Graduate Texts in Mathematics

David A. Cox
John Little
Donal O′Shea

Using Algebraic Geometry

Second Edition

代数几何应用 第2版

Springer

世界图书出版公司
www.wpcbj.com.cn

David A. Cox
John Little
Donal O'Shea

Using Algebraic Geometry

Second Edition

With 24 Illustrations

Springer

图书在版编目（CIP）数据

代数几何应用：第 2 版 = Using Algebraic Geometry 2nd ed：英文/（美）考克斯（Cox，D. A.）著．—影印本．—北京：世界图书出版公司北京公司，2012. 9
ISBN 978 - 7 - 5100 - 5285 - 9

Ⅰ.①代…　Ⅱ.①考…　Ⅲ.①代数几何—应用—英文　Ⅳ.①O187

中国版本图书馆 CIP 数据核字（2012）第 217109 号

书　　名：	Using Algebraic Geometry 2nd ed.
作　　者：	David A. Cox，John Little，Donal O' Shea
中 译 名：	代数几何应用 第 2 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. 5
版　　次：	2013 年 1 月
版权登记：	图字：01 - 2012 - 5880
书　　号：	978 - 7 - 5100 - 5285 - 9　　定　　价：　95. 00 元

Graduate Texts in Mathematics 185

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. 2nd ed.
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 J.-P. 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 J.-P. 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.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.

(continued after index)

Preface to the Second Edition

Since the first edition of *Using Algebraic Geometry* was published in 1998, the field of computational algebraic geometry and its applications has developed rapidly. Many new results concerning topics we discussed have appeared. Moreover, a number of new introductory texts have been published. Our goals in this revision have been to update the references to reflect these additions to the literature, to add discussions of some new material, to improve some of the proofs, and to fix typographical errors. The major changes in this edition are the following:

- A unified discussion of how matrices can be used to specify monomial orders in §2 of Chapter 1.
- A rewritten presentation of the Mora normal form algorithm in §3 of Chapter 4 and the division of §4 into two sections.
- The addition of two sections in Chapter 8: §4 introduces the Gröbner fan of an ideal and §5 discusses the Gröbner Walk basis conversion algorithm.
- The replacement of §5 of Chapter 9 by a new Chapter 10 on the theory of order domains, associated codes, and the Berlekamp-Massey-Sakata decoding algorithm. The one-point geometric Goppa codes studied in the first edition are special cases of this construction.
- The Maple code has been updated and *Macaulay* has been replaced by *Macaulay 2*.

We would like to thank the many readers who helped us find typographical errors in the first edition. Special thanks go to Rainer Steinwandt for his heroic efforts. We also want to give particular thanks to Rex Agacy, Alicia Dickenstein, Dan Grayson, Serkan Hoşten, Christoph Kögl, Nick Loehr, Jim Madden, Mike O'Sullivan, Lyle Ramshaw, Hal Schenck, Hans Sterk, Mike Stillman, Bernd Sturmfels, and Irena Swanson for their help.

August, 2004

David Cox
John Little
Donal O'Shea

Preface to the First Edition

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 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., [AM] for Atiyah and Macdonald), 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 [Bla] 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), and Wiland Schmale 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 to the Second Edition v

Preface to the First Edition vii

1 Introduction **1**

§1 Polynomials and Ideals 1

§2 Monomial Orders and Polynomial Division 6

§3 Gröbner Bases 13

§4 Affine Varieties 19

2 Solving Polynomial Equations **26**

§1 Solving Polynomial Systems by Elimination 26

§2 Finite-Dimensional Algebras 37

§3 Gröbner Basis Conversion 49

§4 Solving Equations via Eigenvalues and Eigenvectors 56

§5 Real Root Location and Isolation 69

3 Resultants **77**

§1 The Resultant of Two Polynomials 77

§2 Multipolynomial Resultants 84

§3 Properties of Resultants 95

§4 Computing Resultants 102

§5 Solving Equations via Resultants 114

§6 Solving Equations via Eigenvalues and Eigenvectors 128

4 Computation in Local Rings **137**

§1 Local Rings 137

§2 Multiplicities and Milnor Numbers 145

§3 Term Orders and Division in Local Rings 158

§4 Standard Bases in Local Rings 174

§5 Applications of Standard Bases 180

5 **Modules** **189**
§1 Modules over Rings 189
§2 Monomial Orders and Gröbner Bases for Modules 207
§3 Computing Syzygies 222
§4 Modules over Local Rings 234

6 **Free Resolutions** **247**
§1 Presentations and Resolutions of Modules 247
§2 Hilbert's Syzygy Theorem 258
§3 Graded Resolutions 266
§4 Hilbert Polynomials and Geometric Applications 280

