2

Groebner Bases

§1 Introduction

In Chapter 1, we have seen how the algebra of the polynomial rings $k[x_1, \ldots, x_n]$ and the geometry of affine algebraic varieties are linked. In this chapter, we will study the method of Groebner bases, which will allow us to solve problems about polynomial ideals in an algorithmic or computational fashion. The method of Groebner bases is also used in several powerful computer algebra systems to study specific polynomial ideals that arise in applications. In Chapter 1, we posed many problems concerning the algebra of polynomial ideals and the geometry of affine varieties. In this chapter and the next, we will focus on four of these problems.

Problems

a. The Ideal Description Problem: Does every ideal $I \subset k[x_1, \ldots, x_n]$ have a finite generating set? In other words, can we write $I = \langle f_1, \ldots, f_s \rangle$ for some $f_i \in k[x_1, \ldots, x_n]$?
b. The Ideal Membership Problem: Given $f \in k[x_1, \ldots, x_n]$ and an ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$. Geometrically, this is closely related to the problem of determining whether $\mathbf{V}(f_1, \ldots, f_s)$ lies on the variety $\mathbf{V}(f)$.
c. The Problem of Solving Polynomial Equations: Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0.$$

Of course, this is the same as asking for the points in the affine variety $\mathbf{V}(f_1, \ldots, f_s)$.
d. The Implicitization Problem: Let V be a subset of k^n given parametrically as

$$\begin{aligned} x_1 &= g_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= g_n(t_1, \ldots, t_m). \end{aligned}$$

If the g_i are polynomials (or rational functions) in the variables t_j, then V will be an affine variety or part of one. Find a system of polynomial equations (in the x_i) that defines the variety.

Some comments are in order. Problem (a) asks whether every polynomial ideal has a finite description via generators. Many of the ideals we have seen so far do have such descriptions—indeed, the way we have specified most of the ideals we have studied has been to give a finite generating set. However, there are other ways of constructing ideals that do not lead directly to this sort of description. The main example we have seen is the ideal of a variety, $\mathbf{I}(V)$. It will be useful to know that these ideals also have finite descriptions. On the other hand, in the exercises, we will see that if we allow *infinitely* many variables to appear in our polynomials, then the answer to (a) is no.

Note that problems (c) and (d) are, so to speak, inverse problems. In (c), we ask for the set of solutions of a given system of polynomial equations. In (d), on the other hand, we are given the solutions, and the problem is to find a system of equations with those solutions.

To begin our study of Groebner bases, let us consider some special cases in which you have seen algorithmic techniques to solve the problems given above.

Example 1. When $n = 1$, we solved the ideal description problem in §5 of Chapter 1. Namely, given an ideal $I \subset k[x]$, we showed that $I = \langle g \rangle$ for some $g \in k[x]$ (see Corollary 4 of Chapter 1, §5). So ideals have an especially simple description in this case.

We also saw in §5 of Chapter 1 that the solution of the Ideal Membership Problem follows easily from the division algorithm: given $f \in k[x]$, to check whether $f \in I = \langle g \rangle$, we divide g into f:

$$f = q \cdot g + r,$$

where $q, r \in k[x]$ and $r = 0$ or $\deg(r) < \deg(g)$. Then we proved that $f \in I$ if and only if $r = 0$. Thus, we have an algorithmic test for ideal membership in the case $n = 1$.

Example 2. Next, let n (the number of variables) be arbitrary, and consider the problem of solving a system of polynomial equations:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n + b_1 &= 0, \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n + b_m &= 0, \end{aligned} \tag{1}$$

where each polynomial is linear (total degree 1).

For example, consider the system

$$\begin{aligned} 2x_1 + 3x_2 - x_3 &= 0, \\ x_1 + x_2 - 1 &= 0, \\ x_1 + x_3 - 3 &= 0. \end{aligned} \tag{2}$$

We row-reduce the matrix of the system to reduced row echelon form:

$$\begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The form of this matrix shows that x_3 is a free variable, and setting $x_3 = t$ (any element of k), we have

$$\begin{aligned} x_1 &= -t + 3, \\ x_2 &= t - 2, \\ x_3 &= t. \end{aligned}$$

These are parametric equations for a line L in k^3. The original system of equations (2) presents L as an affine variety.

In the general case, one performs row operations on the matrix of (1)

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & -b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & -b_m \end{pmatrix}.$$

until it is in *reduced row echelon form* (where the first nonzero entry on each row is 1, and all other entries in the column containing a leading 1 are zero). Then we can find all solutions of the original system (1) by substituting values for the *free variables* in the reduced row echelon form system. In some examples there may be only one solution, or no solutions. This last case will occur, for instance, if the reduced row echelon matrix contains a row $(0 \ldots 0\, 1)$, corresponding to the inconsistent equation $0 = 1$.

Example 3. Once again, take n arbitrary, and consider the subset V of k^n parametrized by

$$\begin{aligned} x_1 &= a_{11}t_1 + \cdots + a_{1m}t_m + b_1, \\ &\vdots \\ x_n &= a_{n1}t_1 + \cdots + a_{nm}t_m + b_n. \end{aligned} \tag{3}$$

We see that V is an affine linear subspace of k^n since V is the image of the mapping $F : k^m \to k^n$ defined by

$$F(t_1, \ldots, t_m) = (a_{11}t_1 + \cdots + a_{1m}t_m + b_1, \ldots, a_{n1}t_1 + \cdots + a_{nm}t_m + b_n).$$

This is a linear mapping, followed by a translation. Let us consider the implicitization problem in this case. In other words, we seek a system of linear equations [as in (1)] whose solutions are the points of V.

For example, consider the affine linear subspace $V \subset k^4$ defined by

$$\begin{aligned} x_1 &= t_1 + t_2 + 1, \\ x_2 &= t_1 - t_2 + 3, \\ x_3 &= 2t_1 - 2, \\ x_4 &= t_1 + 2t_2 - 3. \end{aligned}$$

We rewrite the equations by subtracting the x_i terms from both sides and apply the row reduction algorithm to the corresponding matrix:

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 0 & -3 \\ 2 & 0 & 0 & 0 & -1 & 0 & 2 \\ 1 & 2 & 0 & 0 & 0 & -1 & 3 \end{pmatrix}$$

(where the coefficients of the x_i have been placed after the coefficients of the t_j in each row). We obtain the reduced row echelon form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\ 0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & 3 \end{pmatrix}.$$

Because the entries in the first two columns of rows 3 and 4 are zero, the last two rows of this matrix correspond to the following two equations with no t_j terms:

$$\begin{aligned} x_1 - (1/4)x_3 - (1/2)x_4 - 3 &= 0, \\ x_2 - (3/4)x_3 + (1/2)x_4 - 3 &= 0. \end{aligned}$$

(Note that this system is also in reduced row echelon form.) These two equations define V in k^4.

The same method can be applied to find implicit equations for any affine linear subspace V given parametrically as in (3): one computes the reduced row echelon form of (3), and the rows involving only $x_1, \ldots, x_n$ give the equations for V. We thus have an algorithmic solution to the implicitization problem in this case.

Our goal in this chapter will be to develop extensions of the methods used in these examples to systems of polynomial equations of any degrees in any number of variables. What we will see is that a sort of "combination" of row-reduction and division of polynomials—the method of Groebner bases mentioned at the outset—allows us to handle all these problems.

EXERCISES FOR §1

1. Determine whether the given polynomial is in the given ideal $I \subset \mathbb{R}[x]$ using the method of Example 1.
   a. $f(x) = x^2 - 3x + 2$, $I = \langle x - 2 \rangle$.
   b. $f(x) = x^5 - 4x + 1$, $I = \langle x^3 - x^2 + x \rangle$.
   c. $f(x) = x^2 - 4x + 4$, $I = \langle x^4 - 6x^2 + 12x - 8,\ 2x^3 - 10x^2 + 16x - 8 \rangle$.
   d. $f(x) = x^3 - 1$, $I = \langle x^9 - 1,\ x^5 + x^3 - x^2 - 1 \rangle$.
2. Find a parametrization of the affine variety defined by each of the following sets of equations:
   a. In $\mathbb{R}^3$ or $\mathbb{C}^3$:

$$\begin{aligned} 2x + 3y - z &= 9, \\ x - y &= 1, \\ 3x + 7y - 2z &= 17. \end{aligned}$$

b. In $\mathbb{R}^4$ or $\mathbb{C}^4$:

$$\begin{aligned} x_1 + x_2 - x_3 - x_4 &= 0, \\ x_1 - x_2 + x_3 &= 0. \end{aligned}$$

c. In $\mathbb{R}^3$ or $\mathbb{C}^3$:

$$\begin{aligned} y - x^3 &= 0, \\ z - x^5 &= 0. \end{aligned}$$

3. Find implicit equations for the affine varieties parametrized as follows.
   a. In $\mathbb{R}^3$ or $\mathbb{C}^3$:

$$\begin{aligned} x_1 &= t - 5, \\ x_2 &= 2t + 1, \\ x_3 &= -t + 6. \end{aligned}$$

   b. In $\mathbb{R}^4$ or $\mathbb{C}^4$:

$$\begin{aligned} x_1 &= 2t - 5u, \\ x_2 &= t + 2u, \\ x_3 &= -t + u, \\ x_4 &= t + 3u. \end{aligned}$$

   c. In $\mathbb{R}^3$ or $\mathbb{C}^3$:

$$\begin{aligned} x &= t, \\ y &= t^4, \\ z &= t^7. \end{aligned}$$

4. Let $x_1, x_2, x_3, \ldots$ be an infinite collection of independent variables indexed by the natural numbers. A *polynomial* with coefficients in a field k in the x_i is a finite linear combination of (finite) monomials $x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$. Let R denote the set of all polynomials in the x_i. Note that we can add and multiply elements of R in the usual way. Thus, R is the polynomial ring $k[x_1, x_2, \ldots]$ in infinitely many variables.
   a. Let $I = \langle x_1, x_2, x_3, \ldots \rangle$ be the set of polynomials of the form $x_{t_1} f_1 + \cdots + x_{t_m} f_m$, where $f_j \in R$. Show that I is an ideal in the ring R.
   b. Show, arguing by contradiction, that I has no finite generating set. Hint: It is not enough only to consider subsets of $\{x_i : i \geq 1\}$.
5. In this problem you will show that all polynomial parametric curves in k^2 are contained in affine algebraic varieties.
   a. Show that the number of distinct monomials $x^a y^b$ of total degree $\leq m$ in $k[x, y]$ is equal to $(m+1)(m+2)/2$. [Note: This is the binomial coefficient $\binom{m+2}{2}$.]
   b. Show that if $f(t)$ and $g(t)$ are polynomials of degree $\leq n$ in t, then for m large enough, the "monomials"

$$[f(t)]^a [g(t)]^b$$

   with $a + b \leq m$ are linearly *dependent*.
   c. Deduce from part (b) that if $C : x = f(t), y = g(t)$ is any polynomial parametric curve in k^2, then C is contained in $\mathbf{V}(F)$ for some $F \in k[x, y]$.

d. Generalize parts a, b, and c of this problem to show that any polynomial parametric surface

$$x = f(t,u), \quad y = g(t,u), \quad z = h(t,u)$$

is contained in an algebraic surface $\mathbf{V}(F)$, where $F \in k[x,y,z]$.

§2 Orderings on the Monomials in $k[x_1, \ldots, x_n]$

If we examine in detail the division algorithm in $k[x]$ and the row-reduction (Gaussian elimination) algorithm for systems of linear equations (or matrices), we see that a notion of *ordering of terms* in polynomials is a key ingredient of both (though this is not often stressed). For example, in dividing $f(x) = x^5 - 3x^2 + 1$ by $g(x) = x^2 - 4x + 7$ by the standard method, we would:

- Write the terms in the polynomials in decreasing order by degree in x.
- At the first step, the leading term (the term of highest degree) in f is $x^5 = x^3 \cdot x^2 = x^3 \cdot$ (leading term in g). Thus, we would subtract $x^3 \cdot g(x)$ from f to cancel the leading term, leaving $4x^4 - 7x^3 - 3x^2 + 1$.
- Then, we would repeat the same process on $f(x) - x^3 \cdot g(x)$, etc., until we obtain a polynomial of degree less than 2.

For the division algorithm on polynomials in one variable, then we are dealing with the degree ordering on the one-variable monomials:

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1. \tag{1}$$

The success of the algorithm depends on working systematically with the leading terms in f and g, and not removing terms "at random" from f using arbitrary terms from g.

