

Undergraduate Texts in Mathematics

Editors

S. Axler

F.W. Gehring

P.R. Halmos

Springer Science+Business Media, LLC

Undergraduate Texts in Mathematics

- Anglin:** Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
- Anglin/Lambek:** The Heritage of Thales.
Readings in Mathematics.
- Apostol:** Introduction to Analytic Number Theory.
Second edition.
- Armstrong:** Basic Topology.
- Armstrong:** Groups and Symmetry.
- Axler:** Linear Algebra Done Right.
- Bak/Newman:** Complex Analysis. Second edition.
- Banchoff/Wermer:** Linear Algebra Through Geometry. Second edition.
- Berberian:** A First Course in Real Analysis.
- Brémaud:** An Introduction to Probabilistic Modeling.
- Bressoud:** Factorization and Primality Testing.
- Bressoud:** Second Year Calculus.
Readings in Mathematics.
- Brickman:** Mathematical Introduction to Linear Programming and Game Theory.
- Browder:** Mathematical Analysis: An Introduction.
- Cederberg:** A Course in Modern Geometries.
- Childs:** A Concrete Introduction to Higher Algebra.
Second edition.
- Chung:** Elementary Probability Theory with Stochastic Processes. Third edition.
- Cox/Little/O'Shea:** Ideals, Varieties, and Algorithms. Second edition.
- Croom:** Basic Concepts of Algebraic Topology.
- Curtis:** Linear Algebra: An Introductory Approach.
Fourth edition.
- Devlin:** The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
- Dixmier:** General Topology.
- Driver:** Why Math?
- Ebbinghaus/Flum/Thomas:** Mathematical Logic.
Second edition.
- Edgar:** Measure, Topology, and Fractal Geometry. Elaydi: Introduction to Difference Equations.
- Exner:** An Accompaniment to Higher Mathematics.
- Fischer:** Intermediate Real Analysis.
- Flanigan/Kazdan:** Calculus Two: Linear and Nonlinear Functions. Second edition.
- Fleming:** Functions of Several Variables. Second edition.
- Foulds:** Combinatorial Optimization for Undergraduates.
- Foulds:** Optimization Techniques: An Introduction.
- Franklin:** Methods of Mathematical Economics.
- Hairer/Wanner:** Analysis by Its History.
Readings in Mathematics.
- Halmos:** Finite-Dimensional Vector Spaces. Second edition.
- Halmos:** Naive Set Theory.
- Hämmerlin/Hoffmann:** Numerical Mathematics.
Readings in Mathematics.
- Hilton/Holton/Pedersen:** Mathematical Reflections: In a Room with Many Mirrors.
- Iooss/Joseph:** Elementary Stability and Bifurcation Theory. Second edition.
- Isaac:** The Pleasures of Probability.
Readings in Mathematics.
- James:** Topological and Uniform Spaces.
- Jänich:** Linear Algebra.
- Jänich:** Topology.
- Kemeny/Snell:** Finite Markov Chains.
- Kinsey:** Topology of Surfaces.
- Klambauer:** Aspects of Calculus.
- Lang:** A First Course in Calculus. Fifth edition.
- Lang:** Calculus of Several Variables. Third edition.
- Lang:** Introduction to Linear Algebra. Second edition.
- Lang:** Linear Algebra. Third edition.
- Lang:** Undergraduate Algebra. Second edition.
- Lang:** Undergraduate Analysis.
- Lax/Burstein/Lax:** Calculus with Applications and Computing. Volume 1.
- LeCuyer:** College Mathematics with APL.
- Lidl/Pilz:** Applied Abstract Algebra.
- Macki-Strauss:** Introduction to Optimal Control Theory.
- Malitz:** Introduction to Mathematical Logic.
- Marsden/Weinstein:** Calculus I, II, III. Second edition.
- Martin:** The Foundations of Geometry and the Non-Euclidean Plane.
- Martin:** Transformation Geometry: An Introduction to Symmetry.
- Millman/Parker:** Geometry: A Metric Approach with Models. Second edition.
- Moschovakis:** Notes on Set Theory.
- Owen:** A First Course in the Mathematical Foundations of Thermodynamics.
- Palka:** An Introduction to Complex Function Theory.
- Pedrick:** A First Course in Analysis.
- Peressini/Sullivan/Uhl:** The Mathematics of Nonlinear Programming.

