Undergraduate Texts in Mathematics

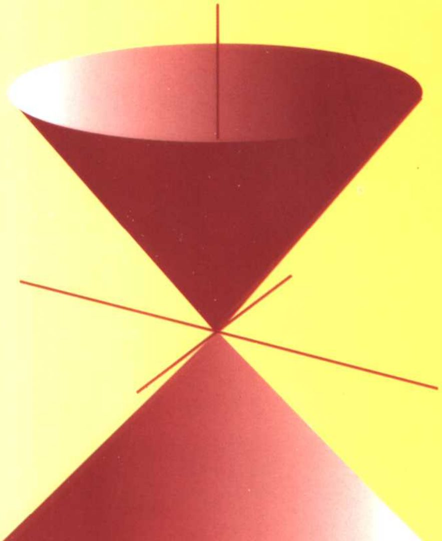
IDEALS VAREIETIES AND ALGORITHMS

An Introduction to Computational Algebraic Geometry and Commutative Algebra

Second Edition

理想数、簇与算法 第2版

David Cox John Little Donal O'Shea



Springer

世界图书出版公司

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

书　　名：Ideals,Varieties, and Algorithms:
An Introduction to Computational Algebraic Geometry and Commutative Algebra 2nd ed
作　　者：David Cox , John Little , Donal O'Shea
中 译 名：理想数、簇与算法 第 2 版
出 版 者：世界图书出版公司北京公司
印 刷 者：北京世图印刷厂
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：010-64015659, 64038347
电子信箱：kjsk@vip.sina.com
开　　本：24 开　　　印　张：23
出版年代：2004 年 4 月
书　　号：7-5062-6598-2/O·451
版权登记：图字:01-2004-1604
定　　价：75.00 元

世界图书出版公司北京公司已获得 Springer-Verlag 授权在中国大陆独家重印发行。

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

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.
ISBN 0-387-94680-2 (alk. paper)
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

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.
Reprinted in China by Beijing World Publishing Corporation, 2004

9 8 7 6 5 4 3 2 1

ISBN 0-387-94680-2 Springer-Verlag New York Berlin Heidelberg SPIN 10490312

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.

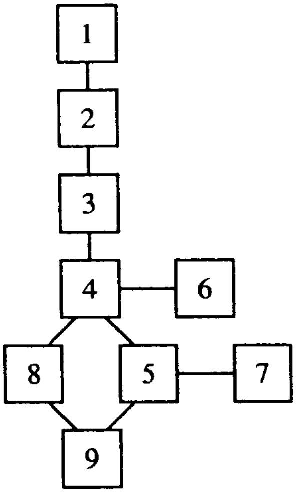
It is our belief that the growing importance of these computational techniques warrants their introduction into the undergraduate (and graduate) mathematics curriculum. Many undergraduates enjoy the concrete, almost nineteenth-century, flavor that a computational emphasis brings to the subject. At the 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 majors 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

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 $\alpha_1, \dots, \alpha_n$ 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 $\alpha = (\alpha_1, \dots, \alpha_n)$ be an n-tuple of non-negative integers. Then we set

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

When $\alpha = (0, \dots, 0)$, 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 $x_1, \dots, x_n$ 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 $\alpha = (\alpha_1, \dots, \alpha_n)$. The set of all polynomials in $x_1, \dots, x_n$ with coefficients in k is denoted $k[x_1, \dots, x_n]$.

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 $k[x_1, \dots, x_n]$.*

(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 $h \in k[x_1, \dots, x_n]$.

One can show that, under addition and multiplication, $k[x_1, \dots, x_n]$ 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 (see Appendix A for the full definition), and for this reason we will refer to $k[x_1, \dots, x_n]$ as a *polynomial ring*.

The next topic to consider is affine space.

Definition 4. *Given a field k and a positive integer n, we define the n-dimensional* **affine space** *over k to be the set*

$$k^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in k\}.$$

For an example of affine space, consider the case $k = \mathbb{R}$. Here we get the familiar space $\mathbb{R}^n$ from calculus and linear algebra. In general, we call $k^1 = k$ the *affine line* and k^2 the *affine plane*.