Similarly, in the row-reduction algorithm on matrices, in any given row, we systematically work with entries to the left first—leading entries are those nonzero entries farthest to the left on the row. On the level of linear equations, this is expressed by ordering the variables $x_1, \ldots, x_n$ as follows:

$$x_1 > x_2 > \cdots > x_n. \tag{2}$$

We write the terms in our equations in decreasing order. Furthermore, in an echelon form system, the equations are listed with their leading terms in decreasing order. (In fact, the precise definition of an echelon form system could be given in terms of this ordering—see Exercise 8.)

From the above evidence, we might guess that a major component of any extension of division and row-reduction to arbitrary polynomials in several variables will be an ordering on the terms in polynomials in $k[x_1, \ldots, x_n]$. In this section, we will discuss the desirable properties such an ordering should have, and we will construct several different examples that satisfy our requirements. Each of these orderings will be useful in different contexts.

First, we note that we can reconstruct the monomial $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ from the n-tuple of exponents $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. This observation establishes a one-to-one correspondence between the monomials in $k[x_1, \ldots, x_n]$ and $\mathbb{Z}_{\geq 0}^n$. Futhermore, any

ordering $>$ we establish on the space $\mathbb{Z}^n_{\geq 0}$ will give us an ordering on monomials: if $\alpha > \beta$ according to this ordering, we will also say that $x^\alpha > x^\beta$.

There are many different ways to define orderings on $\mathbb{Z}^n_{\geq 0}$. For our purposes, most of these orderings will not be useful, however, since we will want our orderings to be "compatible" with the algebraic structure of polynomial rings.

To begin, since a polynomial is a sum of monomials, we would like to be able to arrange the terms in a polynomial unambiguously in descending (or ascending) order. To do this, we must be able to compare every pair of monomials to establish their proper relative positions. Thus, we will require that our orderings be *linear or total* orderings. This means that for every pair of monomials x^α and x^β, exactly one of the three statements

$$x^\alpha > x^\beta, \qquad x^\alpha = x^\beta, \quad x^\beta > x^\alpha$$

should be true.

Next, we must take into account the effect of the sum and product operations on polynomials. When we add polynomials, after combining like terms, we may simply rearrange the terms present into the appropriate order, so sums present no difficulties. Products are more subtle, however. Since multiplication in a polynomial ring distributes over addition, it suffices to consider what happens when we multiply a monomial times a polynomial. If doing this changed the relative ordering of terms, significant problems could result in any process similar to the division algorithm in $k[x]$, in which we must identify the "leading" terms in polynomials. The reason is that the leading term in the product could be different from the product of the monomial and the leading term of the original polynomial.

Hence, we will require that all monomial orderings have the following additional property. If $x^\alpha > x^\beta$ and x^γ is any monomial, then we require that $x^\alpha x^\gamma > x^\beta x^\gamma$. In terms of the exponent vectors, this property means that if $\alpha > \beta$ in our ordering on $\mathbb{Z}^n_{\geq 0}$, then, for all $\gamma \in \mathbb{Z}^n_{\geq 0}$, $\alpha + \gamma > \beta + \gamma$.

With these considerations in mind, we make the following definition.

Definition 1. *A* **monomial ordering** $>$ *on* $k[x_1, \ldots, x_n]$ *is any relation* $>$ *on* $\mathbb{Z}^n_{\geq 0}$*, or equivalently, any relation on the set of monomials* $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$*, satisfying:*

(i) $>$ *is a total (or linear) ordering on* $\mathbb{Z}^n_{\geq 0}$.
(ii) *If* $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$*, then* $\alpha + \gamma > \beta + \gamma$.
(iii) $>$ *is a well-ordering on* $\mathbb{Z}^n_{\geq 0}$*. This means that every nonempty subset of* $\mathbb{Z}^n_{\geq 0}$ *has a smallest element under* $>$.

The following lemma will help us understand what the well-ordering condition of part (iii) of the definition means.

Lemma 2. *An order relation* $>$ *on* $\mathbb{Z}^n_{\geq 0}$ *is a well-ordering if and only if every strictly decreasing sequence in* $\mathbb{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

eventually terminates.

Proof. We will prove this in contrapositive form: $>$ is not a well-ordering if and only if there is an infinite strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$.

If $>$ is not a well-ordering, then some nonempty subset $S \subset \mathbb{Z}^n_{\geq 0}$ has no least element. Now pick $\alpha(1) \in S$. Since $\alpha(1)$ is not the least element, we can find $\alpha(1) > \alpha(2)$ in S. Then $\alpha(2)$ is also not the least element, so that there is $\alpha(2) > \alpha(3)$ in S. Continuing this way, we get an infinite strictly decreasing sequence

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots .$$

Conversely, given such an infinite sequence, then $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ is a nonempty subset of $\mathbb{Z}^n_{\geq 0}$ with no least element, and thus, $>$ is not a well-ordering. □

The importance of this lemma will become evident in the sections to follow. It will be used to show that various algorithms must terminate because some term strictly decreases (with respect to a fixed monomial order) at each step of the algorithm.

In §4, we will see that given parts (i) and (ii) in Definition 1, the well-ordering condition of part (iii) is equivalent to $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$.

For a simple example of a monomial order, note that the usual numerical order

$$\cdots > m+1 > m > \cdots > 3 > 2 > 1 > 0$$

on the elements of $\mathbb{Z}_{\geq 0}$ satisfies the three conditions of Definition 1. Hence, the degree ordering (1) on the monomials in $k[x]$ is a monomial ordering.

Our first example of an ordering on n-tuples will be lexicographic order (or **lex** order, for short).

Definition 3 (Lexicographic Order). *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.*

Here are some examples:

a. $(1, 2, 0) >_{lex} (0, 3, 4)$ since $\alpha - \beta = (1, -1, -4)$.
b. $(3, 2, 4) >_{lex} (3, 2, 1)$ since $\alpha - \beta = (0, 0, 3)$.
c. The variables $x_1, \ldots, x_n$ are ordered in the usual way [see (2)] by the lex ordering:

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \cdots >_{lex} (0, \ldots, 0, 1).$$

so $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

In practice, when we work with polynomials in two or three variables, we will call the variables x, y, z rather than x_1, x_2, x_3. We will also assume that the alphabetical order $x > y > z$ on the variables is used to define the lexicographic ordering unless we explicitly say otherwise.

Lex order is analogous to the ordering of words used in dictionaries (hence the name). We can view the entries of an n-tuple $\alpha \in \mathbb{Z}^n_{\geq 0}$ as analogues of the letters in a word. The letters are ordered alphabetically:

$$\mathrm{a} > \mathrm{b} > \cdots > \mathrm{y} > \mathrm{z}.$$

Then, for instance,

$$\text{arrow} >_{lex} \text{arson}$$

since the third letter of "arson" comes after the third letter of "arrow" in alphabetical order, whereas the first two letters are the same in both. Since all elements $\alpha \in \mathbb{Z}^n_{\geq 0}$ have length n, this analogy only applies to words with a fixed number of letters.

For completeness, we must check that the lexicographic order satisfies the three conditions of Definition 1.

Proposition 4. *The lex ordering on $\mathbb{Z}^n_{\geq 0}$ is a monomial ordering.*

Proof. (i) That $>_{lex}$ is a total ordering follows directly from the definition and the fact that the usual numerical order on $\mathbb{Z}_{\geq 0}$ is a total ordering.

(ii) If $\alpha >_{lex} \beta$, then we have that the leftmost nonzero entry in $\alpha - \beta$, say $\alpha_k - \beta_k$, is positive. But $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ and $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Then in $(\alpha+\gamma)-(\beta+\gamma) = \alpha-\beta$, the leftmost nonzero entry is again $\alpha_k - \beta_k > 0$.

(iii) Suppose that $>_{lex}$ were not a well-ordering. Then by Lemma 2, there would be an infinite strictly descending sequence

$$\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \cdots$$

of elements of $\mathbb{Z}^n_{\geq 0}$. We will show that this leads to a contradiction.

Consider the first entries of the vectors $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. By the definition of the lex order, these first entries form a nonincreasing sequence of nonnegative integers. Since $\mathbb{Z}_{\geq 0}$ is well-ordered, the first entries of the $\alpha(i)$ must "stabilize" eventually. That is, there exists a k such that all the first components of the $\alpha(i)$ with $i \geq k$ are equal.

Beginning at $\alpha(k)$, the second and subsequent entries come into play in determining the lex order. The second entries of $\alpha(k), \alpha(k+1), \ldots$ form a nonincreasing sequence. By the same reasoning as before, the second entries "stabilize" eventually as well. Continuing in the same way, we see that for some l, the $\alpha(l), \alpha(l+1), \ldots$ all are equal. This contradicts the fact that $\alpha(l) >_{lex} \alpha(l+1)$. □

It is important to realize that there are many lex orders, corresponding to how the variables are ordered. So far, we have used lex order with $x_1 > x_2 > \ldots > x_n$. But given *any* ordering of the variables $x_1, \ldots, x_n$, there is a corresponding lex order. For example, if the variables are x and y, then we get one lex order with $x > y$ and a second with $y > x$. In the general case of n variables, there are $n!$ lex orders. In what follows, the phrase "lex order" will refer to the one with $x_1 > \cdots > x_n$ unless otherwise stated.

In lex order, notice that a variable dominates *any* monomial involving only smaller variables, regardless of its total degree. Thus, for the lex order with $x > y > z$, we have $x >_{lex} y^5 z^3$. For some purposes, we may also want to take the total degrees of the monomials into account and order monomials of bigger degree first. One way to do this is the graded lexicographic order (or **grlex** order).

Definition 5 (Graded Lex Order). *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \quad \text{or} \quad |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

We see that grlex orders by total degree first, then "breaks ties" using lex order. Here are some examples:

1. $(1, 2, 3) >_{grlex} (3, 2, 0)$ since $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$.
2. $(1, 2, 4) >_{grlex} (1, 1, 5)$ since $|(1, 2, 4)| = |(1, 1, 5)|$ and $(1, 2, 4) >_{lex} (1, 1, 5)$.
3. The variables are ordered according to the lex order, i.e., $x_1 >_{grlex} \cdots >_{grlex} x_n$. We will leave it as an exercise to show that the grlex ordering satisfies the three conditions of Definition 1. As in the case of lex order, there are $n!$ grlex orders on n variables, depending on how the variables are ordered.

Another (somewhat less intuitive) order on monomials is the graded reverse lexicographical order (or grevlex order). Even though this ordering "takes some getting used to," it has recently been shown that for some operations, the grevlex ordering is the most efficient for computations.

Definition 6 (Graded Reverse Lex Order). *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \quad \text{or} \quad |\alpha| = |\beta| \text{ and the rightmost nonzero entry of } \alpha - \beta \in \mathbb{Z}^n \text{ is negative.}$$

Like grlex, grevlex orders by total degree, but it "breaks ties" in a different way. For example:

1. $(4, 7, 1) >_{grevlex} (4, 2, 3)$ since $|(4, 7, 1)| = 12 > |(4, 2, 3)| = 9$.
2. $(1, 5, 2) >_{grevlex} (4, 1, 3)$ since $|(1, 5, 2)| = |(4, 1, 3)|$ and $(1, 5, 2) - (4, 1, 3) = (-3, 4, -1)$.

You will show in the exercises that the grevlex ordering gives a monomial ordering.

Note also that lex and grevlex give the same ordering on the variables. That is,

$$(1, 0, \ldots, 0) >_{grevlex} (0, 1, \ldots, 0) >_{grevlex} \cdots >_{grevlex} (0, \ldots, 0, 1)$$

or

$$x_1 >_{grevlex} x_2 >_{grevlex} \cdots >_{grevlex} x_n.$$

Thus, grevlex is really different from the grlex order with the variables rearranged (as one might be tempted to believe from the name).

To explain the relation between grlex and grevlex, note that both use total degree in the same way. To break a tie, grlex uses lex order, so that it looks at the leftmost (or largest) variable and favors the *larger* power. In contrast, when grevlex finds the same total degree, it looks at the rightmost (or smallest) variable and favors the *smaller* power. In the exercises, you will check that this amounts to a "double-reversal" of lex order. For example,

$$x^5yz >_{grlex} x^4yz^2,$$

since both monomials have total degree 7 and $x^5yz >_{lex} x^4yz^2$. In this case, we also have

$$x^5yz >_{grevlex} x^4yz^2,$$

but for a different reason: x^5yz is larger because the smaller variable z appears to a smaller power.

As with lex and grlex, there are $n!$ grevlex orderings corresponding to how the n variables are ordered.

There are many other monomial orders besides the ones considered here. Some of these will be explored in the exercises to §4. Most computer algebra systems implement lex order, and most also allow other orders, such as grlex and grevlex. Once such an order is chosen, these systems allow the user to specify any of the $n!$ orderings of the variables. As we will see in §8 of this chapter and in later chapters, this facility becomes very useful when studying a variety of questions.

