Undergraduate Texts in Mathematics

David Cox
John Little
Donal O'Shea

Ideals, Varieties, and Algorithms

An Introduction to Computational Algebraic Geometry and Commutative Algebra

Third Edition

理想、簇与算法 第3版

Springer

世界图书出版公司
www.wpcbj.com.cn

David Cox John Little Donal O'Shea

Ideals, Varieties, and Algorithms

An Introduction to Computational Algebraic Geometry and Commutative Algebra

Third Edition

Springer

图书在版编目（CIP）数据

理想、簇与算法 = Ideals，varieties，and algorithms：第3版：英文/（美）考克斯（Cox，D.）著．—影印本．—北京：世界图书出版公司北京公司，2013.3
ISBN 978-7-5100-5840-0

Ⅰ．①理…　Ⅱ．①考…　Ⅲ．①理想（数学）—高等学校—教材—英文②簇—高等学校—教材—英文　Ⅳ．①O15②O187.2

中国版本图书馆CIP数据核字（2013）第035241号

书　　名：	Ideals，Varieties，and Algorithms：An Introduction to Computational Algebraic Geometry and Commutative Algebra 3rd ed.
作　　者：	David Cox，John Little and Donal O'Shea
中 译 名：	理想、簇与算法 第3版
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河市国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街137号 100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@wpcbj.com.cn
开　　本：	24开
印　　张：	24
版　　次：	2013年3月
版权登记：	图字：01-2012-857
书　　号：	978-7-5100-5840-0
定　　价：	89.00元

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

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

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

ISBN: 978-0-387-35650-1 e-ISBN: 978-0-387-35651-8

Library of Congress Control Number: 2006930875

Mathematics Subject Classification (2000): 14-01, 13-01, 13Pxx

Reprint from English language edition:

Ideals, Varieties, and Algorithms

by David Cox, John Little and Donal O' Shea

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.

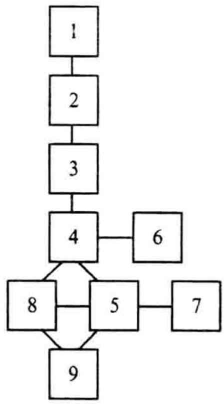
It is our belief that the growing importance of these computational techniques warrants their introduction into the undergraduate (and graduate) mathematics curriculum. Many undergraduates enjoy the concrete, almost nineteenth-century, flavor that a computational emphasis brings to the subject. At the 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 following 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. For a list of errors and other information relevant to the book, see our web site `http://www.cs.amherst.edu/~dac/iva.html`.

October 1996

David Cox
John Little
Donal O'Shea

Preface to the Third Edition

The new features of the third edition of *Ideals, Varieties, and Algorithms* are as follows:

- A significantly shorter proof of the Extension Theorem is presented in §6 of Chapter 3. We are grateful to A. H. M. Levelt for bringing this argument to our attention.
- A major update of the section on Maple appears in Appendix C. We also give updated information on AXIOM, CoCoA, Macaulay 2, Magma, Mathematica, and SINGULAR.
- Changes have been made on over 200 pages to enhance clarity and correctness.

We are also grateful to the many individuals who reported typographical errors and gave us feedback on the earlier editions. Thank you all!