(continued after index)

David Cox John Little Donal O'Shea

Ideals, Varieties, and Algorithms

An Introduction to Computational Algebraic
Geometry and Commutative Algebra

Second Edition

With 91 Illustrations

Springer

世界图书出版公司

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
Department of
Mathematics
Michigan State University
East Lansing, MI 48824
USA

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

P.R. Halmos
Department of
Mathematics
Santa Clara University
Santa Clara, CA 95053
USA

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

Library of Congress Cataloging-in-Publication Data
Cox, David A.

Ideals, varieties, and algorithms : an introduction to
computational algebraic geometry and commutative algebra / by David
Cox, John Little, Donal O'Shea. — 2nd ed.

p. cm.—(Undergraduate texts in mathematics)

Includes bibliographical references (p. —) and index.

1. Geometry, Algebraic—Data processing. 2. Commutative algebra—
Data processing. I. Little, John B. II. O'Shea, Donal.

III. Title. IV. Series.

QA564.C688 1996

516.3'5—dc20

96-8023

ISBN 978-1-4757-2695-4 ISBN 978-1-4757-2693-0 (eBook)

DOI 10.1007/978-1-4757-2693-0

© 1997, 1992 Springer Science+Business Media New York

Originally published by Springer-Verlag New York, Inc in 1997.

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.

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the People's Republic of China only and not for export therefrom.

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

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

*To Mary and my children.
D.O'S.*

Preface to the First Edition

We wrote this book to introduce undergraduates to some interesting ideas in algebraic geometry and commutative algebra. Until recently, these topics involved a lot of abstract mathematics and were only taught in graduate school. But in the 1960s, Buchberger and Hironaka discovered new algorithms for manipulating systems of polynomial equations. Fueled by the development of computers fast enough to run these algorithms, the last two decades have seen a minor revolution in commutative algebra. The ability to compute efficiently with polynomial equations has made it possible to investigate complicated examples that would be impossible to do by hand, and has changed the practice of much research in algebraic geometry. This has also enhanced the importance of the subject for computer scientists and engineers, who have begun to use these techniques in a whole range of problems.

It is our belief that the growing importance of these computational techniques warrants their introduction into the undergraduate (and graduate) mathematics curriculum. Many undergraduates enjoy the concrete, almost nineteenth-century, flavor that a computational emphasis brings to the subject. At the same time, one can do some substantial mathematics, including the Hilbert Basis Theorem, Elimination Theory, and the Nullstellensatz.

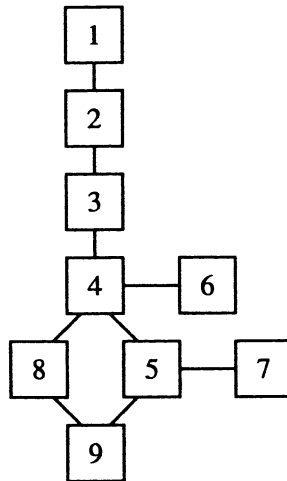
The mathematical prerequisites of the book are modest: the students should have had a course in linear algebra and a course where they learned how to do proofs. Examples of the latter sort of course include discrete math and abstract algebra. It is important to note that abstract algebra is *not* a prerequisite. On the other hand, if all of the students have had abstract algebra, then certain parts of the course will go much more quickly.