We will end this section with a discussion of how a monomial ordering can be applied to polynomials. If $f = \sum_\alpha a_\alpha x^\alpha$ is a polynomial in $k[x_1, \ldots, x_n]$ and we have selected a monomial ordering $>$, then we can order the monomials of f in an unambiguous way with respect to $>$. For example, let $f = 4xy^2z+4z^2-5x^3+7x^2z^2 \in k[x, y, z]$. Then:

a. With respect to the lex order, we would reorder the terms of f in decreasing order as

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$

b. With respect to the grlex order, we would have

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2.$$

c. With respect to the grevlex order, we would have

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

We will use the following terminology.

Definition 7. *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.*

(i) *The* **multidegree** *of f is*

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$$

(the maximum is taken with respect to $>$).

(ii) *The* **leading coefficient** *of f is*

$$\text{LC}(f) = a_{\text{multideg}(f)} \in k.$$

(iii) *The* **leading monomial** *of f is*

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

(with coefficient 1).

(iv) *The* **leading term** *of f is*

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

To illustrate, let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ as before and let $>$ denote the lex order. Then

$$\begin{aligned} \text{multideg}(f) &= (3, 0, 0), \\ \mathrm{LC}(f) &= -5, \\ \mathrm{LM}(f) &= x^3, \\ \mathrm{LT}(f) &= -5x^3. \end{aligned}$$

In the exercises, you will show that the multidegree has the following useful properties.

Lemma 8. *Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials. Then:*

(i) *multideg(fg) = multideg(f) + multideg(g).*

(ii) *If $f + g \neq 0$, then multideg$(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. If, in addition,* multideg$(f) \neq$ multideg(g)*, then equality occurs.*

From now on, we will assume that one particular monomial order has been selected, and that leading terms, etc., will be computed relative to that order only.

EXERCISES FOR §2

1. Rewrite each of the following polynomials, ordering the terms using the lex order, the grlex order, and the grevlex order, giving LM(f), LT(f), and multideg(f) in each case.
   a. $f(x, y, z) = 2x + 3y + z + x^2 - z^2 + x^3$.
   b. $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$.
2. Each of the following polynomials is written with its monomials ordered according to (exactly) one of lex, grlex, or grevlex order. Determine which monomial order was used in each case.
   a. $f(x, y, z) = 7x^2y^4z - 2xy^6 + x^2y^2$.
   b. $f(x, y, z) = xy^3z + xy^2z^2 + x^2z^3$.
   c. $f(x, y, z) = x^4y^5z + 2x^3y^2z - 4xy^2z^4$.
3. Repeat Exercise 1 when the variables are ordered $z > y > x$.
4. Show that grlex is a monomial order according to Definition 1.
5. Show that grevlex is a monomial order according to Definition 1.
6. Another monomial order is the **inverse lexicographic** or **invlex** order defined by the following: for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{invlex} \beta$ if and only if, in $\alpha - \beta$, the rightmost nonzero entry is positive. Show that invlex is equivalent to the lex order with the variables permuted in a certain way. (Which permutation?)
7. Let $>$ be any monomial order.
   a. Show that $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$.
   b. Show that if x^α divides x^β, then $\alpha \leq \beta$. Is the converse true?
   c. Show that if $\alpha \in \mathbb{Z}^n_{\geq 0}$, then α is the smallest element of $\alpha + \mathbb{Z}^n_{\geq 0}$.
8. Write a precise definition of what it means for a system of linear equations to be in echelon form, using the ordering given in equation (2).

9. In this exercise, we will study grevlex in more detail. Let $>_{invlex}$, be the order given in Exercise 6, and define $>_{rinvlex}$ to be the reversal of this ordering, i.e., for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$.

$$\alpha >_{rinvlex} \beta \Longleftrightarrow \beta >_{invlex} \alpha.$$

Notice that rinvlex is a "double reversal" of lex, in the sense that we first reverse the order of the variables and then we reverse the ordering itself.

   a. Show that $\alpha >_{grevlex} \beta$ if and only if $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and $\alpha >_{rinvlex} \beta$.
   b. Is rinvlex a monomial ordering according to Definition 1? If so, prove it; if not, say which properties fail.

10. In $\mathbb{Z}_{\geq 0}$ with the usual ordering, between any two integers, there are only a finite number of other integers. Is this necessarily true in $\mathbb{Z}^n_{\geq 0}$ for a monomial order? Is it true for the grlex order?
11. Let $>$ be a monomial order on $k[x_1, \ldots, x_n]$.
   a. Let $f \in k[x_1, \ldots, x_n]$ and let m be a monomial. Show that $\mathrm{LT}(m \cdot f) = m \cdot \mathrm{LT}(f)$.
   b. Let $f, g \in k[x_1, \ldots, x_n]$. Is $\mathrm{LT}(f \cdot g)$ necessarily the same as $\mathrm{LT}(f) \cdot \mathrm{LT}(g)$?
   c. If $f_i, g_i \in k[x_1, \ldots, x_n]$, $1 \leq i \leq s$, is $\mathrm{LM}(\sum_{i=1}^s f_i g_i)$ necessarily equal to $\mathrm{LM}(f_i) \cdot \mathrm{LM}(g_i)$ for some i?
12. Lemma 8 gives two properties of the multidegree.
   a. Prove Lemma 8. Hint: The arguments used in Exercise 11 may be relevant.
   b. Suppose that $\mathrm{multideg}(f) = \mathrm{multideg}(g)$ and $f + g \neq 0$. Give examples to show that $\mathrm{multideg}(f + g)$ may or may not equal $\max(\mathrm{multideg}(f), \mathrm{multideg}(g))$.

§3 A Division Algorithm in $k[x_1, \ldots, x_n]$

In §1, we saw how the division algorithm could be used to solve the ideal membership problem for polynomials of one variable. To study this problem when there are more variables, we will formulate a division algorithm for polynomials in $k[x_1, \ldots, x_n]$ that extends the algorithm for $k[x]$. In the general case, the goal is to divide $f \in k[x_1, \ldots, x_n]$ by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. As we will see, this means expressing f in the form

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where the "quotients" $a_1, \ldots, a_s$ and remainder r lie in $k[x_1, \ldots, x_n]$. Some care will be needed in deciding how to characterize the remainder. This is where we will use the monomial orderings introduced in §2. We will then see how the division algorithm applies to the ideal membership problem.

The basic idea of the algorithm is the same as in the one-variable case: we want to cancel the leading term of f (with respect to a fixed monomial order) by multiplying some f_i by an appropriate monomial and subtracting. Then this monomial becomes a term in the corresponding a_i. Rather than state the algorithm in general, let us first work through some examples to see what is involved.

Example 1. We will first divide $f = xy^2 + 1$ by $f_1 = xy + 1$ and $f_2 = y + 1$, using lex order with $x > y$. We want to employ the same scheme as for division of one-variable polynomials, the difference being that there are now several divisors and quotients. Listing the divisors f_1, f_2 and the quotients a_1, a_2 *vertically*, we have the

following setup:

$$\begin{array}{rl} a_1: & \\ a_2: & \\ xy+1 & \overline{)\,xy^2+1} \\ y+1 & \end{array}$$

The leading terms $\mathrm{LT}(f_1) = xy$ and $\mathrm{LT}(f_2) = y$ both divide the leading term $\mathrm{LT}(f) = xy^2$. Since f_1 is listed first, we will use it. Thus, we divide xy into xy^2, leaving y, and then subtract $y \cdot f_1$ from f:

$$\begin{array}{rll} a_1: & y & \\ a_2: & & \\ xy+1 & \overline{)\,xy^2+1} & \\ y+1 & \underline{xy^2+y} & \\ & -y+1 & \end{array}$$

Now we repeat the same process on $-y+1$. This time we must use f_2 since $\mathrm{LT}(f_1) = xy$ does not divide $\mathrm{LT}(-y+1) = -y$. We obtain

$$\begin{array}{rll} a_1: & y & \\ a_2: & -1 & \\ xy+1 & \overline{)\,xy^2+1} & \\ y+1 & \underline{xy^2+y} & \\ & -y+1 & \\ & \underline{-y-1} & \\ & 2 & \end{array}$$

Since $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$ do not divide 2, the remainder is $r = 2$ and we are, done. Thus, we have written $f = xy^2 + 1$ in the form

$$xy^2 + 1 = y \cdot (xy+1) + (-1) \cdot (y+1) + 2.$$

Example 2. In this example, we will encounter an unexpected subtlety that can occur when dealing with polynomials of more than one variable. Let us divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$. As in the previous example, we will use lex order with $x > y$. The first two steps of the algorithm go as usual, giving us the following partially completed division (remember that when both leading terms divide, we use f_1):

$$\begin{array}{rll} a_1: & x+y & \\ a_2: & & \\ xy-1 & \overline{)\,x^2y+xy^2+y^2} & \\ y^2-1 & \underline{x^2y-x} & \\ & xy^2+x+y^2 & \\ & \underline{xy^2-y} & \\ & x+y^2+y & \end{array}$$

Note that neither $\mathrm{LT}(f_1) = xy$ nor $\mathrm{LT}(f_2) = y^2$ divides $\mathrm{LT}(x + y^2 + y) = x$. However, $x + y^2 + y$ is *not* the remainder since $\mathrm{LT}(f_2)$ divides y^2. Thus, if we move x to the remainder, we can continue dividing. (This is something that never happens in the one-variable case: once the leading term of the divisor no longer divides the leading term of what is left under the radical, the algorithm terminates.)

To implement this idea, we create a remainder column r, to the right of the radical, where we put the terms belonging to the remainder. Also, we call the polynomial under the radical the *intermediate dividend*. Then we continue dividing until the intermediate dividend is zero. Here is the next step, where we move x to the remainder column (as indicated by the arrow):

$$
\begin{array}{rl}
a_1: & x+y \\
a_2: & \\
xy-1 & \overline{\left.\begin{array}{l} x^2y+xy^2+y^2 \\ x^2y-x \end{array}\right.} \\
y^2-1 &
\end{array}
\qquad
\begin{array}{r} r \\ \hline \\ \\ \\ \\ \\ x \end{array}
$$

$$
\begin{array}{r}
\overline{} \\
xy^2+x+y^2 \\
xy^2-y \\
\overline{} \\
x+y^2+y \\
\overline{} \\
y^2+y
\end{array}
\quad \longrightarrow
$$

Now we continue dividing. If we can divide by $\mathrm{LT}(f_1)$ or $\mathrm{LT}(f_2)$, we proceed as usual, and if neither divides, we move the leading term of the intermediate dividend to the remainder column. Here is the rest of the division:

$$
\begin{array}{rl}
a_1: & x+y \\
a_2: & 1 \\
xy-1 & \overline{\left.\begin{array}{l} x^2y+xy^2+y^2 \\ x^2y-x \end{array}\right.} \\
y^2-1 &
\end{array}
\qquad
\begin{array}{r} r \\ \hline \\ \\ \\ \\ \\ \\ \\ \\ x \\ \\ x+y \\ x+y+1 \end{array}
$$

$$
\begin{array}{r}
\overline{} \\
xy^2+x+y^2 \\
xy^2-y \\
\overline{} \\
x+y^2+y \\
\overline{} \\
y^2+y \\
y^2-1 \\
\overline{} \\
y+1 \\
\overline{} \\
1 \\
\overline{0}
\end{array}
\quad \longrightarrow \quad \longrightarrow \quad \longrightarrow
$$

Thus, the remainder is $x + y + 1$, and we obtain

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1. \tag{1}$$

Note that the remainder is a sum of monomials, none of which is divisible by the leading terms $\mathrm{LT}(f_1)$ or $\mathrm{LT}(f_2)$.

The above example is a fairly complete illustration of how the division algorithm works. It also shows us what property we want the remainder to have: none of its terms should be divisible by the leading terms of the polynomials by which we are dividing. We can now state the general form of the division algorithm.