7 **Polytopes, Resultants, and Equations** **305**
§1 Geometry of Polytopes 305
§2 Sparse Resultants 313
§3 Toric Varieties 322
§4 Minkowski Sums and Mixed Volumes 332
§5 Bernstein's Theorem 342
§6 Computing Resultants and Solving Equations 357

8 **Polyhedral Regions and Polynomials** **376**
§1 Integer Programming 376
§2 Integer Programming and Combinatorics 392
§3 Multivariate Polynomial Splines 405
§4 The Gröbner Fan of an Ideal 426
§5 The Gröbner Walk 436

9 **Algebraic Coding Theory** **451**
§1 Finite Fields 451
§2 Error-Correcting Codes 459
§3 Cyclic Codes 468
§4 Reed-Solomon Decoding Algorithms 480

10 **The Berlekamp-Massey-Sakata Decoding Algorithm** **494**
§1 Codes from Order Domains 494
§2 The Overall Structure of the BMS Algorithm 508
§3 The Details of the BMS Algorithm 522

References **533**

Index **547**

Chapter 1

Introduction

Algebraic geometry is the study of geometric objects defined by polynomial equations, using algebraic means. Its roots go back to Descartes' introduction of coordinates to describe points in Euclidean space and his idea of describing curves and surfaces by algebraic equations. Over the long history of the subject, both powerful general theories and detailed knowledge of many specific examples have been developed. Recently, with the development of computer algebra systems and the discovery (or rediscovery) of algorithmic approaches to many of the basic computations, the techniques of algebraic geometry have also found significant applications, for example in geometric design, combinatorics, integer programming, coding theory, and robotics. Our goal in *Using Algebraic Geometry* is to survey these algorithmic approaches and many of their applications.

For the convenience of the reader, in this introductory chapter we will first recall the basic algebraic structure of *ideals* in polynomial rings. In §2 and §3 we will present a rapid summary of the *Gröbner basis algorithms* developed by Buchberger for computations in polynomial rings, with several worked out examples. Finally, in §4 we will recall the geometric notion of an *affine algebraic variety*, the simplest type of geometric object defined by polynomial equations. The topics in §1, §2, and §3 are the common prerequisites for all of the following chapters. §4 gives the geometric context for the algebra from the earlier sections. We will make use of this language at many points. If these topics are familiar, you may wish to proceed directly to the later material and refer back to this introduction as needed.

§1 Polynomials and Ideals

To begin, we will recall some terminology. A *monomial* in a collection of variables $x_1, \ldots, x_n$ is a product

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \tag{1.1}$$

where the α_i are non-negative integers. To abbreviate, we will sometimes rewrite (1.1) as x^α where $\alpha = (\alpha_1, \ldots, \alpha_n)$ is the vector of exponents in the monomial. The *total degree* of a monomial x^α is the sum of the exponents: $\alpha_1 + \cdots + \alpha_n$. We will often denote the total degree of the monomial x^α by $|\alpha|$. For instance $x_1^3 x_2^2 x_4$ is a monomial of total degree 6 in the variables x_1, x_2, x_3, x_4, since $\alpha = (3, 2, 0, 1)$ and $|\alpha| = 6$.

If k is any field, we can form finite linear combinations of monomials with coefficients in k. The resulting objects are known as *polynomials* in $x_1, \ldots, x_n$. We will also use the word *term* on occasion to refer to a product of a nonzero element of k and a monomial appearing in a polynomial. Thus, a general polynomial in the variables $x_1, \ldots, x_n$ with coefficients in k has the form

$$f = \sum_\alpha c_\alpha x^\alpha,$$

where $c_\alpha \in k$ for each α, and there are only finitely many terms $c_\alpha x^\alpha$ in the sum. For example, taking k to be the field $\mathbb{Q}$ of rational numbers, and denoting the variables by x, y, z rather than using subscripts,

$$p = x^2 + \tfrac{1}{2} y^2 z - z - 1 \tag{1.2}$$

is a polynomial containing four terms.

In most of our examples, the field of coefficients will be either $\mathbb{Q}$, the field of real numbers, $\mathbb{R}$, or the field of complex numbers, $\mathbb{C}$. Polynomials over finite fields will also be introduced in Chapter 9. We will denote by $k[x_1, \ldots, x_n]$ the collection of all polynomials in $x_1, \ldots, x_n$ with coefficients in k. Polynomials in $k[x_1, \ldots, x_n]$ can be added and multiplied as usual, so $k[x_1, \ldots, x_n]$ has the structure of a *commutative ring* (with identity). However, only nonzero constant polynomials have multiplicative inverses in $k[x_1, \ldots, x_n]$, so $k[x_1, \ldots, x_n]$ is not a field. However, the set of *rational functions* $\{f/g : f, g \in k[x_1, \ldots, x_n], g \neq 0\}$ is a field, denoted $k(x_1, \ldots, x_n)$.