The book assumes that the students will have access to a computer algebra system. Appendix C describes the features of AXIOM, Maple, Mathematica, and REDUCE that are most relevant to the text. We do not assume any prior experience with a computer. However, many of the algorithms in the book are described in pseudocode, which may be unfamiliar to students with no background in programming. Appendix B contains a careful description of the pseudocode that we use in the text.

In writing the book, we tried to structure the material so that the book could be used in a variety of courses, and at a variety of different levels. For instance, the book could serve as a basis of a second course in undergraduate abstract algebra, but we think that it just as easily could provide a credible alternative to the first course. Although the book is aimed primarily at undergraduates, it could also be used in various graduate courses, with some supplements. In particular, beginning graduate courses in algebraic geometry or computational algebra may find the text useful. We hope, of course, that

mathematicians and colleagues in other disciplines will enjoy reading the book as much as we enjoyed writing it.

The first four chapters form the core of the book. It should be possible to cover them in a 14-week semester, and there may be some time left over at the end to explore other parts of the text. The follows chart explains the logical dependence of the chapters:



See the table of contents for a description of what is covered in each chapter. As the chart indicates, there are a variety of ways to proceed after covering the first four chapters. Also, a two-semester course could be designed that covers the entire book. For instructors interested in having their students do an independent project, we have included a list of possible topics in Appendix D.

It is a pleasure to thank the New England Consortium for Undergraduate Science Education (and its parent organization, the Pew Charitable Trusts) for providing the major funding for this work. The project would have been impossible without their support. Various aspects of our work were also aided by grants from IBM and the Sloan Foundation, the Alexander von Humboldt Foundation, the Department of Education's FIPSE program, the Howard Hughes Foundation, and the National Science Foundation. We are grateful for their help.

We also wish to thank colleagues and students at Amherst College, George Mason University, Holy Cross College, Massachusetts Institute of Technology, Mount Holyoke College, Smith College, and the University of Massachusetts who participated in courses based on early versions of the manuscript. Their feedback improved the book considerably. Many other colleagues have contributed suggestions, and we thank you all.

Corrections, comments and suggestions for improvement are welcome!

November 1991

*David Cox
John Little
Donal O'Shea*

Preface to the Second Edition

In preparing a new edition of *Ideals, Varieties, and Algorithms*, our goal was to correct some of the omissions of the first edition while maintaining the readability and accessibility of the original. The major changes in the second edition are as follows:

- Chapter 2: A better acknowledgement of Buchberger's contributions and an improved proof of the Buchberger Criterion in §6.
- Chapter 5: An improved bound on the number of solutions in §3 and a new §6 which completes the proof of the Closure Theorem begun in Chapter 3.
- Chapter 8: A complete proof of the Projection Extension Theorem in §5 and a new §7 which contains a proof of Bezout's Theorem.
- Appendix C: a new section on AXIOM and an update on what we say about Maple, Mathematica, and REDUCE.

Finally, we fixed some typographical errors, improved and clarified notation, and updated the bibliography by adding many new references.

We also want to take this opportunity to acknowledge our debt to the many people who influenced us and helped us in the course of this project. In particular, we would like to thank:

- David Bayer and Monique Lejeune-Jalabert, whose thesis BAYER (1982) and notes LEJEUNE-JALABERT (1985) first acquainted us with this wonderful subject.
 - Frances Kirwan, whose book KIRWAN (1992) convinced us to include Bezout's Theorem in Chapter 8.
 - Steven Kleiman, who showed us how to prove the Closure Theorem in full generality. His proof appears in Chapter 5.
 - Michael Singer, who suggested improvements in Chapter 5, including the new Proposition 8 of §3.
 - Bernd Sturmfels, whose book STURMFELS (1993) was the inspiration for Chapter 7.
- There are also many individuals who found numerous typographical errors and gave us feedback on various aspects of the book. We are grateful to you all!

As with the first edition, we welcome comments and suggestions, and we pay \$1 for every new typographical error.