Theorem 3 (Division Algorithm in $k[x_1, \ldots, x_n]$). *Fix a monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$, and let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then every $f \in k[x_1, \ldots, x_n]$ can be written as*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where $a_i, r \in k[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. We will call r a **remainder** *of f on division by F. Furthermore, if $a_i\ f_i \neq 0$, then we have*

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i f_i).$$

Proof. We prove the existence of $a_1, \ldots, a_s$ and r by giving an algorithm for their construction and showing that it operates correctly on any given input. We recommend that the reader review the division algorithm in $k[x]$ given in Proposition 2 of Chapter 1, §5 before studying the following generalization:

Input: $f_1, \ldots, f_s, f$
Output: $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots;\ a_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
    $i := 1$
    divisionoccurred := false
    WHILE $i \leq s$ AND divisionoccurred = false DO
        IF $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ THEN
            $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
            $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))\, f_i$
            divisionoccurred:= true
        ELSE
            $i := i + 1$
    IF divisionoccurred = false THEN
        $r := r + \mathrm{LT}(p)$
        $p := p - \mathrm{LT}(p)$

We can relate this algorithm to the previous example by noting that the variable p represents the intermediate dividend at each stage, the variable r represents the column on the right-hand side, and the variables $a_1, \ldots, a_s$ are the quotients listed above the radical. Finally, the boolean variable "divisionoccurred" tells us when some $\mathrm{LT}(f_i)$ divides the leading term of the intermediate dividend. You should check that each time we go through the main WHILE ... DO loop, precisely one of two things happens:

- (Division Step) If some $\text{LT}(f_i)$ divides $\text{LT}(p)$, then the algorithm proceeds as in the one-variable case.
- (Remainder Step) If no $\text{LT}(f_i)$ divides $\text{LT}(p)$, then the algorithm adds $\text{LT}(p)$ to the remainder.

These steps correspond exactly to what we did in Example 2.

To prove that the algorithm works, we will first show that

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{2}$$

holds at every stage. This is clearly true for the initial values of $a_1, \ldots, a_s$, p, and r. Now suppose that (2) holds at one step of the algorithm. If the next step is a Division Step, then some $\text{LT}(f_i)$ divides $\text{LT}(p)$, and the equality

$$a_i f_i + p = (a_i + \text{LT}(p)/\text{LT}(f_i)) f_i + (p - (\text{LT}(p)/\text{LT}(f_i)) f_i)$$

shows that $a_i f_i + p$ is unchanged. Since all other variables are unaffected, (2) remains true in this case. On the other hand, if the next step is a Remainder Step, then p and r will be changed, but the sum $p + r$ is unchanged since

$$p + r = (p - \text{LT}(p)) + (r + \text{LT}(p)).$$

As before, equality (2) is still preserved.

Next, notice that the algorithm comes to a halt when $p = 0$. In this situation, (2) becomes

$$f = a_1 f_1 + \cdots + a_s f_s + r.$$

Since terms are added to r only when they are divisible by none of the $\text{LT}(f_i)$, it follows that $a_1, \ldots, a_s$ and r have the desired properties when the algorithm terminates.

Finally, we need to show that the algorithm does eventually terminate. The key observation is that each time we redefine the variable p, either its multidegree drops (relative to our term ordering) or it becomes 0. To see this, first suppose that during a Division Step, p is redefined to be

$$p' = p - \frac{\text{LT}(p)}{\text{LT}(f_i)} f_i.$$

By Lemma 8 of §2, we have

$$\text{LT}\left(\frac{\text{LT}(p)}{\text{LT}(f_i)} f_i\right) = \frac{\text{LT}(p)}{\text{LT}(f_i)} \text{LT}(f_i) = \text{LT}(p),$$

so that p and $(\text{LT}(p)/\text{LT}(f_i)) f_i$ have the same leading term. Hence, their difference p' must have strictly smaller multidegree when $p' \neq 0$. Next, suppose that during a Remainder Step, p is redefined to be

$$p' = p - \text{LT}(p).$$

Here, it is obvious that $\text{multideg}(p') < \text{multideg}(p)$ when $p' \neq 0$. Thus, in either case, the multidegree must decrease. If the algorithm never terminated, then we would get an infinite decreasing sequence of multidegrees. The well-ordering property of $>$, as stated

in Lemma 2 of §2, shows that this cannot occur. Thus $p = 0$ must happen eventually, so that the algorithm terminates after finitely many steps.

It remains to study the relation between multideg(f) and multideg$(a_i f_i)$. Every term in a_i is of the form $\text{LT}(p)/\text{LT}(f_i)$ for some value of the variable p. The algorithm starts with $p = f$, and we just finished proving that the multidegree of p decreases. This shows that $\text{LT}(p) < \text{LT}(f)$, and then it follows easily [using condition (ii) of the definition of a monomial order] that multideg$(a_i f_i) <$ multideg(f) when $a_i f_i \neq 0$ (see Exercise 4). This completes the proof of the theorem. □

The algebra behind the division algorithm is very simple (there is nothing beyond high school algebra in what we did), which makes it surprising that this form of the algorithm was first isolated and exploited only within the past 30 years.

We will conclude this section by asking whether the division algorithm has the same nice properties as the one-variable version. Unfortunately, the answer is not pretty—the examples given below will show that the division algorithm is far from perfect. In fact, the algorithm achieves its full potential only when coupled with the Groebner bases studied in §§5 and 6.

A first important property of the division algorithm in $k[x]$ is that the remainder is uniquely determined. To see how this can fail when there is more than one variable, consider the following example.

Example 4. Let us divide $f = x^2y + xy^2 + y^2$ by $f_1 = y^2 - 1$ and $f_2 = xy - 1$. We will use lex order with $x > y$. This is the same as Example 2, except that we have changed the order of the divisors. For practice, we suggest that the reader should do the division. You should get the following answer:

$$
\begin{array}{rl}
a_1: & x+1 \\
a_2: & x \\
y^2-1 & \big| \; x^2y + xy^2 + y^2 \\
xy-1 & \big| \; x^2y - x \\
\hline
 & \quad xy^2 + x + y^2 \\
 & \quad xy^2 - x \\
\hline
 & \qquad 2x + y^2 \\
\hline
 & \qquad\quad y^2 \\
 & \qquad\quad y^2 - 1 \\
\hline
 & \qquad\quad\;\; 1 \\
 & \qquad\quad\;\; \overline{0}
\end{array}
\qquad
\begin{array}{l}
r \\
\hline
\\
\\
\\
\\
\\
\\
\longrightarrow \quad 2x \\
\\
\longrightarrow \quad 2x+1 \\
\longrightarrow \quad 2x+1
\end{array}
$$

This shows that

$$x^2y + xy^2 + y^2 = (x+1)\cdot(y^2-1) + x\cdot(xy-1) + 2x + 1. \tag{3}$$

If you compare this with equation (1), you will see that the remainder is different from what we got in Example 2.

This shows that the remainder r is not uniquely characterized by the requirement that none of its terms be divisible by $\mathrm{LT}(f_i), \ldots, \mathrm{LT}(f_s)$. The situation is not completely chaotic: if we follow the algorithm precisely as stated [most importantly, testing $\mathrm{LT}(p)$ for divisibility by $\mathrm{LT}(f_1)$, $\mathrm{LT}(f_2)$, ... in that order], then $a_1, \ldots, a_s$ and r are uniquely determined. (See Exercise 11 for a more detailed discussion of how to characterize the output of the algorithm.) However, Examples 2 and 4 show that the *ordering* of the s-tuple of polynomials $(f_1, \ldots, f_s)$ definitely matters, both in the number of steps the algorithm will take to complete the calculation and in the results. The a_i and r can change if we simply rearrange the f_i. (The a_i and r may also change if we change the monomial ordering, but that is another story.)

One nice feature of the division algorithm in $k[x]$ is the way it solves the ideal membership problem—recall Example 1 from §1. Do we get something similar for several variables? One implication is an easy corollary of Theorem 3: if after division of f by $F = (f_1, \ldots, f_s)$ we obtain a remainder $r = 0$, then

$$f = a_1 f_1 + \cdots + a_s f_s,$$

so that $f \in \langle f_1, \ldots, f_s \rangle$. Thus $r = 0$ is a *sufficient* condition for ideal membership. However, as the following example shows, $r = 0$ is not a *necessary* condition for being in the ideal.

Example 5. Let $f_1 = xy + 1$, $f_2 = y^2 - 1 \in k[x, y]$ with the lex order. Dividing $f = xy^2 - x$ by $F = (f_1, f_2)$, the result is

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

With $F = (f_2, f_1)$, however, we have

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

The second calculation shows that $f \in \langle f_1, f_2 \rangle$. Then the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$, it is still possible to obtain a nonzero remainder on division by $F = (f_1, f_2)$.

Thus, we must conclude that the division algorithm given in Theorem 3 is an imperfect generalization of its one-variable counterpart. To remedy this situation, we turn to one of the lessons learned in Chapter 1. Namely, in dealing with a collection of polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, it is frequently desirable to pass to the ideal I they generate. This allows the possibility of going from $f_1, \ldots, f_s$ to a different generating set for I. So we can still ask whether there might be a "good" generating set for I. For such a set, we would want the remainder r on division by the "good" generators to be uniquely determined and the condition $r = 0$ should be *equivalent* to membership in the ideal. In §6, we will see that Groebner bases have exactly these "good" properties.

In the exercises, you will experiment with a computer algebra system to try to discover for yourself what properties a "good" generating set should have. We will give a precise definition of "good" in §5 of this chapter.

EXERCISES FOR §3

1. Compute the remainder on division of the given polynomial f by the order set F (by hand). Use the grlex order, then the lex order in each case.
   a. $f = x^7y^2 + x^3y^2 - y + 1 \quad F = (xy^2 - x, x - y^3)$.
   b. Repeat part a with the order of the pair F reversed.
2. Compute the remainder on division:
   a. $f = xy^2z^2 + xy - yz \quad F = (x - y^2, y - z^3, z^2 - 1)$.
   b. Repeat part a with the order of the set F permuted cyclically.
3. Using a computer algebra system, check your work from Exercises 1 and 2. (You may need to consult documentation to learn whether the system you are using has an explicit polynomial division command or you will need to perform the individual steps of the algorithm yourself.)
4. Let $f = a_1f_1 + \cdots + a_sf_s + r$ be the output of the division algorithm.
   a. Complete the proof begun in the text that multideg$(f) \geq$ multideg(a_if_i) when $a_if_i \neq 0$.
   b. Prove that multideg$(f) \geq$ multideg(r) when $r \neq 0$.

The following problems investigate in greater detail the way the remainder computed by the division algorithm depends on the ordering and the form of the s-tuple of divisors $F = (f_1, \ldots, f_s)$. You may wish to use a computer algebra system to perform these calculations.

5. We will study the division of $f = x^3 - x^2y - x^2z + x$ by $f_1 = x^2y - z$ and $f_2 = xy - 1$.
   a. Compute using grlex order:

$$r_1 = \text{remainder of } f \text{ on division by } (f_1, f_2).$$
$$r_2 = \text{remainder of } f \text{ on division by } (f_2, f_1).$$

   Your results should be *different*. Where in the division algorithm did the difference occur? (You may need to do a few steps by hand here.)
   b. Is $r = r_1 - r_2$ in the ideal $\langle f_1, f_2\rangle$? If so, find an explicit expression $r = Af_1 + Bf_2$. If not, say why not.
   c. Compute the remainder of r on division by (f_1, f_2). Why could you have predicted your answer before doing the division?
   d. Find another polynomial $g \in \langle f_1, f_2\rangle$ such that the remainder on division of g by (f_1, f_2) is nonzero. Hint: $(xy + 1) \cdot f_2 = x^2y^2 - 1$, whereas $y \cdot f_1 = x^2y^2 - yz$.
   e. Does the division algorithm give us a solution for the ideal membership problem for the ideal $\langle f_1, f_2\rangle$? Explain your answer.
6. Using the grlex order, find an element g of $\langle f_1, f_2\rangle = \langle 2xy^2 - x, 3x^2y - y - 1\rangle \subset \mathbb{R}[x, y]$ whose remainder on division by (f_1, f_2) is nonzero. Hint: You can find such a g where the remainder is g itself.
7. Answer the question of Exercise 6 for $\langle f, f_2, f_3\rangle = \langle x^4y^2 - z, x^4y^2 - z, x^3y^2 - z, x^3y^3 - 1, x^2y^4 - 2z\rangle \subset \mathbb{R}[x, y, z]$. Find two different polynomials g (not constant multiples of each other).
8. Try to formulate a general pattern that fits the examples in Exercises 5(c,d), 6, and 7. What condition on the leading term of the polynomial $g = A_1f_1 + \cdots + A_sf_s$ would guarantee that there was a nonzero remainder on division by $(f_1, \ldots, f_s)$? What does your condition imply about the ideal membership problem?
9. The discussion around equation (2) of Chapter 1, §4 shows that every polynomial $f \in \mathbb{R}[x, y, z]$ can be written as

$$f = h_1(y - x^2) + h_2(z - x^3) + r,$$

where r is a polynomial in x alone and $\mathbf{V}(y - x^2, z - x^3)$ is the twisted cubic curve in $\mathbb{R}^3$.

a. Give a proof of this fact using the division algorithm. Hint: You need to specify carefully the monomial ordering to be used.
b. Use the parametrization of the twisted cubic to show that $z^2 - x^4 y$ vanishes at every point of the twisted cubic.
c. Find an explicit representation

$$z^2 - x^4 y = h_1(y - x^2) + h_2(z - x^3)$$

using the division algorithm.

