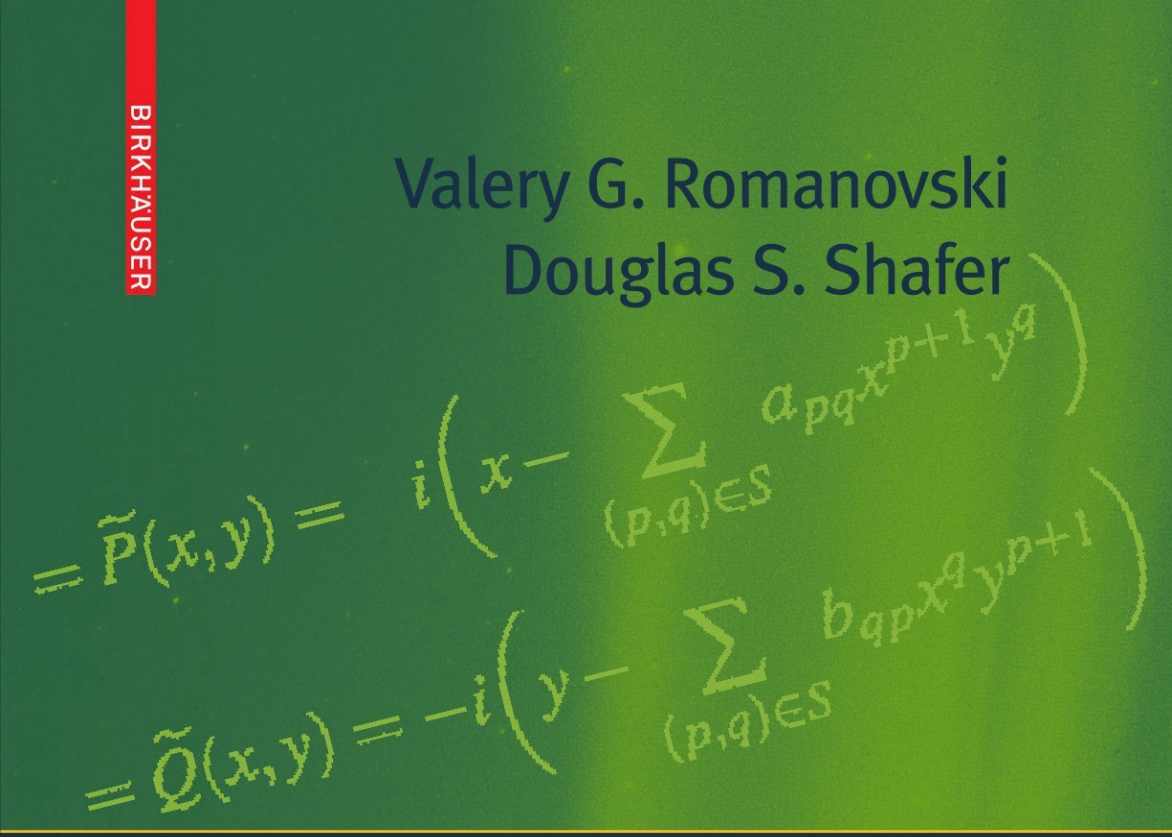
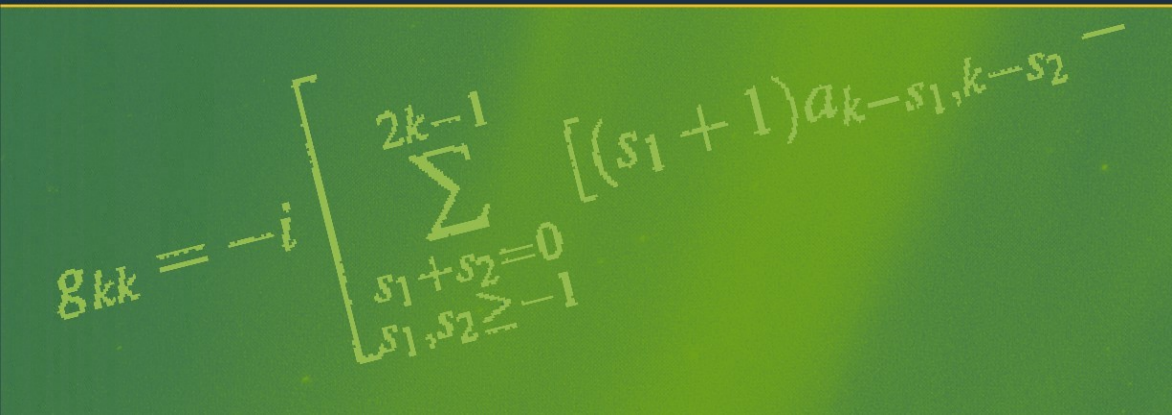
BIRKHÄUSER

Valery G. Romanovski
Douglas S. Shafer



The Center and Cyclicity Problems

A Computational Algebra Approach



BIRKHÄUSER

Valery G. Romanovski
Douglas S. Shafer

The Center and Cyclicity Problems:
A Computational Algebra Approach

Birkhäuser
Boston • Basel • Berlin

Valery G. Romanovski
Center for Applied Mathematics
and Theoretical Physics
University of Maribor
Krekova 2
2000 Maribor, Slovenia
valery.romanovsky@uni-mb.si

Douglas S. Shafer
Department of Mathematics
University of North Carolina
Charlotte, NC 28025
USA
dsshafer@uncc.edu

ISBN 978-0-8176-4726-1 eISBN 978-0-8176-4727-8
DOI 10.1007/978-0-8176-4727-8

Library of Congress Control Number: PCN applied for

Mathematics Subject Classification (2000): 34C07, 37G15, 37G05, 34C23, 34C14, 34-01, 37-01, 13-01, 14-01

Cover designed by Alex Gerasev.

Printed on acid-free paper.

Springer is part of Springer Science+Business Media (www.springer.com)

To our families and teachers.

Preface

The primary object of study in this book is small-amplitude periodic solutions of two-dimensional autonomous systems of ordinary differential equations,

$$\dot{x} = P(x,y), \qquad \dot{y} = Q(x,y),$$

for which the right-hand sides are polynomials. Such systems are called polynomial systems. If the origin is an isolated singularity of a polynomial (or real analytic) system, and if there does not exist an orbit that tends to the singularity, in either forward or reverse time, with a definite limiting tangent direction, then the singularity must be either a *center*, in which case there is a neighborhood of the origin in which every orbit except the origin is periodic, or a *focus*, in which case there is a neighborhood of the origin in which every orbit spirals towards or away from the origin. The problem of distinguishing between a center and a focus for a given polynomial system or a family of such systems is known as the Poincaré center problem or the center-focus problem. Although it dates from the end of the 19th century, it is completely solved only for linear and quadratic systems ($\max\{\deg(P), \deg(Q)\}$ equal to 1 or 2, respectively) and a few particular cases in families of higher degree.

Relatively simple analysis shows that when the matrix of the linearization of the system at the the singular point has eigenvalues with nonzero real parts, the singular point is a focus. If, however, the real parts of the eigenvalues are zero then the type of the singular point depends on the nonlinear terms of polynomials in a nontrivial way. A general method due to Poincaré and Lyapunov reduces the problem to that of solving an infinite system of polynomial equations whose variables are parameters of the system of differential equations. That is, the center-focus problem is reduced to the problem of finding the variety of the ideal generated by a collection of polynomials, called the focus quantities of the system.

A second problem, called the cyclicity problem, is to estimate the number of limit cycles, that is, isolated periodic solutions, that can bifurcate from a center or focus when the coefficients of the system of differential equations are perturbed by an arbitrarily small amount, but in such a way as to remain in a particular family of systems, for example in the family of all quadratic polynomial systems if the

original system was quadratic. This problem is a part of the still unresolved 16th Hilbert problem and is often called the local 16th Hilbert problem. In fact, in order to find an upper bound for the cyclicity of a center or focus in a polynomial system it is sufficient to obtain a basis for the above-mentioned ideal of focus quantities. Thus the study of these two famous problems in the qualitative theory of differential equations can be carried out through the study of polynomial ideals, that is, through the study of an object of commutative algebra.

Recent decades have seen a surge of interest in the center and cyclicity problems. Certainly an important reason for this is that the resolution of these problems involves extremely laborious computations, which nowadays can be carried out using powerful computational facilities. Applications of concepts that could not be utilized even 30 years ago are now feasible, often even on a personal computer, because of advances in the mathematical theory, in the computer software of computational algebra, and in computer technology. This book is intended to give the reader a thorough grounding in the theory, and explains and illustrates methods of computational algebra, as a means of approaching the center-focus and cyclicity problems.

The methods we present can be most effectively exploited if the original real system of differential equations is properly complexified; hence, the idea of complexifying a real system, and more generally working in a complex setting, is one of the central ideas of the text. Although the idea of extracting information about a real system of ordinary differential equations from its complexification goes back to Lyapunov, it is still relatively scantily used. Our belief that it deserves exposition at the level of a textbook has been a primary motivation for this work. In addition to that, it has appeared to us that by and large specialists in the qualitative theory of differential equations are not well versed in these new methods of computational algebra, and conversely that there appears to be a general lack of knowledge on the part of specialists in computational algebra about the possibility of an algebraic treatment of these problems of differential equations. We have written this work with the intention of trying to help to draw together these two mathematical communities.