October 1996

*David Cox
John Little
Donal O'Shea*

Contents

Preface to the First Edition	vii
Preface to the Second Edition	ix
1. Geometry, Algebra, and Algorithms	1
§1. Polynomials and Affine Space	1
§2. Affine Varieties	5
§3. Parametrizations of Affine Varieties	14
§4. Ideals	29
§5. Polynomials of One Variable	37
2. Groebner Bases	47
§1. Introduction	47
§2. Orderings on the Monomials in $k[x_1, \dots, x_n]$	52
§3. A Division Algorithm in $k[x_1, \dots, x_n]$	59
§4. Monomial Ideals and Dickson's Lemma	67
§5. The Hilbert Basis Theorem and Groebner Bases	73
§6. Properties of Groebner Bases	79
§7. Buchberger's Algorithm	86
§8. First Applications of Groebner Bases	93
§9. (Optional) Improvements on Buchberger's Algorithm	99
3. Elimination Theory	112
§1. The Elimination and Extension Theorems	112
§2. The Geometry of Elimination	120
§3. Implicitization	124
§4. Singular Points and Envelopes	133
§5. Unique Factorization and Resultants	146
§6. Resultants and the Extension Theorem	158

4. The Algebra–Geometry Dictionary	167
§1. Hilbert’s Nullstellensatz	167
§2. Radical Ideals and the Ideal–Variety Correspondence	173
§3. Sums, Products, and Intersections of Ideals	180
§4. Zariski Closure and Quotients of Ideals	190
§5. Irreducible Varieties and Prime Ideals	195
§6. Decomposition of a Variety into Irreducibles	200
§7. (Optional) Primary Decomposition of Ideals	206
§8. Summary	210
5. Polynomial and Rational Functions on a Variety	212
§1. Polynomial Mappings	212
§2. Quotients of Polynomial Rings	218
§3. Algorithmic Computations in $k[x_1, \dots, x_n]/I$	226
§4. The Coordinate Ring of an Affine Variety	235
§5. Rational Functions on a Variety	245
§6. (Optional) Proof of the Closure Theorem	254
6. Robotics and Automatic Geometric Theorem Proving	261
§1. Geometric Description of Robots	261
§2. The Forward Kinematic Problem	267
§3. The Inverse Kinematic Problem and Motion Planning	274
§4. Automatic Geometric Theorem Proving	286
§5. Wu’s Method	302
7. Invariant Theory of Finite Groups	311
§1. Symmetric Polynomials	311
§2. Finite Matrix Groups and Rings of Invariants	321
§3. Generators for the Ring of Invariants	329
§4. Relations Among Generators and the Geometry of Orbits	338
8. Projective Algebraic Geometry	349
§1. The Projective Plane	349
§2. Projective Space and Projective Varieties	360
§3. The Projective Algebra–Geometry Dictionary	370
§4. The Projective Closure of an Affine Variety	378
§5. Projective Elimination Theory	384
§6. The Geometry of Quadric Hypersurfaces	399
§7. Bezout’s Theorem	412
9. The Dimension of a Variety	429
§1. The Variety of a Monomial Ideal	429
§2. The Complement of a Monomial Ideal	433

§3. The Hilbert Function and the Dimension of a Variety	446
§4. Elementary Properties of Dimension	457
§5. Dimension and Algebraic Independence	465
§6. Dimension and Nonsingularity	473
§7. The Tangent Cone	483
Appendix A. Some Concepts from Algebra	497
§1. Fields and Rings	497
§2. Groups	498
§3. Determinants	499
Appendix B. Pseudocode	501
§1. Inputs, Outputs, Variables, and Constants	501
§2. Assignment Statements	502
§3. Looping Structures	502
§4. Branching Structures	503
Appendix C. Computer Algebra Systems	505
§1. AXIOM	505
§2. Maple	508
§3. Mathematica	510
§4. REDUCE	512
§5. Other Systems	516
Appendix D. Independent Projects	518
§1. General Comments	518
§2. Suggested Projects	518
References	523
Index	527