10. Let $V \subset \mathbb{R}^3$ be the curve parametrized by (t, t^m, t^n), $n, m \geq 2$.
    a. Show that V is an affine variety.
    b. Adapt the ideas in Exercise 9 to determine $\mathbf{I}(V)$.
11. In this exercise, we will characterize completely the expression

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

that is produced by the division algorithm (among all the possible expressions for f of this form). Let $\mathrm{LM}(f_i) = x^{\alpha(i)}$ and define

$$\begin{aligned}
\Delta_1 &= \alpha(1) + \mathbb{Z}^n_{\geq 0},\\
\Delta_2 &= (\alpha(2) + \mathbb{Z}^n_{\geq 0}) - \Delta_1,\\
&\vdots\\
\Delta_s &= (\alpha(s) + \mathbb{Z}^n_{\geq 0}) - \left(\bigcup_{i=1}^{s-1} \Delta_i\right)\\
\overline{\Delta} &= \mathbb{Z}^n_{\geq 0} - \left(\bigcup_{i=1}^{s} \Delta_i\right).
\end{aligned}$$

(Note that $\mathbb{Z}^n_{\geq 0}$ is the disjoint union of the Δ_i and $\overline{\Delta}$.)

a. Show that $\beta \in \Delta_i$, if and only if $x^{\alpha(i)}$ divides x^β, but no $x^{\alpha(j)}$ with $j < i$ divides x^β.
b. Show that $\gamma \in \overline{\Delta}$ if and only if no $x^{\alpha(i)}$ divides x^γ.
c. Show that in the expression $f = a_1 f_1 + \cdots + a_s f_s + r$ computed by the division algorithm, for every i, every monomial x^β in a_i satisfies $\beta + \alpha(i) \in \Delta_i$, and every monomial x^γ in r satisfies $\gamma \in \overline{\Delta}$.
d. Show that there is exactly one expression $f = a_1 f_1 + \cdots + a_s f_s + r$ satisfying the properties given in part c.

12. Show that the operation of computing remainders on division by $F = (f_1 \ldots f_s)$ is linear over k. That is, if the remainder on division of g_i by F is r_i, $i = 1, 2$, then, for any $c_1, c_2 \in k$, the remainder on division of $c_1 g_1 + c_2 g_2$ is $c_1 r_1 + c_2 r_2$. Hint: Use Exercise 11.

§4 Monomial Ideals and Dickson's Lemma

In this section, we will consider the ideal description problem of §1 for the special case of monomial ideals. This will require a careful study of the properties of these ideals. Our results will also have an unexpected application to monomial orderings.

To start, we define monomial ideals in $k[x_1, \ldots, x_n]$.

Definition 1. *An ideal $I \subset k[x_1, \ldots, x_n]$ is a* **monomial ideal** *if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, \ldots, x_n]$. In this case, we write $I = \langle x^\alpha : \alpha \in A \rangle$.*

An example of a monomial ideal is given by $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle \subset k[x, y]$. More interesting examples of monomial ideals will be given in §5.

We first need to characterize all monomials that lie in a given monomial ideal.

Lemma 2. *Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof. If x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$ by the definition of ideal. Conversely, if $x^\beta \in I$, then $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, where $h_i \in k[x_1, \ldots, x_n]$ and $\alpha(i) \in A$. If we expand each h_i as a linear combination of monomials, we see that every term on the right side of the equation is divisible by some $x^{\alpha(i)}$. Hence, the left side x^β must have the same property. □

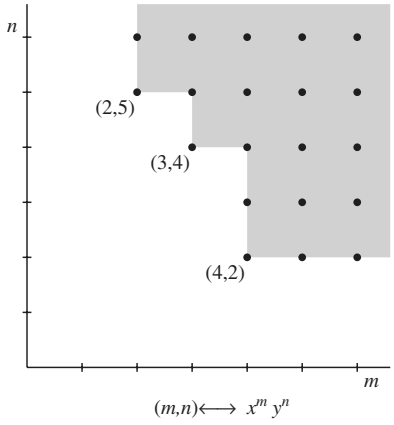
Note that x^β is divisible by x^α exactly when $x^\beta = x^\alpha \cdot x^\gamma$ for some $\gamma \in \mathbb{Z}^n_{\geq 0}$. This is equivalent to $\beta = \alpha + \gamma$. Thus, the set

$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma : \gamma \in \mathbb{Z}^n_{\geq 0}\}$$

consists of the exponents of all monomials divisible by x^α. This observation and Lemma 2 allows us to draw pictures of the monomials in a given monomial ideal. For example, if $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$, then the exponents of the monomials in I form the set

$$((4, 2) + \mathbb{Z}^2_{\geq 0}) \cup ((3, 4) + \mathbb{Z}^2_{\geq 0}) \cup ((2, 5) + \mathbb{Z}^2_{\geq 0}).$$

We can visualize this set as the union of the integer points in three translated copies of the first quadrant in the plane:



Let us next show that whether a given polynomial f lies in a monomial ideal can be determined by looking at the monomials of f.

Lemma 3. *Let I be a monomial ideal, and let $f \in k[x_1, \ldots, x_n]$. Then the following are equivalent:*

(i) $f \in I$.
(ii) *Every term of f lies in I.*
(iii) *f is a k-linear combination of the monomials in I.*

Proof. The implications (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) are trivial. The proof of (i) $\Rightarrow$ (iii) is similar to what we did in Lemma 2 and is left as an exercise. □

An immediate consequence of part (iii) of the lemma is that a monomial ideal is uniquely determined by its monomials. Hence, we have the following corollary.

Corollary 4. *Two monomial ideals are the same if and only if they contain the same monomials.*

The main result of this section is that all monomial ideals of $k[x_1, \ldots, x_n]$, are finitely generated.

Theorem 5 (Dickson's Lemma). *Let $I = \langle x^\alpha : \alpha \in A\rangle \subseteq k[x_1, \ldots, x_n]$ be a monomial ideal. Then I can be written in the form $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$, where $\alpha(1), \ldots, \alpha(s) \in A$. In particular, I has a finite basis.*

Proof. (By induction on n, the number of variables.) If $n = 1$, then I is generated by the monomials x_1^α, where $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Let β be the smallest element of $A \subset \mathbb{Z}_{\geq 0}$. Then $\beta \leq \alpha$ for all $\alpha \in A$, so that x_1^β, divides all other generators x_1^α. From here, $I = \langle x_1^\beta\rangle$ follows easily.

Now assume that $n > 1$ and that the theorem is true for $n - 1$. We will write the variables as $x_1, \ldots, x_{n-1}, y$, so that monomials in $k[x_1, \ldots, x_{n-1}, y]$ can be written as $x^\alpha y^m$, where $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ and $m \in \mathbb{Z}_{\geq 0}$.

Suppose that $I \subset k[x_1, \ldots, x_{n-1}, y]$ is a monomial ideal. To find generators for I, let J be the ideal in $k[x_1, \ldots, x_{n-1}]$ generated by the monomials x^α for which $x^\alpha y^m \in I$ for some $m \geq 0$. Since J is a monomial ideal in $k[x_1, \ldots, x_{n-1}]$, our inductive hypothesis implies that finitely many of the x^α's generate J, say $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$. The ideal J can be understood as the "projection" of I into $k[x_1, \ldots, x_{n-1}]$.

For each i between 1 and s, the definition of J tells us that $x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$. Let m be the largest of the m_i. Then, for each k between 0 and $m - 1$, consider the ideal $J_k \subset k[x_1, \ldots, x_{n-1}]$ generated by the monomials x^β such that $x^\beta y^k \in I$. One can think of J_k as the "slice" of I generated by monomials containing y exactly to the kth power. Using our inductive hypothesis again, J_k has a finite generating set of monomials, say $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)}\rangle$.

We claim that I is generated by the monomials in the following list:

$$\begin{aligned}
\text{from } J &: x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m,\\
\text{from } J_0 &: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)},\\
\text{from } J_1 &: x^{\alpha_1(1)}y, \ldots, x^{\alpha_1(s_1)}y,\\
&\vdots\\
\text{from } J_{m-1} &: x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1},
\end{aligned}$$

First note that every monomial in I is divisible by one on the list. To see why, let $x^\alpha y^p \in I$. If $p \geq m$, then $x^\alpha y^p$ is divisible by some $x^{\alpha(i)}y^m$ by the construction of J. On the other hand, if $p \leq m-1$, then $x^\alpha y^p$ is divisible by some $x^{\alpha_p(j)}y^p$ by the construction of J_p. It follows from Lemma 2 that the above monomials generate an ideal having the same monomials as I. By Corollary 4, this forces the ideals to be the same, and our claim is proved.

To complete the proof of the theorem, we need to show that the finite set of generators can be chosen from a given set of generators for the ideal. If we switch back to writing the variables as $x_1, \ldots, x_n$, then our monomial ideal is $I = \langle x^\alpha : \alpha \in A\rangle \subset k[x_1, \ldots, x_n]$. We need to show that I is generated by finitely many of the x^α's, where $\alpha \in A$. By the previous paragraph, we know that $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)}\rangle$ for some monomials $x^{\beta(i)}$ in I. Since $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A\rangle$, Lemma 2 tells us that each $x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ for some $\alpha(i) \in A$. From here, it is easy to show that $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$ (see Exercise 6 for the details). This completes the proof. □

To better understand how the proof of Theorem 5 works, let us apply it to the ideal $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle$ discussed earlier in the section. From the picture of the exponents, you can see that the "projection" is $J = \langle x^2\rangle \subset k[x]$. Since $x^2y^5 \in I$, we have $m = 5$. Then we get the "slices" $J_k, 0 \leq k \leq 4 = m-1$, generated by monomials containing y^k:

$$\begin{aligned}
J_0 = J_1 &= \{0\},\\
J_2 = J_3 &= \langle x^4\rangle,\\
J_4 &= \langle x^3\rangle.
\end{aligned}$$

These "slices" are easy to see using the picture of the exponents. Then the proof of Theorem 5 gives $I = \langle x^2y^5, x^4y^2, x^4y^3, x^3y^4\rangle$.

Theorem 5 solves the ideal description problem for monomial ideals, for it tells that such an ideal has a finite basis. This, in turn, allows us to solve the ideal membership problem for monomial ideals. Namely, if $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$, then one can easily show that a given polynomial f is in I if and only if the remainder of f on division by $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ is zero. See Exercise 9 for the details.

We can also use Dickson's Lemma to prove the following important fact about monomial orderings in $k[x_1, \ldots, x_n]$.

Corollary 6. *Let $>$ be a relation on $\mathbb{Z}^n_{\geq 0}$ satisfying:*
(i) *$>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$.*
(ii) *if $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.*
Then $>$ is well-ordering if and only if $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Proof. $\Rightarrow$: Assuming $>$ is a well-ordering, let α_0 be the smallest element of $\mathbb{Z}^n_{\geq 0}$. It suffices to show $\alpha_0 \geq 0$. This is easy: if $0 > \alpha_0$, then by hypothesis (ii), we can add α_0 to both sides to obtain $\alpha_0 > 2\alpha_0$, which is impossible since α_0 is the smallest element of $\mathbb{Z}^n_{\geq 0}$.

$\Leftarrow$: Assuming that $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$, let $A \subset \mathbb{Z}^n_{\geq 0}$ be nonempty. We need to show that A has a smallest element. Since $I = \langle x^\alpha : \alpha \in A \rangle$ is a monomial ideal, Dickson's Lemma gives us $\alpha(1), \ldots, \alpha(s) \in A$ so that $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Relabeling if necessary, we can assume that $\alpha(1) < \alpha(2) < \cdots < \alpha(s)$. We claim that $\alpha(1)$ is the smallest element of A. To prove this, take $\alpha \in A$. Then $x^\alpha \in I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, so that by Lemma 2, x^α is divisible by some $x^{\alpha(i)}$. This tells us that $\alpha = \alpha(i) + \gamma$ for some $\gamma \in \mathbb{Z}^n_{\geq 0}$. Then $\gamma \geq 0$ and hypothesis (ii) imply that

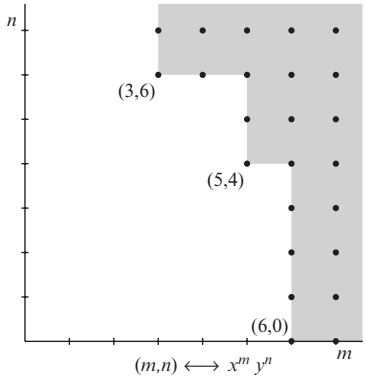
$$\alpha = \alpha(i) + \gamma \geq \alpha(i) + 0 = \alpha(i) \geq \alpha(1).$$

Thus, $\alpha(1)$ is the least element of A. □

As a result of this corollary, the definition of monomial ordering given in Definition 1 of §2 can be simplified. Conditions (i) and (ii) in the definition would be unchanged, but we could replace (iii) by the simpler condition that $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$. This makes it *much* easier to verify that a given ordering is actually a monomial ordering. See Exercises 10–12 for some examples.