Thus, the readers we have had in mind in writing this work have been graduate students and researchers in nonlinear differential equations and computational algebra, and in fields outside mathematics in which the investigation of nonlinear oscillation is relevant. The book is designed to be suitable for use as a primary textbook in an advanced graduate course or as a supplementary source for beginning graduate courses. Among other things, this has meant motivating and illustrating the material with many examples, and including a great many exercises, arranged in the order in which the topics they cover appear in the text. It has also meant that we have given complete proofs of a number of theorems that are not readily available in the current literature and that we have given much more detailed versions of proofs that were written for specialists. All in all, researchers working in the theory of limit cycles of polynomial systems should find it a valuable reference resource, and because it is self-contained and written to be accessible to nonspecialists, researchers in other fields should find it an understandable and helpful introduction to the tools

they need to study the onset of stable periodic motion, such as ideals in polynomial rings and Gröbner bases.

The first two chapters introduce the primary technical tools for this approach to the center and cyclicity problems, as well as questions of linearizability and isochronicity that are naturally investigated in the same manner. The first chapter lays the groundwork of computational algebra. We give the main properties of ideals in polynomial rings and their affine varieties, explain the concept of Gröbner bases, a key component of various algorithms of computational algebra, and provide explicit algorithms for elimination and implicitization problems and for basic operations on ideals in polynomial rings and on their varieties. The second chapter begins with the main theorems of Lyapunov's second method, theorems that are aimed at the investigation of the stability of singularities (in this context often termed equilibrium points) by means of Lyapunov functions. We then cover the basics of the theory of normal forms of ordinary differential equations, including an algorithm for the normalization procedure and a criterion for convergence of normalization transformations and normal forms.

Chapter 3 is devoted to the center problem. We describe how the concept of a center can be generalized to complex systems, in order to take advantage of working over the algebraically closed field $\mathbb{C}$ in place of $\mathbb{R}$. This leads to the study of the variety, in the space of parameters of the system, that corresponds to systems with a center, which is called the center variety. We present an efficient computational algorithm for computing the focus quantities, which are the polynomials that define the center variety. Then we describe two main mechanisms for proving the existence of a center in a polynomial system, Darboux integrability and time-reversibility, thereby completing the description of all the tools needed for this method of approach to the center-focus problem. This program and its efficiency are demonstrated by applying it to resolve the center problem for the full family of quadratic systems and for one particular family of cubic systems. In a final section, as a complement to the rest of the chapter, particularly aspects of symmetry, the important special case of Liénard systems is presented.

If all solutions in a neighborhood of a singular point are periodic, then a question that arises naturally is whether all solutions have the same period. This is the so-called isochronicity problem that has attracted study from the time of Huygens and the Bernoullis. In Chapter 4 we present a natural generalization of the concept of isochronicity to complex systems of differential equations, the idea of linearizability. We then introduce and develop methods for investigating linearizability in the complex setting.

As indicated above, one possible mechanism for the existence of a center is time-reversibility of the system. Chapter 5 presents an algorithm for computing all time-reversible systems within a given polynomial family. This takes on additional importance because in all known cases the set of time-reversible systems forms exactly one component of the center variety. The algorithm is derived using the study of invariants of the rotation group of the system and is a nice application of that theory and the algebraic theory developed in Chapter 1.

The last chapter is devoted to the cyclicity problem. We describe Bautin's method, which reduces the study of cyclicity to finding a basis of the ideal of focus quantities, and then show how to obtain the solution for the cyclicity problem in the case that the ideal of focus quantities is radical. In the case that the ideal generated by the first few focus quantities is not radical, the problem becomes much more difficult; at present there is no algorithmic approach for its treatment. Nevertheless we present a particular family of cubic systems for which it is possible, using Gröbner basis calculations, to obtain a bound on cyclicity. Finally, as a further illustration of the applicability of the ideas developed in the text, we investigate the problem of the maximum number of cycles that can maintain the original period of an isochronous center in $\mathbb{R}^2$ when it is perturbed slightly within the collection of centers, the so-called problem of bifurcation of critical periods.

Specialists perusing the table of contents and the bibliography will surely miss some of their favorite topics and references. For example, we have not mentioned methods that approach the center and cyclicity problems based on the theory of resultants and triangular decomposition, and have not treated the cyclicity problem specifically in the important special case of Liénard systems, such as we did for the center problem. We are well aware that there is much more that could be included, but one has to draw the line somewhere, and we can only say that we have made choices of what to include and what to omit based on what seemed best to us, always with an eye to what we hoped would be most valuable to the readers of this book.

The first author acknowledges the financial support of this work by the Slovenian Research Agency. We thank all those with whom we consulted on various aspects of this work, especially Vladimir Basov, Carmen Chicone, Freddy Dumortier, Maoan Han, Evan Houston, and Dongming Wang.

Maribor, Charlotte
May 2008

Valery G. Romanovski
Douglas S. Shafer

Contents

List of Tables

Notation and Conventions

$\mathbb{N}$	the set of natural numbers $\{1,2,3,\ldots\}$
$\mathbb{N}_0$	$\mathbb{N}\cup\{0\}$
$\mathbb{Z}$	the ring of integers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{R}$	the field of real numbers
$\mathbb{C}$	the field of complex numbers
$A \subset B$	A is a subset of B, $A = B$ allowed
$A \subsetneq B$	A is a proper subset of B
$A \setminus B$	elements that are in A and are not in B

See the Index of Notation beginning on p. 323 for a full list of notation.

Chapter 1
Polynomial Ideals and Their Varieties

As indicated in the Preface, solutions of the fundamental questions addressed in this book, the center and cyclicity problems, are expressed in terms of the sets of common zeros of collections of polynomials in the coefficients of the underlying family of systems of differential equations. These sets of common zeros are termed *varieties*. They are determined not so much by the specific polynomials themselves as by larger collections of polynomials, the so-called ideals that the original collections of polynomials generate. In the first section of this chapter we discuss these basic concepts: polynomials, varieties, and ideals. An ideal can have more than one set of generating polynomials, and a fundamental problem is that of deciding when two ideals, hence the varieties they determine, are the same, even though presented by different sets of generators. To address this and related isssues, in Sections 1.2 and 1.3 we introduce the concept of a Gröbner basis and certain fundamental techniques and algorithms of computational algebra for the study of polynomial ideals and their varieties. The last section is devoted to the decomposition of varieties into their simplest components and shows how this decomposition is connected to the structure of the generating ideals. For a fuller exposition of the concepts presented here, the reader may consult [1, 18, 23, 60].

1.1 Fundamental Concepts

A *polynomial* in variables $x_1, x_2, \ldots, x_n$ with coefficients in a field k is a formal expression of the form

$$f = \sum_{\alpha \in S} a_\alpha \mathbf{x}^\alpha, \tag{1.1}$$

where S is a finite subset of $\mathbb{N}_0^n$, $a_\alpha \in k$, and for $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\mathbf{x}^\alpha$ denotes the *monomial* $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. In most cases of interest k will be $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. The product $a_\alpha \mathbf{x}^\alpha$ is called a *term* of the polynomial f. The set of all polynomials in the variables $x_1, \ldots, x_n$ with coefficients in k is denoted by $k[x_1, \ldots, x_n]$. With the natural and well-known addition and multiplication, $k[x_1, \ldots, x_n]$ is a commutative ring. The

V.G. Romanovski, D.S. Shafer, *The Center and Cyclicity Problems*,
DOI 10.1007/978-0-8176-4727-8_1,

full degree of a monomial $\mathbf{x}^\alpha$ is the number $|\alpha| = \alpha_1 + \cdots + \alpha_n$. The *full degree* of a term $a_\alpha \mathbf{x}^\alpha$ is the full degree of the monomial $\mathbf{x}^\alpha$. The *full degree* of a polynomial f as in (1.1), denoted by $\deg(f)$, is the maximum of $|\alpha|$ among all monomials (with nonzero coefficients a_α, of course) of f.

If a field k and a natural number n are given, then we term the set

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

n-dimensional affine space. If f is the polynomial in (1.1) and $(a_1, \ldots, a_n) \in k^n$, then $f(a_1, \ldots, a_n)$ will denote the element $\sum_\alpha a_\alpha a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ of k. Thus, to any polynomial $f \in k[x_1, \ldots, x_n]$ is associated the function $f : k^n \to k$ defined by

$$f : (a_1, \ldots, a_n) \ \mapsto f(a_1, \ldots, a_n)\,.$$

This ability to consider polynomials as functions defines a kind of duality between the algebra and geometry of affine spaces. In the case of an arbitrary field k this interconnection between polynomials and functions on affine spaces can hold some surprises. For example, the statements "f is the zero polynomial" (all coefficients a_α are equal to zero) and "f is the zero function" ($f|_{k^n} \equiv 0$) are not necessarily equivalent (see Exercise 1.1). However, we will work mainly with the infinite fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, for which the following two statements show that our naive intuition is correct.