Let us next see how polynomials relate to affine space. The key idea is that a polynomial $f = \Sigma_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ gives a function

$$f : k^n \rightarrow k$$

defined as follows: given $(a_1, \ldots, a_n) \in k^n$, replace every x_i by a_i in the expression for f. Since all of the coefficients also lie in k, this operation gives an element $f(a_1, \ldots, a_n) \in k$. The ability to regard a polynomial as a function is what makes it possible to link algebra and geometry.

This dual nature of polynomials has some unexpected consequences. For example, the question "is $f = 0$?" now has two potential meanings: is f the zero polynomial?, which means that all of its coefficients a_α are zero, or is f the zero function?, which means that $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in k^n$. The surprising fact is that these two statements are not equivalent in general. For an example of how they can differ, consider the set consisting of the two elements 0 and 1. In the exercises, we will see that this can be made into a field where $1 + 1 = 0$. This field is usually called $\mathbb{F}_2$. Now consider the polynomial $x^2 - x = x(x - 1) \in \mathbb{F}_2[x]$. Since this polynomial vanishes at 0 and 1, we have found a nonzero polynomial which gives the zero function on the affine space $\mathbb{F}_2^1$. Other examples will be discussed in the exercises.

However, as long as k is infinite, there is no problem.

Proposition 5. *Let k be an infinite field, and let $f \in k[x_1, \ldots, x_n]$. Then $f = 0$ in $k[x_1, \ldots, x_n]$ if and only if $f : k^n \rightarrow k$ is the zero function.*

Proof. One direction of the proof is obvious since the zero polynomial clearly gives the zero function. To prove the converse, we need to show that if $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in k^n$, then f is the zero polynomial. We will use induction on the number of variables n.

When $n = 1$, it is well known that a nonzero polynomial in $k[x]$ of degree m has at most m distinct roots (we will prove this fact in Corollary 3 of §5). For our particular $f \in k[x]$, we are assuming $f(a) = 0$ for all $a \in k$. Since k is infinite, this means that f has infinitely many roots, and, hence, f must be the zero polynomial.

Now assume that the converse is true for $n - 1$, and let $f \in k[x_1, \ldots, x_n]$ be a polynomial that vanishes at all points of k^n. By collecting the various powers of x_n, we can write f in the form

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1})x_n^i,$$

where $g_i \in k[x_1, \ldots, x_{n-1}]$. We will show that each g_i is the zero polynomial in $n-1$ variables, which will force f to be the zero polynomial in $k[x_1, \ldots, x_n]$.

If we fix $(a_1, \ldots, a_{n-1}) \in k^{n-1}$, we get the polynomial $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$. By our hypothesis on f, this vanishes for every $a_n \in k$. It follows from the case $n = 1$ that $f(a_1, \ldots, a_{n-1}, x_n)$ is the zero polynomial in $k[x_n]$. Using the above formula for f, we see that the coefficients of $f(a_1, \ldots, a_{n-1}, x_n)$ are $g_i(a_1, \ldots, a_{n-1})$, and thus, $g_i(a_1, \ldots, a_{n-1}) = 0$ for all i. Since $(a_1, \ldots, a_{n-1})$ was arbitrarily chosen in k^{n-1}, it follows that each $g_i \in k[x_1, \ldots, x_{n-1}]$ gives the zero function on k^{n-1}. Our inductive assumption then implies that each g_i is the zero polynomial in $k[x_1, \ldots, x_{n-1}]$. This forces f to be the zero polynomial in $k[x_1, \ldots, x_n]$ and completes the proof of the proposition. □

Note that in the statement of Proposition 5, the assertion "$f = 0$ in $k[x_1, \ldots, x_n]$" means that f is the zero polynomial, i.e., that every coefficient of f is zero. Thus, we use the same symbol "0" to stand for the zero element of k and the zero polynomial in $k[x_1, \ldots, x_n]$. The context will make clear which one we mean.

As a corollary, we see that two polynomials are equal precisely when they give the same function on affine space.

Corollary 6. *Let k be an infinite field, and let $f, g \in k[x_1, \ldots, x_n]$. Then $f = g$ in $k[x_1, \ldots, x_n]$ if and only if $f : k^n \to k$ and $g : k^n \to k$ are the same function.*

Proof. To prove the nontrivial direction, suppose that $f, g \in k[x_1, \ldots, x_n]$ give the same function on k^n. By hypothesis, the polynomial $f - g$ vanishes at all points of k^n. Proposition 4 then implies that $f - g$ is the zero polynomial. This proves that $f = g$ in $k[x_1, \ldots, x_n]$. □

Finally, we need to record a special property of polynomials over the field of complex numbers $\mathbb{C}$.