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

November, 2006

David Cox
John Little
Donal O'Shea

Undergraduate Texts in Mathematics

Undergraduate Texts in Mathematics

Abbott: Understanding Analysis.
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. Second edition.
Beardon: Limits: A New Approach to Real Analysis.
Bak/Newman: Complex Analysis. Second edition.
Banchoff/Wermer: Linear Algebra Through Geometry. Second edition.
Berberian: A First Course in Real Analysis.
Bix: Conics and Cubics: A Concrete Introduction to Algebraic Curves.
Brèmaud: 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.
Buchmann: Introduction to Cryptography. Second edition.
Buskes/van Rooij: Topological Spaces: From Distance to Neighborhood.
Callahan: The Geometry of Spacetime: An Introduction to Special and General Relavitity.
Carter/van Brunt: The Lebesgue– Stieltjes Integral: A Practical Introduction.
Cederberg: A Course in Modern Geometries. Second edition.
Chambert-Loir: A Field Guide to Algebra
Childs: A Concrete Introduction to Higher Algebra. Second edition.
Chung/AitSahlia: Elementary Probability Theory: With Stochastic Processes and an Introduction to Mathematical Finance. Fourth edition.
Cox/Little/O'Shea: Ideals, Varieties, and Algorithms. Third edition.
Croom: Basic Concepts of Algebraic Topology.
Cull/Flahive/Robson: Difference Equations. From Rabbits to Chaos.
Curtis: Linear Algebra: An Introductory Approach. Fourth edition.
Daepp/Gorkin: Reading, Writing, and Proving: A Closer Look at Mathematics.
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: An Introduction to Difference Equations. Third edition.
Erdõs/Surányi: Topics in the Theory of Numbers.
Estep: Practical Analysis on One Variable.
Exner: An Accompaniment to Higher Mathematics.
Exner: Inside Calculus.
Fine/Rosenberger: The Fundamental Theory of Algebra.
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.
Frazier: An Introduction to Wavelets Through Linear Algebra.
Gamelin: Complex Analysis.
Ghorpade/Limaye: A Course in Calculus and Real Analysis.
Gordon: Discrete Probability.
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.
Harris/Hirst/Mossinghoff: Combinatorics and Graph Theory.
Hartshorne: Geometry: Euclid and Beyond.
Hijab: Introduction to Calculus and Classical Analysis.
Hilton/Holton/Pedersen: Mathematical Reflections: In a Room with Many Mirrors.
Hilton/Holton/Pedersen: Mathematical Vistas: From a Room with Many Windows.

(continued after index)

Contents

Preface to the First Edition vii

Preface to the Second Edition ix

Preface to the Third Edition xi

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 38

2. Groebner Bases 49

§1. Introduction 49
§2. Orderings on the Monomials in $k[x_1, \ldots, x_n]$ 54
§3. A Division Algorithm in $k[x_1, \ldots, x_n]$ 61
§4. Monomial Ideals and Dickson's Lemma 69
§5. The Hilbert Basis Theorem and Groebner Bases 75
§6. Properties of Groebner Bases 82
§7. Buchberger's Algorithm 88
§8. First Applications of Groebner Bases 95
§9. (Optional) Improvements on Buchberger's Algorithm 102

3. Elimination Theory 115

§1. The Elimination and Extension Theorems 115
§2. The Geometry of Elimination 123
§3. Implicitization 128
§4. Singular Points and Envelopes 137
§5. Unique Factorization and Resultants 150
§6. Resultants and the Extension Theorem 162

4. The Algebra–Geometry Dictionary 169

§1. Hilbert's Nullstellensatz 169
§2. Radical Ideals and the Ideal–Variety Correspondence 175
§3. Sums, Products, and Intersections of Ideals 183
§4. Zariski Closure and Quotients of Ideals 193
§5. Irreducible Varieties and Prime Ideals 198
§6. Decomposition of a Variety into Irreducibles 204
§7. (Optional) Primary Decomposition of Ideals 210
§8. Summary 214

5. Polynomial and Rational Functions on a Variety 215

§1. Polynomial Mappings 215
§2. Quotients of Polynomial Rings 221
§3. Algorithmic Computations in $k[x_1, \ldots, x_n]/I$ 230
§4. The Coordinate Ring of an Affine Variety 239
§5. Rational Functions on a Variety 248
§6. (Optional) Proof of the Closure Theorem 258

6. Robotics and Automatic Geometric Theorem Proving 265

§1. Geometric Description of Robots 265
§2. The Forward Kinematic Problem 271
§3. The Inverse Kinematic Problem and Motion Planning 279
§4. Automatic Geometric Theorem Proving 291
§5. Wu's Method 307

7. Invariant Theory of Finite Groups 317

§1. Symmetric Polynomials 317
§2. Finite Matrix Groups and Rings of Invariants 327
§3. Generators for the Ring of Invariants 336
§4. Relations Among Generators and the Geometry of Orbits 345

8. Projective Algebraic Geometry 357

§1. The Projective Plane 357
§2. Projective Space and Projective Varieties 368
§3. The Projective Algebra–Geometry Dictionary 379
§4. The Projective Closure of an Affine Variety 386
§5. Projective Elimination Theory 393
§6. The Geometry of Quadric Hypersurfaces 408
§7. Bezout's Theorem 422

9. The Dimension of a Variety 439

§1. The Variety of a Monomial Ideal 439
§2. The Complement of a Monomial Ideal 443

§3. The Hilbert Function and the Dimension of a Variety 456
§4. Elementary Properties of Dimension 468
§5. Dimension and Algebraic Independence 477
§6. Dimension and Nonsingularity 484
§7. The Tangent Cone 495