Proposition 1.1.1. *Let k be an infinite field and $f \in k[x_1, \ldots, x_n]$. Then f is the zero element of $k[x_1, \ldots, x_n]$ (that is, all coefficients a_α of f are equal to zero) if and only if $f : k^n \to k$ is the zero function.*

Proof. Certainly if every coefficient of the polynomial f is the zero polynomial then the corresponding function is the zero function. We must establish the converse:

$$\text{If } f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in k^n, \text{ then } f \text{ is the zero polynomial.} \quad (1.2)$$

We will do this by induction on the number of variables in the polynomial ring.

Basis step. For $n = 1$, the antecedent in (1.2) means that either (i) f is the zero polynomial or (ii) $\deg(f)$ is defined and at least 1 and f has infinitely many roots. It is well known, however (Exercise 1.2), that every polynomial $f \in k[x]$ for which $\deg(f) = s > 0$ has at most s roots. Hence only alternative (i) is possible, so (1.2) holds for $n = 1$.

Inductive step. Suppose (1.2) holds in the ring $k[x_1, \ldots, x_p]$ for $p = 1, 2, \ldots, n-1$. Let $f \in k[x_1, \ldots, x_n]$ be such that the antecedent in (1.2) holds for f. We can write f in the form

$$f = \sum_{j=0}^{m} g_j(x_1, \ldots, x_{n-1}) x_n^j$$

for some finite m, and will show that g_j is the zero polynomial for each j, $1 \le j \le m$. This will imply that f is the zero polynomial. Thus fix any $a = (a_1, \ldots, a_{n-1}) \in k^{n-1}$ and define $f_a \in k[x_n]$ by

$$f_a = \sum_{j=0}^{m} g_j(a_1, \ldots, a_{n-1}) x_n^j .$$

By hypothesis, $f_a(a_n) = 0$ for all $a_n \in k$. Hence, by the induction hypothesis, f_a is the zero polynomial; that is, its coefficients $g_k(a_1, \ldots, a_{n-1})$ are equal to zero for all j, $0 \leq j \leq m$. But $(a_1, \ldots, a_{n-1})$ was an arbitrary point in k^{n-1}, hence the evaluation function corresponding to g_j is the zero function for $j = 1, \ldots, m$, which, by the induction hypothesis, implies that g_j is the zero polynomial for $j = 1, \ldots, m$, as required. Thus the proposition holds. □

The proposition yields the following result.

Corollary 1.1.2. *If k is an infinite field and f and g are elements of $k[x_1, \ldots, x_n]$, then $f = g$ in $k[x_1, \ldots, x_n]$ if and only if the functions $f : k^n \to k$ and $g : k^n \to k$ are equal.*

Proof. Suppose f and g in $k[x_1, \ldots, x_n]$ define the same function on k^n. Then $f - g$ is the zero function. Hence, by Proposition 1.1.1, $f - g$ is the zero polynomial in $k[x_1, \ldots, x_n]$, so that $f = g$ in $k[x_1, \ldots, x_n]$. The converse is clear. □

Throughout this chapter, unless otherwise indicated k will denote an arbitrary field. The main geometric object of study in this chapter is what is called an *affine variety* in k^n, defined as follows.

Definition 1.1.3. Let k be a field and let $f_1, \ldots, f_s$ be (finitely many) elements of $k[x_1, \ldots, x_n]$. The *affine variety* defined by the polynomials $f_1, \ldots, f_s$ is the set

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \ : \ f_j(a_1, \ldots, a_n) = 0 \text{ for } 1 \leq j \leq s\} .$$

An *affine variety* is a subset V of k^n for which there exist finitely many polynomials such that $V = \mathbf{V}(f_1, \ldots, f_s)$. A *subvariety* of V is a subset of V that is itself an affine variety.

In other words, the affine variety $\mathbf{V}(f_1, \ldots, f_s) \subset k^n$ is the set of solutions of the system

$$f_1 = 0, \ f_2 = 0, \ \ldots, \ f_s = 0 \tag{1.3}$$

of finitely many polynomial equations in k^n. Of course, this set depends on k and could very well be empty: $\mathbf{V}(x^2 + y^2 + 1) = \varnothing$ for $k = \mathbb{R}$ but not for $k = \mathbb{C}$, while $\mathbf{V}(x^2 + y^2 + 1, x, y) = \varnothing$ no matter what k is, since k is a field.

The following proposition gives an important property of affine varieties. The proof is left as Exercise 1.3, in which the reader is asked to prove in addition that the arbitrary (that is, possibly infinite) intersection of affine varieties is still an affine variety.

Proposition 1.1.4. *If $V \subset k^n$ and $W \subset k^n$ are affine varieties, then $V \cup W$ and $V \cap W$ are also affine varieties.*

It is easy to see that, given an affine variety V, the collection of polynomials $\{f_1,\dots,f_s\}$ such that $V=\mathbf{V}(f_1,\dots,f_s)$ is not unique, and thus cannot be uniquely recovered from the point set V. For example, for any a and b in k, $a\neq 0$, it is apparent that $\mathbf{V}(f_1,\dots,f_s)=\mathbf{V}(af_1+bf_2,f_2,\dots,f_s)$. See also Example 1.1.13 and Proposition 1.1.11. In order to connect a given variety with a particular collection of polynomials, we need the concept of an ideal, the main algebraic object of study in this chapter.

Definition 1.1.5. An *ideal* of $k[x_1,\dots,x_n]$ is a subset I of $k[x_1,\dots,x_n]$ satisfying
(a) $0\in I$,
(b) if $f,g\in I$ then $f+g\in I$, and
(c) if $f\in I$ and $h\in k[x_1,\dots,x_n]$, then $hf\in I$.

Let $f_1,\dots,f_s$ be elements of $k[x_1,\dots,x_n]$. We denote by $\langle f_1,\dots,f_s\rangle$ the set of all linear combinations of $f_1,\dots,f_s$ with coefficients from $k[x_1,\dots,x_n]$:

$$\langle f_1,\dots,f_s\rangle=\left\{\sum_{j=1}^{s}h_jf_j\ :\ h_1,\dots,h_s\in k[x_1,\dots,x_n]\right\}. \tag{1.4}$$

It is easily seen that the set $\langle f_1,\dots,f_s\rangle$ is an ideal in $k[x_1,\dots,x_n]$. We call $\langle f_1,\dots,f_s\rangle$ the *ideal generated by the polynomials* $f_1,\dots,f_s$, and the polynomials themselves *generators* of I. A generalization of this idea that will be important later is the following: if F is any nonempty subset of $k[x_1,\dots,x_n]$ (possibly infinite), then we let $\langle f:f\in F\rangle$ denote the set of all *finite* linear combinations of elements of F with coefficients from $k[x_1,\dots,x_n]$. (Occasionally we will abbreviate the notation to just $\langle F\rangle$.) Then $\langle f:f\in F\rangle$ is also an ideal, the *ideal generated by the elements of* F, which are likewise called its generators (Exercise 1.4; see Exercise 1.38). An arbitrary ideal $I\subset k[x_1,\dots,x_n]$ is called *finitely generated* if there exist polynomials $f_1,\dots,f_s\in k[x_1,\dots,x_n]$ such that $I=\langle f_1,\dots,f_s\rangle$; the set $f_1,\dots,f_s$ is called a *basis* of I. The concept of an ideal arises in the context of arbitrary commutative rings. In that setting an ideal need not be finitely generated, but in a polynomial ring over a field it must be:

Theorem 1.1.6 (Hilbert Basis Theorem). *If k is a field, then every ideal in the polynomial ring $k[x_1,\dots,x_n]$ is finitely generated.*

For a proof of the Hilbert Basis Theorem the reader is referred to [1, 60, 132, 195].

Corollary 1.1.7. *Every ascending chain of ideals $I_1\subset I_2\subset I_3\subset\cdots$ in a polynomial ring over a field k stabilizes. That is, there exists $m\geq 1$ such that for every $j>m$, $I_j=I_m$.*

Proof. Let $I_1\subset I_2\subset I_3\subset\cdots$ be an ascending chain of ideals in $k[x_1,\dots,x_n]$ and set $I=\cup_{j=1}^{\infty}I_j$, clearly an ideal in $k[x_1,\dots,x_n]$. By the Hilbert Basis Theorem there exist $f_1,\dots,f_s$ in $k[x_1,\dots,x_n]$ such that $I=\langle f_1,\dots,f_s\rangle$. Choose any $N\in\mathbb{N}$ such that $F=\{f_1,\dots,f_s\}\subset I_N$, and suppose that $g\in I_p$ for some $p\geq N$. Since $g\in I$ and F is a basis for I, there exist $h_1,\dots,h_s\in k[x_1,\dots,x_n]$ such that $g=h_1f_1+\cdots+h_sf_s$.