Theorem 7. *Every nonconstant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

Proof. This is the Fundamental Theorem of Algebra, and proofs can be found in most introductory texts on complex analysis (although many other proofs are known). □

We say that a field k is *algebraically closed* if every nonconstant polynomial in $k[x]$ has a root in k. Thus $\mathbb{R}$ is not algebraically closed (what are the roots of $x^2 + 1$?), whereas the above theorem asserts that $\mathbb{C}$ is algebraically closed. In Chapter 4 we will prove a powerful generalization of Theorem 7 called the Hilbert Nullstellensatz.

EXERCISES FOR §1

1. Let $\mathbb{F}_2 = \{0, 1\}$, and define addition and multiplication by $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ and $1 \cdot 1 = 1$. Explain why $\mathbb{F}_2$ is a field. (You need not check the associative and distributive properties, but you should verify the existence of identities and inverses, both additive and multiplicative.)
2. Let $\mathbb{F}_2$ be the field from Exercise 1.

a. Consider the polynomial $g(x, y) = x^2y + y^2x \in \mathbb{F}_2[x, y]$. Show that $g(x, y) = 0$ for every $(x, y) \in \mathbb{F}_2^2$, and explain why this does not contradict Proposition 5.
b. Find a nonzero polynomial in $\mathbb{F}_2[x, y, z]$ which vanishes at every point of $\mathbb{F}_2^3$. Try to find one involving all three variables.
c. Find a nonzero polynomial in $\mathbb{F}_2[x_1, \dots, x_n]$ which vanishes at every point of $\mathbb{F}_2^n$. Can you find one in which all of $x_1, \dots, x_n$ appear?

3. (Requires abstract algebra). Let p be a prime number. The ring of integers modulo p is a field with p elements, which we will denote $\mathbb{F}_p$.
a. Explain why $\mathbb{F}_p - \{0\}$ is a group under multiplication.
b. Use Lagrange's Theorem to show that $a^{p-1} = 1$ for all $a \in \mathbb{F}_p - \{0\}$.
c. Prove that $a^p = a$ for all $a \in \mathbb{F}_p$. Hint: Treat the cases $a = 0$ and $a \neq 0$ separately.
d. Find a nonzero polynomial $\mathbb{F}_p[x]$ which vanishes at every point of $\mathbb{F}_p$. Hint: Use part c.
4. (Requires abstract algebra.) Let F be a finite field with q elements. Adapt the argument of Exercise 3 to prove that $x^q - x$ is a nonzero polynomial in $F[x]$ which vanishes at every point of F. This shows that Proposition 5 fails for *all* finite fields.
5. In the proof of Proposition 5, we took $f \in k[x_1, \dots, x_n]$ and wrote it as a polynomial in x_n with coefficients in $k[x_1, \dots, x_{n-1}]$. To see what this looks like in a specific case, consider the polynomial

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3.$$

a. Write f as a polynomial in x with coefficients in $k[y, z]$.
b. Write f as a polynomial in y with coefficients in $k[x, z]$.
c. Write f as a polynomial in z with coefficients in $k[x, y]$.

6. Inside of $\mathbb{C}^n$, we have the subset $\mathbb{Z}^n$, which consists of all points with integer coordinates.
a. Prove that if $f \in \mathbb{C}[x_1, \dots, x_n]$ vanishes at every point of $\mathbb{Z}^n$, then f is the zero polynomial. Hint: Adapt the proof of Proposition 5.
b. Let $f \in \mathbb{C}[x_1, \dots, x_n]$, and let M be the largest power of any variable that appears in f. Let $\mathbb{Z}^n_{M+1}$ be the set of points of $\mathbb{Z}^n$, all coordinates of which lie between 1 and $M + 1$. Prove that if f vanishes at all points of $\mathbb{Z}^n_{M+1}$, then f is the zero polynomial.

§2 Affine Varieties

We can now define the basic geometric object of the book.