Appendix A. Some Concepts from Algebra **509**

§1. Fields and Rings 509
§2. Groups 510
§3. Determinants 511

Appendix B. Pseudocode **513**

§1. Inputs, Outputs, Variables, and Constants 513
§2. Assignment Statements 514
§3. Looping Structures 514
§4. Branching Structures 515

Appendix C. Computer Algebra Systems **517**

§1. AXIOM 517
§2. Maple 520
§3. Mathematica 522
§4. REDUCE 524
§5. Other Systems 528

Appendix D. Independent Projects **530**

§1. General Comments 530
§2. Suggested Projects 530

References **535**

Index **541**

1

Geometry, Algebra, and Algorithms

This chapter will introduce some of the basic themes of the book. The geometry we are interested in concerns *affine varieties*, which are curves and surfaces (and higher dimensional objects) defined by polynomial equations. To understand affine varieties, we will need some algebra, and in particular, we will need to study *ideals* in the polynomial ring $k[x_1, \ldots, x_n]$. Finally, we will discuss polynomials in one variable to illustrate the role played by *algorithms*.

§1 Polynomials and Affine Space

To link algebra and geometry, we will study polynomials over a field. We all know what polynomials are, but the term *field* may be unfamiliar. The basic intuition is that a field is a set where one can define addition, subtraction, multiplication, and division with the usual properties. Standard examples are the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$, whereas the integers $\mathbb{Z}$ are not a field since division fails (3 and 2 are integers, but their quotient 3/2 is not). A formal definition of field may be found in Appendix A.

One reason that fields are important is that linear algebra works over *any* field. Thus, even if your linear algebra course restricted the scalars to lie in $\mathbb{R}$ or $\mathbb{C}$, most of the theorems and techniques you learned apply to an arbitrary field k. In this book, we will employ different fields for different purposes. The most commonly used fields will be:

- The rational numbers $\mathbb{Q}$: the field for most of our computer examples.
- The real numbers $\mathbb{R}$: the field for drawing pictures of curves and surfaces.
- The complex numbers $\mathbb{C}$: the field for proving many of our theorems.

On occasion, we will encounter other fields, such as fields of rational functions (which will be defined later). There is also a very interesting theory of finite fields—see the exercises for one of the simpler examples.

We can now define polynomials. The reader certainly is familiar with polynomials in one and two variables, but we will need to discuss polynomials in n variables $x_1, \ldots, x_n$ with coefficients in an arbitrary field k. We start by defining monomials.

Definition 1. *A* **monomial** *in $x_1, \ldots, x_n$ is a product of the form*

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. The **total degree** *of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$.*

We can simplify the notation for monomials as follows: let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an n-tuple of nonnegative integers. Then we set

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

When $\alpha = (0, \ldots, 0)$, note that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1 + \cdots + \alpha_n$ denote the total degree of the monomial x^α.

Definition 2. *A* **polynomial** *f in $x_1, \ldots, x_n$ with coefficients in k is a finite linear combination (with coefficients in k) of monomials. We will write a polynomial f in the form*

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in k,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

When dealing with polynomials in a small number of variables, we will usually dispense with subscripts. Thus, polynomials in one, two, and three variables lie in $k[x]$, $k[x, y]$ and $k[x, y, z]$, respectively. For example,

$$f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$$

is a polynomial in $\mathbb{Q}[x, y, z]$. We will usually use the letters f, g, h, p, q, r to refer to polynomials.

We will use the following terminology in dealing with polynomials.

Definition 3. *Let $f = \Sigma_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, \ldots, x_n]$.*

(i) *We call a_α the* **coefficient** *of the monomial x^α.*
(ii) *If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a* **term** *of f.*
(iii) *The* **total degree** *of f, denoted* $\deg(f)$, *is the maximum $|\alpha|$ such that the coefficient a_α is nonzero.*

As an example, the polynomial $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ given above has four terms and total degree six. Note that there are two terms of maximal total degree, which is something that cannot happen for polynomials of one variable. In Chapter 2, we will study how to *order* the terms of a polynomial.

The sum and product of two polynomials is again a polynomial. We say that a polynomial f *divides* a polynomial g provided that $g = fh$ for some $h \in k[x_1, \ldots, x_n]$.

One can show that, under addition and multiplication, $k[x_1, \ldots, x_n]$ satisfies all of the field axioms except for the existence of multiplicative inverses (because, for example, $1/x_1$ is not a polynomial). Such a mathematical structure is called a commutative ring