But then because $F \subset I_N$ and I_N is an ideal, $g \in I_N$. Thus $I_p \subset I_N$, and the ascending chain has stabilized by I_N. □

Rings in which every strictly ascending chain of ideals stabilizes are called *Noetherian* rings. The Hilbert Basis Theorem and its corollary hold under the milder condition that k be only a commutative Noetherian ring. Some condition is necessary, though, which is why in the statements above we explicitly included the condition that k be a field, which is enough for our puposes.

Occasionally we will find that it is important not to distinguish between two polynomials whose difference lies in a particular ideal I. Thus, we define a relation on $k[x_1,\ldots,x_n]$ by saying that f and g are related if $f-g \in I$. This relation is an equivalence relation (Exercise 1.5) and is the basis for the following definition.

Definition 1.1.8. Let I be an ideal in $k[x_1,\ldots,x_n]$. Two polynomials f and g in $k[x_1,\ldots,x_n]$ are congruent modulo I, denoted $f \equiv g \bmod I$, if $f-g \in I$. The set of equivalence classes is denoted $k[x_1,\ldots,x_n]/I$.

As a simple example, if in $\mathbb{R}[x]$ we take $I = \langle x \rangle$, then $f \equiv g \bmod I$ precisely when $f(x) - g(x) = xh(x)$ for some polynomial h. Hence f and g are equivalent if and only if they have the same constant term.

If for $f \in k[x_1,\ldots,x_n]$ the equivalence class of f is denoted $[f]$, then for any f_1 and f_2 in $[f]$ and for any g_1 and g_2 in $[g]$, $(f_1+g_1)-(f_2+g_2) \in I$ and $f_1g_1 - f_2g_2 \in I$. We conclude that an addition and multiplication are defined on $k[x_1,\ldots,x_n]/I$ by $[f]+[g] = [f+g]$ and $[f][g] = [fg]$, which give it the structure of a ring (Exercise 1.6).

Suppose $f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$ and consider system (1.3), whose solution set is the affine variety $V = \mathbf{V}(f_1,\ldots,f_s)$. The reader may readily verify that for any $\mathbf{a} \in k^n$, $\mathbf{a} \in V$ if and only if $f(\mathbf{a}) = 0$ for *every* $f \in I = \langle f_1,\ldots,f_s \rangle$. V is the set of common zeros of the full (typically infinite) set I of polynomials. Moreover, given the ideal I, as the following proposition states, the particular choice of generators is unimportant; the same variety will be determined. Thus, it is the *ideal* that determines the variety, and not the particular collection of polynomials $f_1,\ldots,f_s$.

Proposition 1.1.9. *Let $f_1,\ldots,f_s$ and $g_1,\ldots,g_m$ be bases of an ideal $I \in k[x_1,\ldots,x_n]$, that is, $I = \langle f_1,\ldots,f_s \rangle = \langle g_1,\ldots,g_m \rangle$. Then $\mathbf{V}(f_1,\ldots,f_s) = \mathbf{V}(g_1,\ldots,g_m)$.*

The straightforward proof is left to the reader.

We have seen how a finite collection of polynomials defines a variety. Conversely, given a variety V, there is naturally associated to it an ideal. As already noted, the collection of polynomials in a system (1.3) for which V is the solution set is not unique, and neither is the ideal they generate, although any such ideal has the property that V is precisely the subset of k^n on which every element of the ideal vanishes. The ideal naturally associated to V is the one given in the following definition.

Definition 1.1.10. Let $V \subset k^n$ be an affine variety. The *ideal of the variety V* is the set

$$\mathbf{I}(V) = \{ f \in k[x_1,\ldots,x_n] \ : \ f(a_1,\ldots,a_n) = 0 \text{ for all } (a_1,\ldots,a_n) \in V \}.$$

In Exercise 1.7 the reader is asked to show that $\mathbf{I}(V)$ *is* an ideal in $k[x_1,\ldots,x_n]$, even if V is not a variety, but simply an arbitrary subset of k^n. (See also the discussion following Theorem 1.3.18.)

The ideal naturally associated to a variety V bears the following relation to the family of ideals that come from the polynomials in any system of equations that define V.

Proposition 1.1.11. *Let $f_1,\ldots,f_s$ be elements of $k[x_1,\ldots,x_n]$. Then the set inclusion $\langle f_1,\ldots,f_s\rangle \subset \mathbf{I}(\mathbf{V}(f_1,\ldots,f_s))$ always holds, but could be strict.*

Proof. Let $f \in \langle f_1,\ldots,f_s\rangle$. Then there exist $h_1,\ldots,h_s \in k[x_1,\ldots,x_n]$ such that $f = h_1f_1 + \cdots + h_sf_s$. Since $f_1,\ldots,f_s$ all vanish on $\mathbf{V}(f_1,\ldots,f_s)$, so does f, so $f \in \mathbf{I}(\mathbf{V}(f_1,\ldots,f_s))$. The demonstration that the inclusion can be strict is given by Example 1.1.13. □

When V is not just a subset of k^n but a variety, the ideal $\mathbf{I}(V)$ naturally determined by V uniquely determines V:

Proposition 1.1.12. *Let V and W be affine varieties in k^n. Then*
1. $V \subset W$ if and only if $\mathbf{I}(W) \subset \mathbf{I}(V)$.
2. $V = W$ if and only if $\mathbf{I}(W) = \mathbf{I}(V)$.

Proof. (1) Suppose $V \subset W$. Then any polynomial that vanishes on W also vanishes on V, so $\mathbf{I}(W) \subset \mathbf{I}(V)$. Suppose conversely that $\mathbf{I}(W) \subset \mathbf{I}(V)$. Choose any collection $\{h_1,\ldots,h_s\} \subset k[x_1,\ldots,x_n]$ such that $W = \mathbf{V}(h_1,\ldots,h_s)$, which must exist, since W is a variety. Then for $1 \le j \le s$, $h_j \in \mathbf{I}(W) \subset \mathbf{I}(V)$, so that if $\mathbf{a} \in V$, then $h_j(\mathbf{a}) = 0$. That is, if $\mathbf{a} \in V$, then $\mathbf{a} \in \mathbf{V}(h_1,\ldots,h_s) = W$, so $V \subset W$.

Statement (2) is an immediate consequence of statement (1). □

Example 1.1.13. Let $V = \{(0,0)\} \subset \mathbb{R}^2$. Then $\mathbf{I}(V)$ is the set of all polynomials in two variables without constant term. We will express V as $\mathbf{V}(f_1,f_2)$ in two different ways. Choosing $f_1 = x$ and $f_2 = y$, $V = \mathbf{V}(f_1,f_2)$ and $I = \langle x,y\rangle$ is the same ideal as $\mathbf{I}(V)$. Choosing $f_1 = x^2$ and $f_2 = y$, $V = \mathbf{V}(f_1,f_2)$, but $J = \langle x^2,y\rangle$ is the set of elements of $\mathbb{R}[x,y]$, every term of which contains x^2 or y; hence $J \subsetneq \mathbf{I}(V)$. Note that both I and J have the property that V is precisely the set of common zeros of all their elements.

Denote by $\mathbb{V}$ the set of all affine varieties of k^n and by $\mathbb{I}$ the set of all polynomial ideals in $k[x_1,\ldots,x_n]$. Then Definition 1.1.10 defines a map

$$\mathbf{I} : \mathbb{V} \to \mathbb{I}. \tag{1.5}$$

Because every ideal I of $k[x_1,\ldots,x_n]$ has a finite basis (Theorem 1.1.6), so that $I = \langle f_1,\ldots,f_s\rangle$, and because the variety defined using any basis of I is the same as that defined using any other (Proposition 1.1.9), there is also a natural map from $\mathbb{I}$ to $\mathbb{V}$ defined by

$$\mathbf{V} : \mathbb{I} \to \mathbb{V} : \langle f_1,\ldots,f_s\rangle \mapsto \mathbf{V}(f_1,\ldots,f_s). \tag{1.6}$$

That is, for an ideal I in $k[x_1,\ldots,x_n]$, $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_s)$ for any finite collection of polynomials satisfying $I = \langle f_1,\ldots,f_s\rangle$. Thus the symbol $\mathbf{V}$ will be doing double duty, since we will continue to write $\mathbf{V}(f_1,\ldots,f_s)$ in place of the more cumbersome $\mathbf{V}(\langle f_1,\ldots,f_s\rangle)$. The following theorem establishes some properties of the maps $\mathbf{I}$ and $\mathbf{V}$. (See also Theorem 1.3.15.)

Theorem 1.1.14. *For any field k, the maps $\mathbf{I}$ and $\mathbf{V}$ are inclusion-reversing. $\mathbf{I}$ is one-to-one (injective) and $\mathbf{V}$ is onto (surjective). Furthermore, for any variety $V \subset k^n$, $\mathbf{V}(\mathbf{I}(V)) = V$.*

Proof. In Exercise 1.8 the reader is asked to show that the maps $\mathbf{I}$ and $\mathbf{V}$ are inclusion-reversing. Now let an affine variety $V = \mathbf{V}(f_1,\ldots,f_s)$ of k^n be given. Since $\mathbf{I}(V)$ is the collection of *all* polynomials that vanish on V, if $\mathbf{a} \in V$, then every element of $\mathbf{I}(V)$ vanishes at $\mathbf{a}$, so $\mathbf{a}$ is in the set of common zeros of $\mathbf{I}(V)$, which is $\mathbf{V}(\mathbf{I}(V))$. Thus, $V \subset \mathbf{V}(\mathbf{I}(V))$. For the reverse inclusion, by the definition of $\mathbf{I}(V)$, $f_j \in \mathbf{I}(V)$, $1 \le j \le s$; hence, $\langle f_1,\ldots,f_s\rangle \subset \mathbf{I}(V)$. Since $\mathbf{V}$ is inclusion-reversing, $\mathbf{V}(\mathbf{I}(V)) \subset \mathbf{V}(\langle f_1,\ldots,f_s\rangle) = \mathbf{V}(f_1,\ldots,f_s) = V$.

Finally, $\mathbf{I}$ is one-to-one because it has a left inverse, and $\mathbf{V}$ is onto because it has a right inverse. □

1.2 The Ideal Membership Problem and Gröbner Bases

One of the main problems of computational algebra is the *Ideal Membership Problem*, formulated as follows.

> **Ideal Membership Problem.** Let $I \subset k[x_1,\ldots,x_n]$ be an ideal and let f be an element of $k[x_1,\ldots,x_n]$. Determine whether or not f is an element of I.

We first consider the polynomial ring with one variable x. One important feature of this ring is the existence of the Division Algorithm: given two polynomials f and g in $k[x]$, $g \neq 0$, there exist unique elements q and r of $k[x]$, the *quotient* and *remainder*, respectively, of f upon division by g, such that $f = qg + r$, and either $r = 0$ or $\deg(r) < \deg(g)$. To *divide* f by g is to express f as $f = qg + r$. We say that g *divides* f if $r = 0$, and write it as $g \mid f$. As outlined in Exercises 1.9–1.12, the greatest common divisor of two polynomials in $k[x]$ is defined, is easily computed using the Euclidean Algorithm, and can be used in conjunction with the Hilbert Basis Theorem to show that every ideal in $k[x]$ is generated by a single element. (An ideal generated by a single element is called a *principal* ideal, and a ring in which every ideal is principal is a *principal ideal domain*). The Ideal Membership Problem is then readily solved: given an ideal I and a polynomial f, we first find a generator g for I, then divide f by g; $f \in I$ if and only if $g \mid f$.

In polynomial rings of several variables, we want to follow an analogous procedure for solving the Ideal Membership Problem: performing a division and examining a remainder. Matters are more complicated, however. In particular, in general

ideals are not generated by just one polynomial, so we have to formulate a procedure for dividing a polynomial f by a set F of polynomials, and although there is a way to generalize the Division Algorithm to do this for elements of $k[x_1,\dots,x_n]$, a complication arises in that the remainder under the division is not necessarily unique.

To describe the division algorithm in $k[x_1,\dots,x_n]$, we must digress for several paragraphs to introduce the concepts of a term ordering and of reduction of a polynomial modulo a set of polynomials, along with attendant terminology. We first of all specify an ordering on the terms of the polynomials. In the case of one variable there is the natural ordering according to degree. In the multivariable case there are different orders that can be used. We will define the general concept of a *term order* and a few of the most frequently used term orders. Observe that because of the one-to-one correspondence between monomials $\mathbf{x}^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ and n-tuples $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}_0^n$, it is sufficient to order elements of $\mathbb{N}_0^n$ (for, as in the one-variable case, the actual coefficients of the terms play no role in the ordering). Underlying this correspondence, of course, is the assumption of the ordering $x_1 > x_2 > \cdots > x_n$ of the variables themselves.

Recall that a *partial order* $\succ$ on a set S is a binary relation that is reflexive ($a \succ a$ for all $a \in S$), antisymmetric ($a \succ b$ and $b \succ a$ only if $a = b$), and transitive ($a \succ b$ and $b \succ c$ implies $a \succ c$). A *total order* $>$ on S is a partial order under which any two elements can be compared: for all a and b in S, either $a = b$, $a > b$, or $b > a$.

Definition 1.2.1. A *term order* on $k[x_1,\dots,x_n]$ is a total order $>$ on $\mathbb{N}_0^n$ having the following two properties:
(a) for all α, β, and γ in $\mathbb{N}_0^n$, if $\alpha > \beta$, then $\alpha+\gamma > \beta+\gamma$; and
(b) $\mathbb{N}_0^n$ is *well-ordered* by $>$: if S is any nonempty subset of $\mathbb{N}_0^n$, then there exists a smallest element μ of S (for all $\alpha \in S \setminus \{\mu\}$, $\alpha > \mu$).

The monomials $\{\mathbf{x}^\alpha : \alpha \in \mathbb{N}_0\}$ are then ordered by the ordering of their exponents, so that $\mathbf{x}^\alpha > \mathbf{x}^\beta$ if and only if $\alpha > \beta$. Note that while we speak of the term order $>$ as being on $k[x_1,\dots,x_n]$, we are not actually ordering all elements of $k[x_1,\dots,x_n]$, but only the monomials, hence the individual terms of the polynomials that comprise $k[x_1,\dots,x_n]$; this explains the terminology *term order*. The terminology *monomial order* is also widely used.

A sequence α_j in $\mathbb{N}_0^n$ is *strictly descending* if, for all j, $\alpha_j > \alpha_{j+1}$ and $\alpha_j \neq \alpha_{j+1}$. Such a sequence *terminates* if it is finite.

Proposition 1.2.2. *A total order $>$ on $\mathbb{N}_0^n$ well-orders $\mathbb{N}_0^n$ if and only if each strictly descending sequence of elements of $\mathbb{N}_0^n$ terminates.*

Proof. If there exists a strictly descending sequence $\alpha_1 > \alpha_2 > \alpha_3 > \cdots$ that does not terminate, then $\{\alpha_1, \alpha_2, \dots\}$ is a nonempty subset of $\mathbb{N}_0^n$ with no minimal element, and $>$ does not well-order $\mathbb{N}_0^n$.

Conversely, if $>$ does not well-order $\mathbb{N}_0^n$, then there exists a nonempty subset A of $\mathbb{N}_0^n$ that has no minimal element. Let α_1 be an arbitrary element of A. It is not minimal; hence there exists $\alpha_2 \in A$, $\alpha_2 \neq \alpha_1$, such that $\alpha_1 > \alpha_2$. Continuing the process, we get a strictly descending sequence that does not terminate. □

We now define the three most commonly used term orders; in Exercise 1.16 we ask the reader to verify that they indeed meet the conditions in Definition 1.2.1. Addition and rescaling in $\mathbb{Z}^n$ are performed componentwise: for α, $\beta \in \mathbb{Z}^n$ and $p \in \mathbb{Z}$, the jth entry of $\alpha + p\beta$ is the jth entry of α plus p times the jth entry of β. The word "graded" is sometimes used where we use the word "degree."

Definition 1.2.3. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be elements of $\mathbb{N}_0^n$.
(a) Lexicographic Order. Define $\alpha >_{\text{lex}} \beta$ if and only if, reading left to right, the first nonzero entry in the n-tuple $\alpha - \beta \in \mathbb{Z}^n$ is positive.
(b) Degree Lexicographic Order. Define $\alpha >_{\text{deglex}} \beta$ if and only if

$$|\alpha| = \sum_{j=1}^{n} \alpha_j > |\beta| = \sum_{j=1}^{n} \beta_j \qquad \text{or} \qquad |\alpha| = |\beta| \text{ and } \alpha >_{\text{lex}} \beta\,.$$

(c) Degree Reverse Lexicographic Order. Define $\alpha >_{\text{degrev}} \beta$ if and only if either $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and, reading right to left, the first nonzero entry in the n-tuple $\alpha - \beta \in \mathbb{Z}^n$ is negative.

For example, if $\alpha = (1,4,4,2)$ and $\beta = (1,2,6,2)$, then α is greater than β with respect to all three orders. Note in particular that this example shows that degrev is not simply the reverse of deglex.

When a term order $>$ on $k[x_1, \ldots, x_n]$ is given, we write $a_\alpha \mathbf{x}^\alpha > a_\beta \mathbf{x}^\beta$ if and only if $\alpha > \beta$. We reiterate that the definitions above are based on the presumed ordering $x_1 > \cdots > x_n$ of the variables. This ordering must be explicitly identified when non-subscripted variables are in use. For instance, if in $k[x,y]$ we choose $y > x$, then $y^5 >_{\text{lex}} x^9$ (since $(5,0) >_{\text{lex}} (0,9)$) and $xy^4 >_{\text{deglex}} x^2y^3$ (since $4+1 = 3+2$ and $(4,1) >_{\text{lex}} (3,2)$), and we will typically write these latter two terms as y^4x and y^3x^2 to reflect the underlying ordering of the variables themselves.