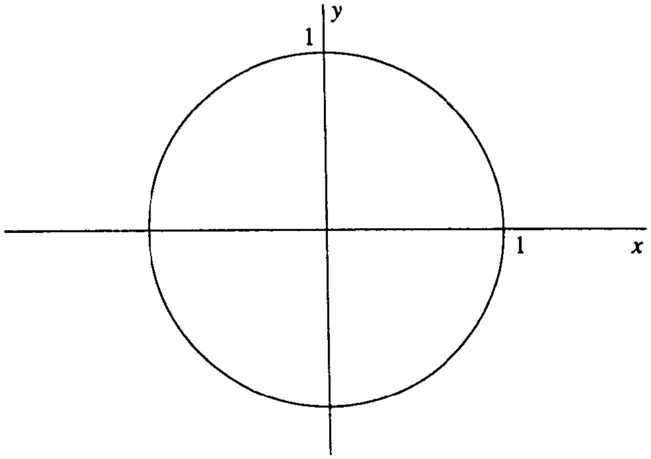
Definition 1. *Let k be a field, and let $f_1, \dots, f_s$ be polynomials in $k[x_1, \dots, x_n]$. Then we set*

$$\mathbf{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \textit{ for all } 1 \leq i \leq s\}.$$

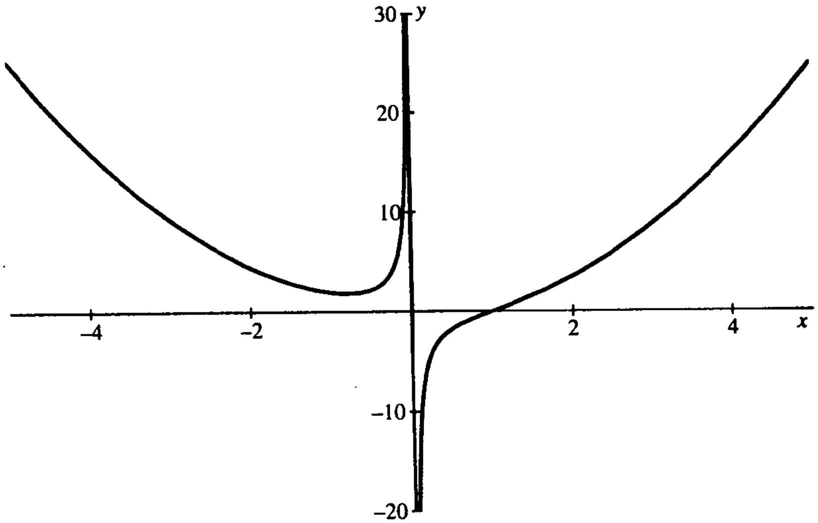
We call $\mathbf{V}(f_1, \dots, f_s)$ *the* **affine variety** *defined by* $f_1, \dots, f_s$.

Thus, an affine variety $\mathbf{V}(f_1, \dots, f_s) \subset k^n$ is the set of all solutions of the system of equations $f_1(x_1, \dots, x_n) = \cdots = f_s(x_1, \dots, x_n) = 0$. We will use the letters V, W, etc. to denote affine varieties. The main purpose of this section is to introduce the reader to *lots* of examples, some new and some familiar. We will use $k = \mathbb{R}$ so that we can draw pictures.

We begin in the plane $\mathbb{R}^2$ with the variety $\mathbf{V}(x^2 + y^2 - 1)$, which is the circle of radius 1 centered at the origin:



The conic sections studied in analytic geometry (circles, ellipses, parabolas, and hyperbolas) are affine varieties. Likewise, graphs of polynomial functions are affine varieties [the graph of $y = f(x)$ is $\mathbf{V}(y - f(x))$]. Although not as obvious, graphs of rational functions are also affine varieties. For example, consider the graph of $y = \frac{x^3-1}{x}$:



It is easy to check that this is the affine variety $\mathbf{V}(xy - x^3 + 1)$.

Next, let us look in 3-dimensional space $\mathbb{R}^3$. A nice affine variety is given by paraboloid of revolution $\mathbf{V}(z - x^2 - y^2)$, which is obtained by rotating the parabola $z = x^2$ about the z-axis (you can check this using polar coordinates). This gives us the picture: