting new applications of algebraic geometry.

One of the goals of *Using Algebraic Geometry* is to illustrate the many uses of algebraic geometry and to highlight the more recent applications of Gröbner bases and resultants. In order to do this, we also provide an introduction to some algebraic objects and techniques more advanced than one typically encounters in a first course, but which are nonetheless of great utility. Finally, we wanted to write a book which would be accessible to nonspecialists and to readers with a diverse range of backgrounds.

To keep the book reasonably short, we often have to refer to basic results in algebraic geometry without proof, although complete references are given. For readers learning algebraic geometry and Gröbner bases for the first time, we would recommend that they read this book in conjunction with one of the following introductions to these subjects:

- *Introduction to Gröbner Bases*, by Adams and Loustaunau [AL]
- *Gröbner Bases*, by Becker and Weispfenning [BW]
- *Ideals, Varieties and Algorithms*, by Cox, Little and O'Shea [CLO]

We have tried, on the other hand, to keep the exposition self-contained outside of references to these introductory texts. We have made no effort at completeness, and have not hesitated to point out the reader to the research literature for more information.

Later in the preface we will give a brief summary of what our book covers.

The Level of the Text

This book is written at the graduate level and hence assumes the reader knows the material covered in standard undergraduate courses, including abstract algebra. But because the text is intended for beginning graduate

students, it does not require graduate algebra, and in particular, the book does not assume that the reader is familiar with modules. Being a graduate text, *Using Algebraic Geometry* covers more sophisticated topics and has a denser exposition than most undergraduate texts, including our previous book [CLO].

However, it is possible to use this book at the undergraduate level, provided proper precautions are taken. With the exception of the first two chapters, we found that most undergraduates needed help reading preliminary versions of the text. That said, if one supplements the other chapters with simpler exercises and fuller explanations, many of the applications we cover make good topics for an upper-level undergraduate applied algebra course. Similarly, the book could also be used for reading courses or senior theses at this level. We hope that our book will encourage instructors to find creative ways for involving advanced undergraduates in this wonderful mathematics.

How to Use the Text

The book covers a variety of topics, which can be grouped roughly as follows:

- Chapters 1 and 2: Gröbner bases, including basic definitions, algorithms and theorems, together with solving equations, eigenvalue methods, and solutions over \mathbb{R} .
- Chapters 3 and 7: Resultants, including multipolynomial and sparse resultants as well as their relation to polytopes, mixed volumes, toric varieties, and solving equations.
- Chapters 4, 5 and 6: Commutative algebra, including local rings, standard bases, modules, syzygies, free resolutions, Hilbert functions and geometric applications.
- Chapters 8 and 9: Applications, including integer programming, combinatorics, polynomial splines, and algebraic coding theory.

One unusual feature of the book's organization is the early introduction of resultants in Chapter 3. This is because there are many applications where resultant methods are much more efficient than Gröbner basis methods. While Gröbner basis methods have had a greater theoretical impact on algebraic geometry, resultants appear to have an advantage when it comes to practical applications. There is also some lovely mathematics connected with resultants.

There is a large degree of independence among most chapters of the book. This implies that there are many ways the book can be used in teaching a course. Since there is more material than can be covered in one semester, some choices are necessary. Here are three examples of how to structure a course using our text.

- **Solving Equations.** This course would focus on the use of Gröbner bases and resultants to solve systems of polynomial equations. Chapters 1, 2, 3 and 7 would form the heart of the course. Special emphasis would be placed on §5 of Chapter 2, §5 and §6 of Chapter 3, and §6 of Chapter 7. Optional topics would include §1 and §2 of Chapter 4, which discuss multiplicities.
- **Commutative Algebra.** Here, the focus would be on topics from classical commutative algebra. The course would follow Chapters 1, 2, 4, 5 and 6, skipping only those parts of §2 of Chapter 4 which deal with resultants. The final section of Chapter 6 is a nice ending point for the course.
- **Applications.** A course concentrating on applications would cover integer programming, combinatorics, splines and coding theory. After a quick trip through Chapters 1 and 2, the main focus would be Chapters 8 and 9. Chapter 8 uses some ideas about polytopes from §1 of Chapter 7, and modules appear naturally in Chapters 8 and 9. Hence the first two sections of Chapter 5 would need to be covered. Also, Chapters 8 and 9 use Hilbert functions, which can be found in either Chapter 6 of this book or Chapter 9 of [CLO].

We want to emphasize that these are only three of many ways of using the text. We would be very interested in hearing from instructors who have found other paths through the book.