Fixing a term order $>$ on $k[x_1, \ldots, x_n]$, any nonzero $f \in k[x_1, \ldots, x_n]$ may be written in the *standard form*, with respect to $>$,

$$f = a_1\mathbf{x}^{\alpha_1} + a_2\mathbf{x}^{\alpha_2} + \cdots + a_s\mathbf{x}^{\alpha_s}, \tag{1.7}$$

where $a_j \neq 0$ for $j = 1, \ldots, s$, $\alpha_i \neq \alpha_j$ for $i \neq j$ and $1 \leq i, j \leq s$, and where, with respect to the specified term order, $\alpha_1 > \alpha_2 > \cdots > \alpha_s$.

Definition 1.2.4. Let a term order on $k[x_1, \ldots, x_n]$ be specified and let f be a nonzero element of $k[x_1, \ldots, x_n]$, written in the standard form (1.7).
(a) The *leading term* $\text{LT}(f)$ of f is the term $\text{LT}(f) = a_1\mathbf{x}^{\alpha_1}$.
(b) The *leading monomial* $\text{LM}(f)$ of f is the monomial $\text{LM}(f) = \mathbf{x}^{\alpha_1}$.
(c) The *leading coefficient* $\text{LC}(f)$ of f is the coefficient $\text{LC}(f) = a_1$.

The concept of division of single-variable polynomials has an obvious generalization to the case of division of one monomial by another: we say that a monomial $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ *divides* a monomial $\mathbf{x}^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n}$, written $\mathbf{x}^\alpha \mid \mathbf{x}^\beta$, if and only if $\beta_j \geq \alpha_j$ for all j, $1 \leq j \leq n$. In such a case the notation $\mathbf{x}^\beta/\mathbf{x}^\alpha$ denotes the monomial

$x_1^{\beta_1-\alpha_1}\cdots x_n^{\beta_n-\alpha_n}$. In $k[x_1,\ldots,x_n]$, to divide a polynomial f by nonzero polynomials $\{f_1,\ldots,f_s\}$ means to represent f in the form

$$f = u_1 f_1 + \cdots + u_s f_s + r,$$

where $u_1,\ldots,u_s, r \in k[x_1,\ldots,x_n]$, and either $r = 0$ or $\deg(r) \le \deg(f)$ (the inequality is not strict). The most important part of this expression is the remainder r, not the weights u_j, for the context in which we intend to apply the division concept is that the f_i are generators of an ideal I, and we want the division to produce a zero remainder r if and only if f is in I.

We must first specify a term order on $k[x_1,\ldots,x_n]$. The main idea then of the algorithm for the division is the same as in the one-variable case: we reduce the leading term of f (as determined by the specified term order) by multiplying some f_j by an appropriate term and subtracting. We will describe the procedure in detail, but to understand the motivation for the following definition, recall that in the familiar one-variable case of polynomial long division, in the first pass through the algorithm dividing, for example, $f = 6x^3 + \cdots$ (lower-order terms omitted) by $g = 7x^2 + \cdots$, we compare the leading terms, multiply g by $\frac{6}{7}x = \frac{6x^3}{7x^2} = \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}$, and then subtract the product from f to obtain a polynomial $h = f - \frac{6}{7}xg$ that satisfies $\deg(h) < \deg(f)$.

Definition 1.2.5. (a) For $f, g, h \in k[x_1,\ldots,x_n]$ with $g \neq 0$, we say that f *reduces to* h *modulo* g *in one step*, written as

$$f \xrightarrow{g} h,$$

if and only if $\mathrm{LM}(g)$ divides a nonzero term X that appears in f and

$$h = f - \frac{X}{\mathrm{LT}(g)}g. \tag{1.8}$$

(b) For $f, f_1,\ldots,f_s, h \in k[x_1,\ldots,x_n]$ with $f_j \neq 0$, $1 \le j \le s$, letting $F = \{f_1,\ldots,f_s\}$, we say that f *reduces to* h *modulo* F, written as

$$f \xrightarrow{F} h,$$

if and only if there exist a sequence of indices $j_1, j_2, \ldots, j_m \in \{1,\ldots,s\}$ and a sequence of polynomials $h_1,\ldots,h_{m-1} \in k[x_1,\ldots,x_n]$ such that

$$f \xrightarrow{f_{j_1}} h_1 \xrightarrow{f_{j_2}} h_2 \xrightarrow{f_{j_3}} \cdots \xrightarrow{f_{j_{m-1}}} h_{m-1} \xrightarrow{f_{j_m}} h.$$

Remark 1.2.6. Applying part (a) of the definition repeatedly shows that if $f \xrightarrow{F} h$, then there exist $u_j \in k[x_1,\ldots,x_n]$ such that $f = u_1 f_1 + \cdots + u_s f_s + h$. Hence, by Definition 1.1.8 f, reduces to h modulo $F = \{f_1,\ldots,f_s\}$ only if $f \equiv h \bmod \langle f_1,\ldots,f_s\rangle$. The converse is false, as shown by Example 1.2.12.

Example 1.2.7. We illustrate each part of Definition 1.2.5.
(a) In $\mathbb{Q}[x,y]$ with $x > y$ and the term order deglex, let $f = x^2y + 2xy - 3x + 5$ and

$g = xy + 6y^2 - 4x$. If the role of X is played by the leading term x^2y in f, then

$$h = f - \frac{x^2y}{xy}\left(xy + 6y^2 - 4x\right) = -6xy^2 + 4x^2 + 2xy - 3x + 5,$$

so $f \xrightarrow{g} h$ and $\mathrm{LM}(h) < \mathrm{LM}(f)$. If the role of X is played by the term $2xy$ in f, then

$$\tilde{h} = f - \frac{2xy}{xy}\left(xy + 6y^2 - 4x\right) = x^2y - 12y^2 + 5x + 5,$$

so $f \xrightarrow{g} \tilde{h}$ and $\mathrm{LT}(\tilde{h}) = \mathrm{LT}(f)$. In either case we remove the term X from f and replace it with a term that is smaller with respect to deglex.
(b) In $\mathbb{Q}[x,y]$ with $y > x$ and the term order deglex, let $f = y^2x + y^2 + 3y$, $f_1 = yx + 2$, and $f_2 = y + x$. Then

$$y^2x + y^2 + 3y \xrightarrow{f_1} y^2 + y \xrightarrow{f_2} -yx + y \xrightarrow{f_2} x^2 + y,$$

so $f \xrightarrow{\{f_1, f_2\}} x^2 + y$.

Definition 1.2.8. Suppose $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, $f_j \neq 0$ for $1 \leq j \leq s$, and let $F = \{f_1, \ldots, f_s\}$.
(a) A polynomial $r \in k[x_1, \ldots, x_n]$ is *reduced with respect to* F if either $r = 0$ or no monomial that appears in the polynomial r is divisible by any element of the set $\{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s)\}$.
(b) A polynomial $r \in k[x_1, \ldots, x_n]$ is a *remainder for* f *with respect to* F if $f \xrightarrow{F} r$ and r is reduced with respect to F.

The Multivariable Division Algorithm is the direct analogue of the procedure used to divide one single-variable polynomial by another. To divide f by the ordered set $F = \{f_1, \ldots, f_s\}$, we proceed iteratively, at each step performing a familiar polynomial long division using one element of F. Typically, the set F of divisors is presented to us in no particular order, so as a preliminary we must order its elements in some fashion; the order selected can affect the final result. At the first step in the actual division process, the "active divisor" is the first element of F, call it f_j, whose leading term divides the leading term of f; at this step we replace f by the polynomial h of (1.8) when $X = \mathrm{LT}(f)$ and $g = f_j$, thereby reducing f somewhat using f_j. At each succeeding step, the active divisor is the first element of F whose leading term divides the leading term of the current polynomial h; at this step we similarly reduce h somewhat using the active divsior. If at any stage no division is possible, then the leading term of h is added to the remainder, and we try the same process again, continuing until no division is possible at all. By Exercise 1.17, building up the remainder successively is permissible. An explicit description of the procedure is given in Table 1.1 on page 12. In the next theorem we will prove that the algorithm works correctly to perform the reduction $f \xrightarrow{F} r$ and generate the components of the expression $f = u_1f_1 + \cdots + u_sf_s + r$, where r is a remainder for f with respect to F (thus showing that a remainder always exists), but first we present an example.