EXERCISES FOR §4

1. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal with the property that for every $f = \sum c_\alpha x^\alpha \in I$, every monomial x^α appearing in f is also in I. Show that I is a monomial ideal.
2. Complete the proof of Lemma 3 begun in the text.
3. Let $I = \langle x^6, x^2y^3, xy^7 \rangle \subset k[x, y]$.
   a. In the (m, n)-plane, plot the set of exponent vectors (m, n) of monomials $x^m y^n$ appearing in elements of I.
   b. If we apply the division algorithm to an element $f \in k[x, y]$, using the generators of I as divisors, what terms can appear in the remainder?
4. Let $I \subset k[x, y]$ be the monomial ideal spanned over k by the monomials x^β corresponding to β in the shaded region below:



a. Use the method given in the proof of Theorem 5 to find an ideal basis for I.
b. Is your basis as small as possible, or can some β's be deleted from your basis, yielding a smaller set that generates the same ideal?

5. Suppose that $I = \langle x^\alpha : \alpha \in A\rangle$ is a monomial ideal, and let S be the set of all exponents that occur as monomials of I. For any monomial order $>$, prove that the smallest element of S with respect to $>$ must lie in A.
6. Let $I = \langle x^\alpha : \alpha \in A\rangle$ be a monomial ideal, and assume that we have a finite basis $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)}\rangle$. In the proof of Dickson's Lemma, we observed that each $x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ for some $\alpha(i) \in A$. Prove that $I = \langle x^{\alpha(1)}, \ldots., x^{\alpha(s)}\rangle$.
7. Prove that Dickson's Lemma (Theorem 5) is equivalent to the following statement: given a subset $A \subset \mathbb{Z}^n_{\geq 0}$, there are finitely many elements $\alpha(1), \ldots, \alpha(s) \in A$ such that for every $\alpha \in A$, there exists some i and some $\gamma \in \mathbb{Z}^n_{\geq 0}$ such that $\alpha = \alpha(i) + \gamma$.
8. A basis $[x^{\alpha(1)}, \ldots, x^{\alpha(s)}]$ for a monomial ideal I is said to be *minimal* if no $x^{\alpha(i)}$ in the basis divides another $x^{\alpha(j)}$ for $i \neq j$.
   a. Prove that every monomial ideal has a minimal basis.
   b. Show that every monomial ideal has a *unique* minimal basis.
9. If $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$ is a monomial ideal, prove that a polynomial f is in I if and only if the remainder of f on division by $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ is zero. Hint: Use Lemmas 2 and 3.
10. Suppose we have the polynomial ring $k[x_1, \ldots, x_n, \ldots, y_1, \ldots, y_m]$. Let us define a monomial order $>_{mixed}$ on this ring that mixes lex order for $x_1, \ldots, x_n$, with grlex order for $y_1, \ldots, y_m$. If we write monomials in the $n + m$ variables as $x^\alpha y^\beta$, where $\alpha \in \mathbb{Z}^n_{\geq 0}$ and $\beta \in \mathbb{Z}^m_{\geq 0}$, then we define

$$x^\alpha y^\beta >_{mixed} x^\gamma y^\delta \Longleftrightarrow x^\alpha >_{lex} x^\gamma \quad \text{or} \quad x^\alpha = x^\gamma \quad \text{and} \quad y^\beta >_{grlex} y^\delta.$$

    Use Corollary 6 to prove that $>_{mixed}$ is a monomial order. This is an example of what is called a *product order*. It is clear that many other monomial orders can be created by this method.
11. In this exercise we will investigate a special case of a *weight order*. Let $\mathbf{u} = (u_1, \ldots, u_n)$ be a vector in $\mathbb{R}^n$ such that $u_1, \ldots, u_n$ are positive and linearly independent over $\mathbb{Q}$. We say that $\mathbf{u}$ is an *independent weight vector*. Then, for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, define

$$\alpha >_{\mathbf{u}} \beta \Longleftrightarrow \mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta,$$

    where the centered dot is the usual dot product of vectors. We call $>_{\mathbf{u}}$ the *weight order* determined by $\mathbf{u}$.
    a. Use Corollary 6 to prove that $>_{\mathbf{u}}$ is a monomial order. Hint: Where does your argument use the linear independence of $u_1, \ldots, u_n$?
    b. Show that $\mathbf{u} = (1, \sqrt{2})$ is an independent weight vector, so that $>_{\mathbf{u}}$ is a weight order on $\mathbb{Z}^2_{\geq 0}$.
    c. Show that $u = (1, \sqrt{2}, \sqrt{3})$ is an independent weight vector, so that $>_{\mathbf{u}}$ is a weight order on $\mathbb{Z}^3_{\geq 0}$.
12. Another important weight order is constructed as follows. Let $\mathbf{u} = (u_1, \ldots, u_n)$ be in $\mathbb{Z}^n_{\geq 0}$, and fix a monomial order $>_\sigma$ (such as $>_{lex}$ or $>_{grevlex}$) on $\mathbb{Z}^n_{\geq 0}$. Then, for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, define $\alpha >_{\mathbf{u},\sigma} \beta$ if and only if

$$\mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta \quad \text{or} \quad \mathbf{u} \cdot \alpha = \mathbf{u} \cdot \beta \quad \text{and} \quad \alpha >_\sigma \beta.$$

    We call $>_{\mathbf{u},\sigma}$ the *weight order* determined by $\mathbf{u}$ and $>_\sigma$.
    a. Use Corollary 6 to prove that $>_{\mathbf{u},\sigma}$ is a monomial order.
    b. Find $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$ so that the weight order $>_{\mathbf{u},lex}$ is the grlex order $>_{grlex}$.

c. In the definition of $>_{\mathbf{u},\sigma}$, the order $>_\sigma$ is used to break ties, and it turns out that ties will *always* occur in this case. More precisely, prove that given $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$, there are $\alpha \neq \beta$ in $\mathbb{Z}^n_{\geq 0}$ such that $\mathbf{u} \cdot \alpha = \mathbf{u} \cdot \beta$. Hint: Consider the linear equation $u_1 a_1 + \cdots + u_n a_n = 0$ over $\mathbb{Q}$. Show that there is a nonzero integer solution $(a_1, \ldots, a_n)$, and then show that $(a_1, \ldots, a_n) = \alpha - \beta$ for some $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$.

d. A useful example of a weight order is the *elimination order* introduced by BAYER and STILLMAN (1987b). Fix an integer $1 \leq i \leq n$ and let $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$, where there are i 1's and $n - i$ 0's. Then the ith *elimination order* $>_i$ is the weight order $>_{\mathbf{u},grevlex}$. Prove that $>_i$ has the following property: if x^α is a monomial in which one of $x_1, \ldots, x_i$ appears, then $x^\alpha >_i x^\beta$ for *any* monomial involving only $x_{i+1}, \ldots, x_n$. Elimination orders play an important role in elimination theory, which we will study in the next chapter.

The weight orders described in Exercises 11 and 12 are only special cases of weight orders. In general, to determine a weight order, one starts with a vector $\mathbf{u}_1 \in \mathbb{R}^n$, whose entries may not be linearly independent over $\mathbb{Q}$. Then $\alpha > \beta$ if $\mathbf{u}_1 \cdot \alpha > \mathbf{u}_1 \cdot \beta$. But to break ties, one uses a second weight vector $\mathbf{u}_2 \in \mathbb{R}^n$. Thus, $\alpha > \beta$ also holds if $\mathbf{u}_1 \cdot \alpha = \mathbf{u}_1 \cdot \beta$ and $\mathbf{u}_2 \cdot \alpha > \mathbf{u}_2 \cdot \beta$. If there are still ties (when $\mathbf{u}_1 \cdot \alpha = \mathbf{u}_1 \cdot \beta$ and $\mathbf{u}_2 \cdot \alpha = \mathbf{u}_2 \cdot \beta$), then one uses a third weight vector $\mathbf{u}_3$, and so on. It can be proved that *every* monomial order on $\mathbb{Z}^n_{\geq 0}$ arises in this way. For a detailed treatment of weight orders and their relation to monomial orders, consult ROBBIANO (1986).

§5 The Hilbert Basis Theorem and Groebner Bases

In this section, we will give a complete solution of the *ideal description problem* from §1. Our treatment will also lead to ideal bases with "good" properties relative to the division algorithm introduced in §3. The key idea we will use is that once we choose a monomial ordering, each $f \in k[x_1, \ldots, x_n]$ has a unique leading term $\mathrm{LT}(f)$. Then, for any ideal I, we can define its *ideal of leading terms* as follows.

Definition 1. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$.*

(i) *We denote by $\mathrm{LT}(I)$ the set of leading terms of elements of I. Thus,*

$$\mathrm{LT}(I) = \{cx^\alpha : \textit{there exists } f \in I \textit{ with } \mathrm{LT}(f) = cx^\alpha\}.$$

(ii) *We denote by $\langle \mathrm{LT}(I) \rangle$ the ideal generated by the elements of $\mathrm{LT}(I)$.*

We have already seen that leading terms play an important role in the division algorithm. This brings up a subtle but important point concerning $\langle \mathrm{LT}(I) \rangle$. Namely, if we are given a finite generating set for I, say $I = \langle f_1, \ldots, f_s \rangle$, then $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ and $\langle \mathrm{LT}(I) \rangle$ may be *different* ideals. It is true that $\mathrm{LT}(f_i) \in \mathrm{LT}(I) \subset \langle \mathrm{LT}(I) \rangle$ by definition, which implies $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \subset \langle \mathrm{LT}(I) \rangle$. However, $\langle \mathrm{LT}(I) \rangle$ can be strictly larger. To see this, consider the following example.

Example 2. Let $I = \langle f_1, f_2 \rangle$, where $f_1 = x^3 - 2xy$ and $f_2 = x^2 y - 2y^2 + x$, and use the grlex ordering on monomials in $k[x, y]$. Then

$$x \cdot (x^2 y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2,$$

so that $x^2 \in I$. Thus $x^2 = \text{LT}(x^2) \in \langle \text{LT}(I) \rangle$. However x^2 is not divisible by $\text{LT}(f_1) = x^3$, or $\text{LT}(f_2) = x^2 y$, so that $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$ by Lemma 2 of §4.

In the exercises to §3, you computed other examples of ideals $I = \langle f_1, \ldots, f_s \rangle$, where $\langle \text{LT}(I) \rangle$ was strictly bigger than $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$. The exercises at the end of the section will explore what this implies about the ideal membership problem.

We will now show that $\langle \text{LT}(I) \rangle$ is a monomial ideal. This will allow us to apply the results of §4. In particular, it will follow that $\langle \text{LT}(I) \rangle$ is generated by finitely many leading terms.

Proposition 3. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal.*
(i) *$\langle \text{LT}(I) \rangle$ is a monomial ideal.*
(ii) *There are $g_1, \ldots, g_t \in I$ such that $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$.*

Proof. (i) The leading monomials $\text{LM}(g)$ of elements $g \in I - \{0\}$ generate the monomial ideal $\langle \text{LM}(g) : g \in I - \{0\} \rangle$. Since $\text{LM}(g)$ and $\text{LT}(g)$ differ by a nonzero constant, this ideal equals $\langle \text{LT}(g) : g \in I - \{0\} \rangle = \langle \text{LT}(I) \rangle$ (see Exercise 4). Thus, $\langle \text{LT}(I) \rangle$ is a monomial ideal.

(ii) Since $\langle \text{LT}(I) \rangle$ is generated by the monomials $\text{LM}(g)$ for $g \in I - \{0\}$, Dickson's Lemma from §4 tells us that $\langle \text{LT}(I) \rangle = \langle \text{LM}(g_1), \ldots, \text{LM}(g_t) \rangle$ for finitely many $g_1, \ldots, g_t \in I$. Since $\text{LM}(g_i)$ differs from $\text{LT}(g_i)$ by a nonzero constant, it follows that $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. This completes the proof. □

We can now use Proposition 3 and the division algorithm to prove the existence of a finite generating set of *every* polynomial ideal, thus giving an affirmative answer to the ideal description problem from §1. Let $I \subset k[x_1, \ldots, x_n]$ be any ideal and consider the associated ideal $\langle \text{LT}(I) \rangle$ as in Definition 1. As always, we have selected one particular monomial order to use in the division algorithm and in computing leading terms.