A polynomial f is said to be *homogeneous* if all the monomials appearing in it with nonzero coefficients have *the same* total degree. For instance, $f = 4x^3 + 5xy^2 - z^3$ is a homogeneous polynomial of total degree 3 in $\mathbb{Q}[x, y, z]$, while $g = 4x^3 + 5xy^2 - z^6$ is not homogeneous. When we study resultants in Chapter 3, homogeneous polynomials will play an important role.

Given a collection of polynomials, $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, we can consider all polynomials which can be built up from these by multiplication by arbitrary polynomials and by taking sums.

(1.3) Definition. Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. We let $\langle f_1, \ldots, f_s \rangle$ denote the collection

$$\langle f_1, \ldots, f_s \rangle = \{p_1 f_1 + \cdots + p_s f_s : p_i \in k[x_1, \ldots, x_n] \text{ for } i = 1, \ldots, s\}.$$

For example, consider the polynomial p from (1.2) above and the two polynomials

$$\begin{aligned} f_1 &= x^2 + z^2 - 1 \\ f_2 &= x^2 + y^2 + (z-1)^2 - 4. \end{aligned}$$

We have

$$\begin{aligned} p &= x^2 + \tfrac{1}{2}y^2z - z - 1 \\ &= (-\tfrac{1}{2}z + 1)(x^2 + z^2 - 1) + (\tfrac{1}{2}z)(x^2 + y^2 + (z-1)^2 - 4). \end{aligned} \tag{1.4}$$

This shows $p \in \langle f_1, f_2 \rangle$.

Exercise 1.
a. Show that $x^2 \in \langle x - y^2, xy \rangle$ in $k[x, y]$ (k any field).
b. Show that $\langle x - y^2, xy, y^2 \rangle = \langle x, y^2 \rangle$.
c. Is $\langle x - y^2, xy \rangle = \langle x^2, xy \rangle$? Why or why not?

Exercise 2. Show that $\langle f_1, \ldots, f_s \rangle$ is closed under sums in $k[x_1, \ldots, x_n]$. Also show that if $f \in \langle f_1, \ldots, f_s \rangle$, and $p \in k[x_1, \ldots, x_n]$ is an arbitrary polynomial, then $p \cdot f \in \langle f_1, \ldots, f_s \rangle$.

The two properties in Exercise 2 are the defining properties of *ideals* in the ring $k[x_1, \ldots, x_n]$.

(1.5) Definition. Let $I \subset k[x_1, \ldots, x_n]$ be a non-empty subset. I is said to be an *ideal* if
a. $f + g \in I$ whenever $f \in I$ and $g \in I$, and
b. $pf \in I$ whenever $f \in I$, and $p \in k[x_1, \ldots, x_n]$ is an arbitrary polynomial.

Thus $\langle f_1, \ldots, f_s \rangle$ is an ideal by Exercise 2. We will call it the *ideal generated by* $f_1, \ldots, f_s$ because it has the following property.

Exercise 3. Show that $\langle f_1, \ldots, f_s \rangle$ is the *smallest* ideal in $k[x_1, \ldots, x_n]$ containing $f_1, \ldots, f_s$, in the sense that if J is any ideal containing $f_1, \ldots, f_s$, then $\langle f_1, \ldots, f_s \rangle \subset J$.

Exercise 4. Using Exercise 3, formulate and prove a general criterion for equality of ideals $I = \langle f_1, \ldots, f_s \rangle$ and $J = \langle g_1, \ldots, g_t \rangle$ in $k[x_1, \ldots, x_n]$. How does your statement relate to what you did in part b of Exercise 1?

Given an ideal, or several ideals, in $k[x_1, \ldots, x_n]$, there are a number of algebraic constructions that yield other ideals. One of the most important of these for geometry is the following.

(1.6) Definition. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The *radical of* I is the set

$$\sqrt{I} = \{g \in k[x_1, \ldots, x_n] : g^m \in I \text{ for some } m \geq 1\}.$$

An ideal I is said to be a *radical ideal* if $\sqrt{I} = I$.

For instance,

$$x + y \in \sqrt{\langle x^2 + 3xy, 3xy + y^2\rangle}$$

in $\mathbb{Q}[x, y]$ since

$$(x + y)^3 = x(x^2 + 3xy) + y(3xy + y^2) \in \langle x^2 + 3xy, 3xy + y^2\rangle.$$

Since each of the generators of the ideal $\langle x^2 + 3xy, 3xy + y^2\rangle$ is homogeneous of degree 2, it is clear that $x + y \notin \langle x^2 + 3xy, 3xy + y^2\rangle$. It follows that $\langle x^2 + 3xy, 3xy + y^2\rangle$ is *not* a radical ideal.