Multivariable Division Algorithm

Input:

$f \in k[x_1,\ldots,x_n]$
ordered set $F = \{f_1,\ldots,f_s\} \subset k[x_1,\ldots,x_n] \setminus \{0\}$

Output:

$u_1,\ldots,u_s,r \in k[x_1,\ldots,x_n]$ such that
1. $f = u_1 f_1 + \cdots + u_s f_s + r$,
2. r is reduced with respect to $\{f_1,\ldots,f_s\}$, and
3. $\max(\mathrm{LM}(u_1)\mathrm{LM}(f_1),\ldots,\mathrm{LM}(u_s)\mathrm{LM}(f_s),\mathrm{LM}(r)) = \mathrm{LM}(f)$

Procedure:

$u_1 := 0;\ \ldots,\ u_s := 0;\ r := 0;\ h := f$
WHILE $h \neq 0$ DO
  IF
  There exists j such that $\mathrm{LM}(f_j)$ divides $\mathrm{LM}(h)$
  THEN
  For the least j such that $\mathrm{LM}(f_j)$ divides $\mathrm{LM}(h)$
  $u_j := u_j + \dfrac{\mathrm{LT}(h)}{\mathrm{LT}(f_j)}$
  $h := h - \dfrac{\mathrm{LT}(h)}{\mathrm{LT}(f_j)} f_j$
  ELSE
  $r := r + \mathrm{LT}(h)$
  $h := h - \mathrm{LT}(h)$

Table 1.1 The Multivariable Division Algorithm

Example 1.2.9. In $\mathbb{Q}[x,y]$ with $x > y$ and the term order lex, we apply the algorithm to divide $f = x^2y + xy^3 + xy^2$ by the polynomials $f_1 = xy + 1$ and $f_2 = y^2 + 1$, ordered f_1 then f_2.

The two panels in Table 1.2 on page 14 show the computation in tabular form and underscore the analogy with the one-variable case. The top panel shows three divsions by f_1, at which point no division (by either divisor) is possible. The leading term $-x$ is sent to the remainder, and the process is restarted. Division by f_1 is impossible, but the bottom panel shows one further division by f_2, and then all remaining terms are sent to the remainder. Therefore,

$$f = u_1 f_1 + u_2 f_2 + r = (x + y^2 + y) f_1 + (-1) f_2 + (-x - y + 1).$$

That is, the quotient is $\{u_1, u_2\} = \{x + y^2 + y, -1\}$ and the remainder is $-x - y + 1$. (In general, the role of the divisor on each step will alternate between the f_j, so that in a hand computation the full table will contain more than s panels, and successive dividends when f_j is the active divisor must be added to obtain u_j.)

Now let us go through exactly the same computation by means of an explicit application of the Multivariable Division Algorithm. That is, we will follow the instructions presented in Table 1.1 in a step-by-step fashion.

First pass:
$\mathrm{LM}(f_1) \mid \mathrm{LM}(h)$ but $\mathrm{LM}(f_2) \nmid \mathrm{LM}(h)$
f_1 is least
$u_1 = 0 + \frac{x^2y}{xy} = x$
$h = (x^2y + xy^3 + xy^2) - x(xy+1) = xy^3 + xy^2 - x$

Second pass:
$\mathrm{LM}(f_1) \mid \mathrm{LM}(h)$ and $\mathrm{LM}(f_2) \mid \mathrm{LM}(h)$
f_1 is least
$u_1 = x + \frac{xy^3}{xy} = x + y^2$
$h = (xy^3 + xy^2 - x) - y^2(xy+1) = xy^2 - x - y^2$

Third pass:
$\mathrm{LM}(f_1) \mid \mathrm{LM}(h)$ and $\mathrm{LM}(f_2) \mid \mathrm{LM}(h)$
f_1 is least
$u_1 = x + y^2 + \frac{xy^2}{xy} = x + y^2 + y$
$h = (xy^2 - x - y^2) - y(xy+1) = -x - y^2 - y$

Fourth pass:
$\mathrm{LM}(f_1) \nmid \mathrm{LM}(h)$ and $\mathrm{LM}(f_2) \nmid \mathrm{LM}(h)$
$r = 0 + (-x) = -x$
$h = (-x - y^2 - y) - (-x) = -y^2 - y$

Fifth pass:
$\mathrm{LM}(f_1) \nmid \mathrm{LM}(h)$ but $\mathrm{LM}(f_2) \mid \mathrm{LM}(h)$
f_2 is least
$u_2 = 0 + \frac{-y^2}{y} = -1$
$h = (-y^2 - y) - (-1)(y^2+1) = -y + 1$

Sixth pass:
$\mathrm{LM}(f_1) \nmid \mathrm{LM}(h)$ and $\mathrm{LM}(f_2) \nmid \mathrm{LM}(h)$
$r = -x + (-y) = -x - y$
$h = (-y+1) - (-y) = 1$

Seventh pass:
$\mathrm{LM}(f_1) \nmid \mathrm{LM}(h)$ and $\mathrm{LM}(f_2) \nmid \mathrm{LM}(h)$
$r = -x - y + 1$
$h = 1 - 1 = 0$

A summary statement in the language of Definition 1.2.5 for these computations is the string of reductions and equalities

$$f \xrightarrow{f_1} h_1 \xrightarrow{f_1} h_2 \xrightarrow{f_1} h_3 = h_4 + (-x) \xrightarrow{f_2} h_5 + (-x) = h_6 + (-x-y)$$
$$= h_7 + (-x-y-1) = -x-y-1$$

or, more succinctly, $f \xrightarrow{\{f_1,f_2\}} -x-y-1$.

$$\begin{array}{rl|lll}
 & x + y^2 + y & \longleftarrow & [u_1] & r: \\
xy+1 & \overline{\left| x^2y + xy^3 + xy^2 \right.} & \longleftarrow & [f] & \\
 & \underline{x^2y \qquad\qquad + x} & & & \\
 & xy^3 + xy^2 - x & \longleftarrow & [h_1] & \\
 & \underline{xy^3 \qquad\quad + y^2} & & & \\
 & xy^2 - x - y^2 & \longleftarrow & [h_2] & \\
 & \underline{xy^2 \qquad + y} & & & \\
 & - x - y^2 - y & \longleftarrow & [h_3] & \\
\end{array}$$

$$\begin{array}{rl|lll}
 & -1 & \longleftarrow & [u_2] & \\
y^2+1 & \overline{\left| -y^2 - y \right.} & \longleftarrow & [h_4] & -x \\
 & \underline{-y^2 \quad - 1} & & & \\
 & - y + 1 & \longleftarrow & [h_5] & \\
 & 1 & \longleftarrow & [h_6] & -x-y \\
 & 0 & \longleftarrow & [h_7] & -x-y+1 \\
\end{array}$$

Table 1.2 The Computations of Example 1.2.9

Theorem 1.2.10. *Let an ordered set $F = \{f_1, \ldots, f_s\} \subset k[x_1, \ldots, x_n] \setminus \{0\}$ of nonzero polynomials and a polynomial $f \in k[x_1, \ldots, x_n]$ be given. The Multivariable Division Algorithm produces polynomials $u_1, \ldots, u_s, r \in k[x_1, \ldots, x_n]$ such that*

$$f = u_1 f_1 + \cdots + u_s f_s + r, \tag{1.9}$$

where r is a remainder for f with respect to F and

$$\mathrm{LM}(f) = \max(\mathrm{LM}(u_1)\mathrm{LM}(f_1), \ldots, \mathrm{LM}(u_s)\mathrm{LM}(f_s), \mathrm{LM}(r)), \tag{1.10}$$

where $\mathrm{LM}(u_j)\mathrm{LM}(f_j)$ is not present in (1.10) if $u_j = 0$.

Proof. The algorithm certainly produces the correct result $u_j = 0$, $1 \le j \le s$, and $r = f$ in the special cases that $f = 0$ or that no leading term in any of the divisors divides any term of f. Otherwise, after the first pass through the WHILE loop for which the IF statement is true, exactly one polynomial u_j is nonzero, and we have

$$\begin{aligned}\max[\mathrm{LM}(u_1)\mathrm{LM}(f_1),\ldots,&\mathrm{LM}(u_s)\mathrm{LM}(f_s),\mathrm{LM}(h)]\\ &= \max[\mathrm{LM}(u_1)LM(f_1),\ldots,\mathrm{LM}(u_s)\mathrm{LM}(f_s)]\,,\end{aligned} \tag{1.11}$$

which clearly holds at every succeeding stage of the algorithm. Consequently, (1.10) holds at that and every succeeding stage of the algorithm, hence holds when the algorithm terminates.

At every stage of the algorithm, $f = u_1 f_1 + \cdots + u_s f_s + r + h$ holds. Because the algorithm halts precisely when $h = 0$, this implies that on the last step (1.9) holds. Moreover, since at each stage we add to r only terms that are not divisible by $\mathrm{LT}(f_j)$ for any j, $1 \le j \le s$, r is reduced with respect to F, and thus is a remainder of f with respect to F.