Theorem 4 (Hilbert Basis Theorem). *Every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in I$.*

Proof. If $I = \{0\}$, we take our generating set to be $\{0\}$, which is certainly finite. If I contains some nonzero polynomial, then a generating set $g_1, \ldots, g_t$ for I can be constructed as follows. By Proposition 3, there are $g_1, \ldots, g_t \in I$ such that $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots \text{LT}(g_t) \rangle$. We claim that $I = \langle g_1, \ldots, g_t \rangle$.

It is clear that $\langle g_1, \ldots, g_t \rangle \subset I$ since each $g_i \in I$. Conversely, let $f \in I$ be any polynomial. If we apply the division algorithm from §3 to divide f by $\langle g_1, \ldots, g_t \rangle$, then we get an expression of the form

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

where no term of r is divisible by any of $\text{LT}(g_1), \ldots, \text{LT}(g_t)$. We claim that $r = 0$. To see this, note that

$$r = f - a_1 g_1 - \cdots - a_t g_t \in I.$$

If $r \neq 0$, then $\text{LT}(r) \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots \text{LT}(g_t) \rangle$, and by Lemma 2 of §4, it follows that $\text{LT}(r)$ must be divisible by some $\text{LT}(g_i)$. This contradicts what it means to be a remainder, and, consequently, r must be zero. Thus,

$$f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle,$$

which shows that $I \subset \langle g_1, \ldots, g_t \rangle$. This completes the proof. □

In addition to answering the ideal description question, the basis $\{g_1, \ldots, g_t\}$ used in the proof of Theorem 4 has the special property that $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. As we saw in Example 2, not all bases of an ideal behave this way. We will give these special bases the following name.

Definition 5. *Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is said to be a* **Groebner basis** *(or* **standard basis***) if*

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle = \langle \text{LT}(I) \rangle.$$

Equivalently, but more informally, a set $\{g_1, \ldots, g_t\} \subset I$ is a Groebner basis of I if and only if the leading term of any element of I is divisible by one of the $\text{LT}(g_i)$ (this follows from Lemma 2 of §4—see Exercise 5). The proof of Theorem 4 also establishes the following result.

Corollary 6. *Fix a monomial order. Then every ideal $I \subset k[x_1, \ldots, x_n]$ other than $\{0\}$ has a Groebner basis. Furthermore, any Groebner basis for an ideal I is a basis of I.*

Proof. Given a nonzero ideal, the set $G = \{g_1, \ldots, g_t\}$ constructed in the proof of Theorem 4 is a Groebner basis by definition. For the second claim, note that if $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, then the argument given in Theorem 4 shows that $I = \langle g_1, \ldots, g_t \rangle$, so that G is a basis for I. (A slightly different proof is given in Exercise 6.) □

In §6 we will study the properties of Groebner bases in more detail, and, in particular, we will see how they give a solution of the ideal membership problem. Groebner bases are the "good" generating sets we hoped for at the end of §3.

For some examples of Groebner bases, first consider the ideal I from Example 2, which had the basis $\{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$. Then $\{f_1, f_2\}$ is *not* a Groebner basis for I with respect to grlex order since we saw in Example 2 that $x^2 \in \langle (\text{LT}(I) \rangle$, but $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$. In §7 we will learn how to find a Groebner basis of I.

Next, consider the ideal $J = \langle g_1, g_2 \rangle = \langle x + z, y - z \rangle$. We claim that g_1 and g_2 form a Groebner basis using lex order in $\mathbb{R}[x, y, z]$. Thus, we must show that the leading term of every nonzero element of J lies in the ideal $\langle \text{LT}(g_1), \text{LT}(g_2) \rangle = \langle x, y \rangle$. By Lemma 2 of §4, this is equivalent to showing that the leading term of *any* nonzero element of J is divisible by either x or y.

To prove this, consider any $f = A_{g_1} + B_{g_2} \in J$. Suppose on the contrary that f is nonzero and $\text{LT}(f)$ is divisible by neither x nor y. Then by the definition of lex order, f must be a polynomial in z alone. However, f vanishes on the linear subspace $L = \mathbf{V}(x+z, y-z) \subset \mathbb{R}^3$ since $f \in J$. It is easy to check that $(x, y, z) = (-t, t, t) \in L$ for any real number t. The only polynomial in z alone that vanishes at all of these points is the zero polynomial, which is a contradiction. It follows that $\langle g_1, g_2 \rangle$ is a Groebner basis for J. In §6, we will learn a more systematic way to detect when a basis is a Groebner basis.

Note, by the way, that the generators for the ideal J come from a row echelon matrix of coefficients:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

This is no accident: for ideals generated by linear polynomials, a Groebner basis for lex order is determined by the row echelon form of the matrix made from the coefficients of the generators (see Exercise 9).

Groebner bases for ideals in polynomial rings were introduced in 1965 by B. Buchberger and named by him in honor of W. Gröbner (1899–1980), Buchberger's thesis adviser. The closely related concept of "standard bases" for ideals in power series rings was discovered independently in 1964 by H. Hironaka. As we will see later in this chapter, Buchberger also developed the fundamental algorithms for working with Groebner bases. We will use the English form "Groebner bases," since this is how the command is spelled in some computer algebra systems.

We conclude this section with two applications of the Hilbert Basis Theorem. The first is an algebraic statement about the ideals in $k[x_1, \ldots, x_n]$. An **ascending chain** of ideals is a nested increasing sequence:

$$I_1 \subset I_2 \subset I_3 \subset \cdots .$$

For example, the sequence

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, \ldots, x_n \rangle \tag{1}$$

forms a (finite) ascending chain of ideals. If we try to *extend* this chain by including an ideal with further generator(s), one of two alternatives will occur. Consider the ideal $\langle x_1, \ldots, x_n, f \rangle$ where $f \in k[x_1, \ldots, x_n]$. If $f \in \langle x_1, \ldots, x_n \rangle$, then we obtain $\langle x_1, \ldots, x_n \rangle$ again and nothing has changed. If, on the other hand, $f \notin \langle x_1, \ldots, x_n \rangle$, then we claim $\langle x_1, \ldots, x_n, f \rangle = k[x_1, \ldots, x_n]$. We leave the proof of this claim to the reader (Exercise 11 of this section). As a result, the ascending chain (1) can be continued in only two ways, either by repeating the last ideal *ad infinitum* or by appending $k[x_1, \ldots, x_n]$ and then repeating it *ad infinitum*. In either case, the ascending chain will have "stabilized" after a finite number of steps, in the sense that all the ideals after that point in the chain will be equal. Our next result shows that the same phenomenon occurs in *every* ascending chain of ideals in $k[x_1, \ldots, x_n]$.

Theorem 7 (The Ascending Chain Condition). *Let*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

be an ascending chain of ideals in $k[x_1, \ldots, x_n]$. *Then there exists an* $N \geq 1$ *such that*

$$I_N = I_{N+1} = I_{N+2} = \cdots .$$

Proof. Given the ascending chain $I_1 \subset I_2 \subset I_3 \subset \cdots$, consider the set $I = \bigcup_{i=1}^{\infty} I_i$. We begin by showing that I is also an ideal in $k[x_1, \ldots, x_n]$. First, $0 \in I$ since $0 \in I_i$ for every i. Next, if $f, g \in I$, then, by definition, $f \in I_i$, and $g \in I_j$ for some i and j (possibly different). However, since the ideals I_i form an ascending chain, if we relabel so that $i \leq j$, then both f and g are in I_j. Since I_j is an ideal, the sum $f + g \in I_j$, hence, $\in I$. Similarly, if $f \in I$ and $r \in k[x_1, \ldots, x_n]$, then $f \in I_i$ for some i, and $r \cdot f \in I_i \subset I$. Hence, I is an ideal.

By the Hilbert Basis Theorem, the ideal I must have a finite generating set: $I = \langle f_1, \ldots, f_s \rangle$. But each of the generators is contained in some one of the I_j, say $f_i \in I_{j_i}$ for some $j_i, i = 1, \ldots, s$. We take N to be the maximum of the j_i. Then by the definition of an ascending chain $f_i \in I_N$ for all i. Hence we have

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I.$$

As a result the ascending chain stabilizes with I_N. All the subsequent ideals in the chain are equal. □

The statement that every ascending chain of ideals in $k[x_1, \ldots, x_n]$ stabilizes is often called the **ascending chain condition**, or ACC for short. In Exercise 12 of this section, you will show that if we assume the ACC as hypothesis, then it follows that every ideal is finitely generated. Thus, the ACC is actually equivalent to the conclusion of the Hilbert Basis Theorem. We will use the ACC in a crucial way in §7, when we give Buchberger's algorithm for constructing Groebner bases. We will also use the ACC in Chapter 4 to study the structure of affine varieties.

Our second consequence of the Hilbert Basis Theorem will be geometric. Up to this point, we have considered affine varieties as the sets of solutions of specific finite sets of polynomial equations:

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0 \text{ for all } i\}.$$

The Hilbert Basis Theorem shows that, in fact, it also makes sense to speak of the affine variety defined by an *ideal* $I \subset k[x_1, \ldots, x_n]$.

Definition 8. *Let* $I \subset k[x_1, \ldots, x_n]$ *be an ideal. We will denote by* $\mathbf{V}(I)$ *the set*

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

Even though a nonzero ideal I always contains infinitely many different polynomials, the set $\mathbf{V}(I)$ can still be defined by a finite set of polynomial equations.

Proposition 9. $\mathbf{V}(I)$ *is an affine variety. In particular, if* $I = \langle f_1, \ldots, f_s \rangle$, *then* $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

Proof. By the Hilbert Basis Theorem, $I = \langle f_1, \ldots, f_s \rangle$ for some finite generating set. We claim that $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$. First, since the $f_i \in I$, if $f(a_1, \ldots, a_n) = 0$ for all $f \in I$, then $f_i(a_1, \ldots, a_n) = 0$, so $\mathbf{V}(I) \subset \mathbf{V}(f_1, \ldots, f_s)$. On the other hand, let $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$ and let $f \in I$. Since $I = \langle f_1, \ldots, f_s \rangle$, we can write

$$f = \sum_{i=1}^{s} h_i f_i$$

for some $h_i \in k[x_1, \ldots, x_n]$. But then

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0. \end{aligned}$$

Thus, $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{V}(I)$ and, hence, they are equal. □

The most important consequence of this proposition is that *varieties are determined by ideals*. For example, in Chapter 1, we proved that $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$ whenever $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$ (see Proposition 4 of Chapter 1, §4). This proposition is an immediate corollary of Proposition 9. The relation between ideals and varieties will be explored in more detail in Chapter 4.

In the exercises, we will exploit Proposition 9 by showing that by using the right generating set for an ideal I, we can gain a better understanding of the variety $\mathbf{V}(I)$.

EXERCISES FOR §5

1. Let $I = \langle g_1, g_2, g_3 \rangle \subset \mathbb{R}[x, y, z]$, where $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$ and $g_3 = x - yz^4$. Using the lex order, give an example of $g \in I$ such that $\mathrm{LT}(g) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle$.
2. For the ideals and generators given in Exercises 5, 6, and 7 of §3, show that $\mathrm{LT}(I)$ is strictly bigger than $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$. Hint: This should follow directly from what you did in those exercises.
3. To generalize the situation of Exercises 1 and 2, suppose that $I = \langle f_1, \ldots, f_s \rangle$ is an ideal such that $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ is strictly smaller than $\langle \mathrm{LT}(I) \rangle$.
   a. Prove that there is some $f \in I$ whose remainder on division by $f_1, \ldots, f_s$ is nonzero. Hint: First show that $\mathrm{LT}(f) \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ for some $f \in I$. Then use Lemma 2 of §4.
   b. What does part a say about the ideal membership problem?
   c. How does part a relate to the conjecture you were asked to make in Exercise 8 of §3?
4. If $I \subset k[x_1, \ldots, x_n]$ is an ideal, prove that $\langle \mathrm{LT}(g) : g \in I - \{0\} \rangle = \langle \mathrm{LM}(g) : g \in I - \{0\} \rangle$.
5. Let I be an ideal of $k[x_1, \ldots, x_n]$. Show that $G = \{g_1, \ldots, g_t\} \subset I$ is a Groebner basis of I if and only if the leading term of any element of I is divisible by one of the $\mathrm{LT}(g_i)$.
6. Corollary 6 asserts that a Groebner basis is a basis, i.e., if $G = \{g_1, \ldots, g_t\} \subset I$ satisfies $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, then $I = \langle g_1, \ldots, g_t \rangle$. We gave one proof of this in the proof of Theorem 4. Complete the following sketch to give a second proof. If $f \in I$, then divide f by $(g_1, \ldots, g_t)$. At each step of the division algorithm, the leading term of the polynomial under the radical will be in $\langle \mathrm{LT}(I) \rangle$ and, hence, will be divisible by one of the

$\text{LT}(g_i)$. Hence, terms are never added to the remainder, so that $f = \sum_{i=1}^{t} a_i g_i$ when the algorithm terminates.