Although it is not obvious from the definition, we have the following property of the radical.

- (Radical Ideal Property) For every ideal $I \subset k[x_1, \ldots, x_n]$, $\sqrt{I}$ is an ideal containing I.

See [CLO], Chapter 4, §2, for example. We will consider a number of other operations on ideals in the exercises.

One of the most important general facts about ideals in $k[x_1, \ldots, x_n]$ is known as the Hilbert Basis Theorem. In this context, a *basis* is another name for a generating set for an ideal.

- (Hilbert Basis Theorem) Every ideal I in $k[x_1, \ldots, x_n]$ has a *finite* generating set. In other words, given an ideal I, there exists a finite collection of polynomials $\{f_1, \ldots, f_s\} \subset k[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s\rangle$.

For polynomials in one variable, this is a standard consequence of the one-variable polynomial division algorithm.

- *(Division Algorithm in $k[x]$) Given two polynomials $f, g \in k[x]$, we can* divide f by g, producing a unique quotient q and remainder r such that

$$f = qg + r,$$

and either $r = 0$, or r has degree strictly smaller than the degree of g.

See, for instance, [CLO], Chapter 1, §5. The consequences of this result for ideals in $k[x]$ are discussed in Exercise 6 below. For polynomials in several variables, the Hilbert Basis Theorem can be proved either as a byproduct of the theory of Gröbner bases to be reviewed in the next section (see [CLO], Chapter 2, §5), or inductively by showing that if every ideal in a ring R is finitely generated, then the same is true in the ring $R[x]$ (see [AL], Chapter 1, §1, or [BW], Chapter 4, §1).

Additional Exercises for §1

Exercise 5. Show that $\langle y - x^2, z - x^3\rangle = \langle z - xy, y - x^2\rangle$ in $\mathbb{Q}[x, y, z]$.

Exercise 6. Let k be any field, and consider the polynomial ring in one variable, $k[x]$. In this exercise, you will give one proof that every ideal in $k[x]$ is finitely generated. In fact, every ideal $I \subset k[x]$ is generated by a single polynomial: $I = \langle g\rangle$ for some g. We may assume $I \neq \{0\}$ for there is nothing to prove in that case. Let g be a nonzero element in I of minimal degree. Show using the division algorithm that every f in I is divisible by g. Deduce that $I = \langle g\rangle$.

Exercise 7.

a. Let k be any field, and let n be any positive integer. Show that in $k[x]$, $\sqrt{\langle x^n\rangle} = \langle x\rangle$.

b. More generally, suppose that

$$p(x) = (x - a_1)^{e_1} \cdots (x - a_m)^{e_m}.$$

What is $\sqrt{\langle p(x)\rangle}$?

c. Let $k = \mathbb{C}$, so that *every* polynomial in one variable factors as in b. What are the radical ideals in $\mathbb{C}[x]$?

Exercise 8. An ideal $I \subset k[x_1, \ldots, x_n]$ is said to be *prime* if whenever a product fg belongs to I, either $f \in I$, or $g \in I$ (or both).

a. Show that a prime ideal is radical.

b. What are the prime ideals in $\mathbb{C}[x]$? What about the prime ideals in $\mathbb{R}[x]$ or $\mathbb{Q}[x]$?

Exercise 9. An ideal $I \subset k[x_1, \ldots, x_n]$ is said to be *maximal* if there are no ideals J satisfying $I \subset J \subset k[x_1, \ldots, x_n]$ other than $J = I$ and $J = k[x_1, \ldots, x_n]$.

a. Show that $\langle x_1, x_2, \ldots, x_n\rangle$ is a maximal ideal in $k[x_1, \ldots, x_n]$.

b. More generally show that if $(a_1, \ldots, a_n)$ is any point in k^n, then the ideal $\langle x_1 - a_1, \ldots, x_n - a_n\rangle \subset k[x_1, \ldots, x_n]$ is maximal.

c. Show that $I = \langle x^2 + 1\rangle$ is a maximal ideal in $\mathbb{R}[x]$. Is I maximal considered as an ideal in $\mathbb{C}[x]$?

Exercise 10. Let I be an ideal in $k[x_1, \ldots, x_n]$, let $\ell \geq 1$ be an integer, and let I_ℓ consist of the elements in I that do not depend on the first ℓ variables:

$$I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n].$$

I_ℓ is called the ℓth *elimination ideal* of I.

a. For $I = \langle x^2 + y^2, x^2 - z^3\rangle \subset k[x, y, z]$, show that $y^2 + z^3$ is in the first elimination ideal I_1.