References

References to the bibliography at the end of the book are by the first three letters of the author's last name (e.g., [Hil] for Hilbert), with numbers for multiple papers by the same author (e.g., [Mac1] for the first paper by Macaulay). When there is more than one author, the first letters of the authors' last names are used (e.g., [BE] for Buchsbaum and Eisenbud), and when several sets of authors have the same initials, other letters are used to distinguish them (e.g., [BoF] is by Bonnesen and Fenchel, while [BuF] is by Burden and Faires).

The bibliography lists books alphabetically by the full author's name, followed (if applicable) by any coauthors. This means, for instance, that [BS] by Billera and Sturmfels is listed before [Bl] by Blahut.

Comments and Corrections

We encourage comments, criticism, and corrections. Please send them to any of us:

| | |
|-------------|---------------------------|
| David Cox | dac@cs.amherst.edu |
| John Little | little@math.holycross.edu |
| Don O'Shea | doshea@mhc.mtholyoke.edu |

For each new typo or error, we will pay \$1 to the first person who reports it to us. We also encourage readers to check out the web site for *Using Algebraic Geometry*, which is at

<http://www.cs.amherst.edu/~dac/uag.html>

This site includes updates and errata sheets, as well as links to other sites of interest.

Acknowledgments

We would like to thank everyone who sent us comments on initial drafts of the manuscript. We are especially grateful to thank Susan Colley, Alicia Dickenstein, Ioannis Emiris, Tom Garrity, Pat Fitzpatrick, Gert-Martin Greuel, Paul Pedersen, Maurice Rojas, Jerry Shurman, Michael Singer, Michael Stanfield, Bernd Sturmfels (and students), Moss Sweedler (and students), Wiland Schmale, and Cynthia Woodburn for especially detailed comments and criticism.

We also gratefully acknowledge the support provided by National Science Foundation grant DUE-9666132, and the help and advice afforded by the members of our Advisory Board: Susan Colley, Keith Devlin, Arnie Ostebee, Bernd Sturmfels, and Jim White.

November, 1997

*David Cox
John Little
Donal O'Shea*

Contents

| | |
|--|------------|
| Preface | vii |
| Chapter 1. Introduction | 1 |
| §1. Polynomials and Ideals | 1 |
| §2. Monomial Orders and Polynomial Division | 6 |
| §3. Gröbner Bases | 11 |
| §4. Affine Varieties | 16 |
| Chapter 2. Solving Polynomial Equations | 24 |
| §1. Solving Polynomial Systems by Elimination | 24 |
| §2. Finite-Dimensional Algebras | 34 |
| §3. Gröbner Basis Conversion | 46 |
| §4. Solving Equations via Eigenvalues | 51 |
| §5. Real Root Location and Isolation | 63 |
| Chapter 3. Resultants | 71 |
| §1. The Resultant of Two Polynomials | 71 |
| §2. Multipolynomial Resultants | 78 |
| §3. Properties of Resultants | 89 |
| §4. Computing Resultants | 96 |
| §5. Solving Equations Via Resultants | 108 |
| §6. Solving Equations via Eigenvalues | 122 |
| Chapter 4. Computation in Local Rings | 130 |
| §1. Local Rings | 130 |
| §2. Multiplicities and Milnor Numbers | 138 |
| §3. Term Orders and Division in Local Rings | 151 |
| §4. Standard Bases in Local Rings | 164 |

| | |
|---|------------|
| Chapter 5. Modules | 179 |
| §1. Modules over Rings | 179 |
| §2. Monomial Orders and Gröbner Bases for Modules | 197 |
| §3. Computing Syzygies | 210 |
| §4. Modules over Local Rings | 222 |
| Chapter 6. Free Resolutions | 234 |
| §1. Presentations and Resolutions of Modules | 234 |
| §2. Hilbert's Syzygy Theorem | 245 |
| §3. Graded Resolutions | 252 |
| §4. Hilbert Polynomials and Geometric Applications | 266 |
| Chapter 7. Polytopes, Resultants, and Equations | 290 |
| §1. Geometry of Polytopes | 290 |
| §2. Sparse Resultants | 298 |
| §3. Toric Varieties | 306 |
| §4. Minkowski Sums and Mixed Volumes | 316 |
| §5. Bernstein's Theorem | 327 |
| §6. Computing Resultants and Solving Equations | 342 |
| Chapter 8. Integer Programming, Combinatorics, and Splines | 359 |
| §1. Integer Programming | 359 |
| §2. Integer Programming and Combinatorics | 374 |
| §3. Multivariate Polynomial Splines | 385 |
| Chapter 9. Algebraic Coding Theory | 407 |
| §1. Finite Fields | 407 |
| §2. Error-Correcting Codes | 415 |
| §3. Cyclic Codes | 424 |
| §4. Reed-Solomon Decoding Algorithms | 435 |
| §5. Codes from Algebraic Geometry | 448 |
| References | 468 |
| Index | 477 |