To show that the algorithm must terminate, let $h_1, h_2, \ldots$ be the sequence of polynomials produced by the successive values of h upon successive passes through the WHILE loop. The algorithm fails to terminate only if for every $j \in \mathbb{N}$ there is a jth pass through the loop, hence an $h_j \neq 0$. Then $\mathrm{LM}(h_j)$ exists for each $j \in \mathbb{N}$, and the sequence $\mathrm{LM}(h_1), \mathrm{LM}(h_2), \ldots$ satisfies $\mathrm{LM}(h_{j+1}) < \mathrm{LM}(h_j)$ and $\mathrm{LM}(h_{j+1}) \neq \mathrm{LM}(h_j)$, which contradicts Proposition 1.2.2. □

If we change the order of the polynomials in Example 1.2.9, dividing first by f_2 and then by f_1, then the quotient and remainder change to $\{xy + x, x - 1\}$ and $-2x + 1$, respectively (Exercise 1.21). Thus we see that, unlike the situation in the one-variable case, the quotient and remainder are not unique. They depend on the ordering of the polynomials in the set of divisors as well as on the term order chosen for the polynomial ring (see Exercise 1.22). But what is even worse from the point of view of solving the Ideal Membership Problem is that, as the following examples show, it is even possible that, keeping the term order fixed, there exist an element of the ideal generated by the divisors whose remainder can be zero under one ordering of the divisors and different from zero under another, or even different from zero no matter how the divisors are ordered.

Example 1.2.11. In the ring $\mathbb{R}[x,y]$ fix the lexicographic term order with $x > y$ and consider the polynomial $f = x^2y + xy + 2x + 2$. When we use the Multivariable Division Algorithm to reduce the polynomial f modulo the ordered set $\{f_1 = x^2 - 1, f_2 = xy + 2\}$, we obtain

$$f = yf_1 + f_2 + (2x + y)\,.$$

Since the corresponding remainder, $2x + y$, is different from zero, we might conclude that f is not in the ideal $\langle f_1, f_2\rangle$. If, however, we change the order of the divisors so that f_2 is first, we obtain

$$f = 0 \cdot f_1 + (x + 1)f_2 + 0 = (x + 1)f_2, \tag{1.12}$$

so that $f \in \langle f_1, f_2\rangle$ after all.

Example 1.2.12. In the ring $\mathbb{R}[x,y]$ fix the lexicographic term order with $x > y$. Then $2y = 1 \cdot (x+y) + (-1) \cdot (x-y) \in \langle x+y, x-y\rangle$, but because $\mathrm{LT}(x+y) = \mathrm{LT}(x-y) = x$

does not divide $2y$ the remainder of $2y$ with respect to $\{x+y, x-y\}$ is unique and is $2y$. Thus, for either ordering of the divisors, the Multivariable Division Algorithm produces this nonzero remainder.

We see then that we have lost the tool that we had in polynomial rings of one variable for resolving the Ideal Membership Problem. Fortunately, not all is lost. While the Multivariable Division Algorithm cannot be improved in general, it has been discovered that if we use a certain special generating set for our ideals, then it is still true that $f \in \langle f_1, \ldots, f_s \rangle$ if and only if the remainder in the Division Algorithm is equal to zero, and we are able to decide the Ideal Membership Problem. Such a special generating set for an ideal is called a *Gröbner basis* or a *standard basis*. It is one of the primary tools of computational algebra and is the basis of numerous algorithms of computational algebra and algebraic geometry. To motivate the definition of a Gröbner basis we discuss Example 1.2.11 again. It showed that in the ring $k[x,y]$, under lex with $x > y$, for $f = x^2y + xy + 2x + 2$, $f_1 = x^2 - 1$, and $f_2 = xy + 2$,

$$f \xrightarrow{\{f_1, f_2\}} 2x + y.$$

But by (1.12), $f \in \langle f_1, f_2 \rangle$, so the remainder $r = 2x + y$ must also be in $\langle f_1, f_2 \rangle$. The trouble is that the leading term of r is not divisible by either $\mathrm{LM}(f_1)$ or $\mathrm{LM}(f_2)$, and this is what halts the division process in the Multivariable Division Algorithm. So the problem is that the ideal $\langle f_1, f_2 \rangle$ contains elements that are not divisible by a leading term of either element of the particular basis $\{f_1, f_2\}$ of the ideal.

If, for any ideal I, we had a basis B with the special property that the leading term of every polynomial in I was divisible by the leading term of some element of B, then the Multivariable Division Algorithm would provide an answer to the Ideal Membership Problem: a polynomial f is in the ideal I if and only if the remainder of f upon division by elements of B, in any order, is zero. This the idea behind the concept of a Gröbner basis of an ideal, and we use this special property as the defining characteristic of a Gröbner basis.

Definition 1.2.13. A *Gröbner basis* (also called a *standard basis*) of an ideal I in $k[x_1, \ldots, x_n]$ is a finite nonempty subset $G = \{g_1, \ldots, g_m\}$ of $I \setminus \{0\}$ with the following property: for every nonzero $f \in I$, there exists $g_j \in G$ such that $\mathrm{LT}(g_j) \mid \mathrm{LT}(f)$.

It is implicit in the definition that we do not consider the concept of a Gröbner basis G for the zero ideal, nor will we need it. See Section 5.2 of [18] for this more general situation, in which G must be allowed to be empty. Note that the requirement that the set G actually be a basis of the ideal I does not appear in the definition of a Gröbner basis but is a consequence of it (Theorem 1.2.16). Note also that whether or not a set G forms a Gröbner basis of an ideal I depends not only on the term order in use, but also on the underlying ordering of the variables. See Exercise 1.23.

With a Gröbner basis we again have the important property of uniqueness of the remainder, which we had in $k[x]$ and which we lost in the multivariable case for division by an arbitrary set of polynomials:

Proposition 1.2.14. *Let G be a Gröbner basis for a nonzero ideal I in $k[x_1,\ldots,x_n]$ and $f \in k[x_1,\ldots,x_n]$. Then the remainder of f with respect to G is unique.*

Proof. Suppose $f \xrightarrow{G} r_1$ and $f \xrightarrow{G} r_2$ and both r_1 and r_2 are reduced with respect to G. Since $f - r_1$ and $f - r_2$ are both in I, $r_1 - r_2 \in I$. By Definition 1.2.8, certainly $r_1 - r_2$ is reduced with respect to G. But then by Definition 1.2.13 it is immediate that $r_1 - r_2 = 0$, since it is in I. □

Definition 1.2.15. Let I be an ideal and f a polynomial in $k[x_1,\ldots,x_n]$. To *reduce f modulo the ideal I* means to find the unique remainder of f upon division by some Gröbner basis G of I. Given a nonzero polynomial g, to *reduce f modulo g* means to reduce f modulo the ideal $\langle g\rangle$.

Proposition 1.2.14 ensures that once a Gröbner basis is selected, the process is well-defined, although the remainder obtained depends on the Gröbner basis specified. We will see when this concept is applied in Section 3.7 that this ambiguity is not important in practice.

Let S be a subset of $k[x_1,\ldots,x_n]$ (possibly an ideal). We denote by $\mathrm{LT}(S)$ the set of leading terms of the polynomials that comprise S and by $\langle \mathrm{LT}(S)\rangle$ the ideal generated by $\mathrm{LT}(S)$ (the set of all finite linear combinations of elements of $\mathrm{LT}(S)$ with coefficients in $k[x_1,\ldots,x_n]$). The following theorem gives the main properties of Gröbner bases. We remind the reader that the expression $f \xrightarrow{F} h$ means that there is some sequence of reductions using the unordered set F of divisors that leads from f to h, which is not necessarily a remainder of f with respect to F. This is in contrast to the Multivariable Division Algorithm, in which F must be ordered, and the particular order selected determines a unique sequence of reductions from f to a remainder r.

Theorem 1.2.16. *Let $I \subset k[x_1,\ldots,x_n]$ be a nonzero ideal, let $G = \{g_1,\ldots,g_s\}$ be a finite set of nonzero elements of I, and let f be an arbitrary element of $k[x_1,\ldots,x_n]$. Then the following statements are equivalent:*

(i) G is a Gröbner basis for I;

(ii) $f \in I \Leftrightarrow f \xrightarrow{G} 0$;

(iii) $f \in I \Leftrightarrow f = \sum_{j=1}^{s} u_j g_j$ and $\mathrm{LM}(f) = \max_{1\le j\le s}(\mathrm{LM}(u_j)\mathrm{LM}(g_j))$;

(iv) $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$.

Proof. (i) ⇒ (ii). Let any $f \in k[x_1,\ldots,x_n]$ be given. By Theorem 1.2.10 there exists $r \in k[x_1,\ldots,x_n]$ such that $f \xrightarrow{G} r$ and r is reduced with respect to G. If $f \in I$, then $r \in I$; hence, by the definition of Gröbner basis and the fact that r is reduced with respect to G, $r = 0$. Conversely, if $f \xrightarrow{G} 0$, then obviously $f \in I$.

(ii) ⇒ (iii). Suppose $f \in I$. Then by (ii) there is a sequence of reductions

$$f \xrightarrow{g_{j_1}} h_1 \xrightarrow{g_{j_2}} h_2 \xrightarrow{g_{j_3}} \cdots \xrightarrow{g_{j_{m-1}}} h_{m-1} \xrightarrow{g_{j_m}} 0$$

which yields $f = u_1 g_1 + \cdots + u_2 g_2$ for some $u_j \in k[x_1,\ldots,x_n]$. Exactly as described in the first paragraph of the proof of Theorem 1.2.10, an equality analogous to (1.11)