7. If we use grlex order with $x > y > z$, is $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$ a Groebner basis for the ideal generated by these polynomials? Why or why not?
8. Repeat Exercise 7 for $I = \langle x - z^2, y - z^3 \rangle$ using the lex order. Hint: The difficult part of this exercise is to determine exactly which polynomials are in $\langle \text{LT}(I) \rangle$.
9. Let $A = (a_{ij})$ be an $m \times n$ matrix with real entries in row echelon form and let $J \subset \mathbb{R}[x_1, \ldots, x_n]$ be an ideal generated by the linear polynomials $\sum_{j=1}^{n} a_{ij}x_j$ for $1 \leq i \leq m$. Show that the given generators form a Groebner basis for J with respect to a suitable lexicographic order. Hint: Order the variables corresponding to the leading 1's before the other variables.
10. Let $I \subset k[x_1, \ldots, x_n]$ be a *principal ideal* (that is, I is generated by a single $f \in I$—see §5 of Chapter 1). Show that any finite subset of I containing a generator for I is a Groebner basis for I.
11. Let $f \in k[x_1, \ldots, x_n]$. If $f \notin \langle x_1, \ldots, x_n \rangle$, then show $\langle x_1, \ldots, x_n, f \rangle = k[x_1, \ldots, x_n]$.
12. Show that if we take as hypothesis that every ascending chain of ideals in $k[x_1, \ldots, x_n]$ stabilizes, then the conclusion of the Hilbert Basis Theorem is a consequence. Hint: Argue by contradiction, assuming that some ideal $I \subset k[x_1, \ldots, x_n]$ has no finite generating set. The arguments you gave in Exercise 12 should not make any special use of properties of polynomials. Indeed, it is true that in any commutative ring R, the following two statements are equivalent:
    i. Every ideal $I \subset R$ is finitely generated.
    ii. Every ascending chain of ideals of R stabilizes.
13. Let
$$V_1 \supset V_2 \supset V_3 \supset \cdots$$
be a **descending chain** of affine varieties. Show that there is some $N \geq 1$ such that $V_N = V_{N+1} = V_{N+2} = \cdots$. Hint: Use Exercise 14 of Chapter 1, §4.
14. Let $f_1, f_2, \ldots \in k[x_1, \ldots, x_n]$ be an infinite collection of polynomials and let $I = \langle f_1, f_2, \ldots \rangle$ be the ideal they generate. Prove that there is an integer N such that $I = \langle f_1, \ldots, f_N \rangle$. Hint: Use $f_1, f_2, \ldots$ to create an ascending chain of ideals.
15. Given polynomials $f_1, f_2, \ldots \in k[x_1, \ldots, x_n]$, let $\mathbf{V}(f_1, f_2, \ldots) \subset k^n$ be the solutions of the infinite system of equations $f_1 = f_2 = \cdots 0$. Show that there is some N such that $\mathbf{V}(f_1, f_2, \ldots) = \mathbf{V}(f_1, \ldots, f_N)$.
16. In Chapter 1, §4, we defined the ideal $\mathbf{I}(V)$ of a variety $V \subset k^n$. In this section, we defined the variety of any ideal (see Definition 8). In particular, this means that $\mathbf{V}(\mathbf{I}(V))$ is a variety. Prove that $\mathbf{V}(\mathbf{I}(V)) = V$. Hint: See the proof of Lemma 7 of Chapter 1, §4.
17. Consider the variety $V = \mathbf{V}(x^2 - y, y + x^2 - 4) \subset \mathbb{C}^2$. Note that $V = \mathbf{V}(I)$, where $I = \langle x^2 - y, y + x^2 - 4 \rangle$.
    a. Prove that $I = \langle x^2 - y, x^2 - 2 \rangle$.
    b. Using the basis from part a, prove that $\mathbf{V}(I) = \{(\pm\sqrt{2}, 2)\}$.

    One reason why the second basis made V easier to understand was that $x^2 - 2$ could be *factored*. This implied that V "split" into two pieces. See Exercise 18 for a general statement.
18. When an ideal has a basis where some of the elements can be factored, we can use the factorization to help understand the variety.
    a. Show that if $g \in k[x_1, \ldots, x_n]$ factors as $g = g_1g_2$, then for any f, $\mathbf{V}(f, g) = \mathbf{V}(f, g_1) \cup \mathbf{V}(f, g_2)$.
    b. Show that in $\mathbb{R}^3$, $\mathbf{V}(y - x^2, xz - y^2) = \mathbf{V}(y - x^2, xz - x^4)$.
    c. Use part a to describe and/or sketch the variety from part b.

§6 Properties of Groebner Bases

As shown in §5, every nonzero ideal $I \subset k[x_1, \ldots, x_n]$ has a Groebner basis. In this section, we will study the properties of Groebner bases and learn how to detect when a given basis is a Groebner basis. We begin by showing that the undesirable behavior of the division algorithm in $k[x_1, \ldots, x_n]$ noted in §3 does not occur when we divide by the elements of a Groebner basis.

Let us first prove that the remainder is uniquely determined when we divide by a Groebner basis.

Proposition 1. *Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then there is a unique $r \in k[x_1, \ldots, x_n]$ with the following two properties:*

(i) *No term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.*

(ii) *There is $g \in I$ such that $f = g + r$.*

In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm.

Proof. The division algorithm gives $f = a_1 g_1 + \cdots + a_t g_t + r$, where r satisfies (i). We can also satisfy (ii) by setting $g = a_1 g_1 + \cdots + a_t g_t \in I$. This proves the existence of r.

To prove uniqueness, suppose that $f = g + r = g' + r'$ satisfy (i) and (ii). Then $r - r' = g' - g \in I$, so that if $r \neq r'$, then $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. By Lemma 2 of §4, it follows that $\mathrm{LT}(r - r')$ is divisible by some $\mathrm{LT}(g_i)$. This is impossible since no term of r, r' is divisible by one of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Thus $r - r'$ must be zero, and uniqueness is proved.

The final part of the proposition follows from the uniqueness of r. □

The remainder r is sometimes called the *normal form of f*, and its uniqueness properties will be explored in Exercises 1 and 4. In fact, Groebner bases can be characterized by the uniqueness of the remainder—see Theorem 5.35 of BECKER and WEISPFENNING (1993) for this and other conditions equivalent to being a Groebner basis.

Although the remainder r is unique, even for a Groebner basis, the "quotients" a_i produced by the division algorithm $f = a_1 g_1 + \cdots + a_t g_t + r$ can change if we list the generators in a different order. See Exercise 2 for an example.

As a corollary, we get the following criterion for when a polynomial lies in an ideal.

Corollary 2. *Let $G = \{g_t, \ldots, g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

Proof. If the remainder is zero, then we have already observed that $f \in I$. Conversely, given $f \in I$, then $f = f + 0$ satisfies the two conditions of Proposition 1. It follows that 0 is the remainder of f on division by G. □

The property given in Corollary 2 is sometimes taken as the definition of a Groebner basis, since one can show that it is true if and only if $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$ (see Exercise 3). For this and similar conditions equivalent to being a Groebner basis, see Proposition 5.38 of BECKER and WEISPFENNING (1993).

Using Corollary 2, we get an algorithm for solving the ideal membership problem from §1 *provided* that we know a Groebner basis G for the ideal in question—we only need to compute a remainder with respect to G to determine whether $f \in I$. In §7, we will learn how to find Groebner bases, and we will give a complete solution of the ideal membership problem in §8.

We will use the following notation for the remainder.

Definition 3. *We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$. If F is a Groebner basis for $(f_1, \ldots, f_s)$, then we can regard F as a set (without any particular order) by Proposition 1.*

For instance, with $F = (x^2y - y^2, x^4y^2 - y^2) \subset k[x, y]$, using the lex order, we have

$$\overline{x^5y}^F = xy^3$$

since the division algorithm yields

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

We next will discuss how to tell whether a given generating set of an ideal is a Groebner basis. As we have indicated, the "obstruction" to $\{f_1, \ldots, f_s\}$ being a Groebner basis is the possible occurrence of polynomial combinations of the f_i whose leading terms are not in the ideal generated by the $\mathrm{LT}(f_i)$. One way this can occur is if the leading terms in a suitable combination

$$ax^\alpha f_i - bx^\beta f_j$$

cancel, leaving only smaller terms. On the other hand, $ax^\alpha f_i - bx^\beta f_j \in I$, so its leading term is in $\langle \mathrm{LT}(I)\rangle$. You should check that this is what happened in Example 2 of §5. To study this cancellation phenomenon, we introduce the following special combinations.

Definition 4. *Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials.*

(i) *If multideg$(f) = \alpha$ and multideg$(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^γ the* **least common multiple** *of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$.*

(ii) *The* **S-polynomial** *of f and g is the combination*

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

(Note that we are inverting the leading coefficients here as well.)

For example, let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $\mathbb{R}[x, y]$ with the grlex order. Then $\gamma = (4, 2)$ and

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

An S-polynomial $S(f, g)$ is "designed" to produce cancellation of leading terms. In fact, the following lemma shows that every cancellation of leading terms among polynomials of the same multidegree results from this sort of cancellation.

Lemma 5. *Suppose we have a sum $\sum_{i=1}^{s} c_i f_i$, where $c_i \in k$ and $\text{multideg}(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ for all i. If $\text{multideg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$, then $\sum_{i=1}^{s} c_i f_i$ is a linear combination, with coefficients in k, of the S-polynomials $S(f_j, f_k)$ for $1 \leq j, k \leq s$. Furthermore, each $S(f_i, f_k)$ has multidegree $< \delta$.*

Proof. Let $d_i = \text{LC}(f_i)$, so that $c_i d_i$ is the leading coefficient of $c_i f_i$. Since the $c_i f_i$ all have multidegree δ and their sum has strictly smaller multidegree, it follows easily that $\sum_{i=1}^{s} c_i d_i = 0$.

Define $p_i = f_i/d_i$, and note that p_i has leading coefficient 1. Consider the telescoping sum

$$\begin{aligned} \sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \\ &\quad (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s. \end{aligned}$$

By assumption, $\text{LT}(f_i) = d_i x^\delta$, which implies that the least common multiple of $\text{LM}(f_j)$ and $\text{LM}(f_k)$ is x^δ. Thus

$$S(f_j, f_k) = \frac{x^\delta}{\text{LT}(f_j)} f_j - \frac{x^\delta}{\text{LT}(f_k)} f_k = \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_k x^\delta} f_k = p_j - p_k. \tag{1}$$

Using this equation and $\sum_{i=1}^{s} c_i d_i = 0$, the above telescoping sum becomes

$$\begin{aligned} \sum_{i=1}^{s} c_i f_i &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) \\ &\quad + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s), \end{aligned}$$

which is a sum of the desired form. Since p_j and p_k have multidegree δ and leading coefficient 1, the difference $p_j - p_k$ has multidegree $< \delta$. By equation (1), the same is true of $S(f_j, f_k)$, and the lemma is proved. □

When $f_1, \ldots, f_s$ satisfy the hypothesis of Lemma 5, we get an equation of the form

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{jk} S(f_j, f_k).$$

Let us consider where the cancellation occurs. In the sum on the left, every summand $c_i f_i$ has multidegree δ, so the cancellation occurs only after adding them up. However, in the sum on the right, each summand $c_{jk}S(f_j, f_k)$ has multidegree $< \delta$, so that the cancellation has already occurred. Intuitively, this means that all cancellation can be accounted for by S-polynomials.

Using S-polynomials and Lemma 5, we can now prove the following criterion of Buchberger for when a basis of an ideal is a Groebner basis.

Theorem 6 (Buchberger's Criterion). *Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ for I is a Groebner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.*

Proof. $\Rightarrow$: If G is a Groebner basis, then since $S(g_i, g_j) \in I$, the remainder on division by G is zero by Corollary 2.

$\Leftarrow$: Let $f \in I$ be a nonzero polynomial. We must show that if the S-polynomials all have zero remainders on division by G, then $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$. Before giving the details, let us outline the strategy of the proof.

Given $f \in I = (g_1, \ldots, g_t)$, there are polynomials $h_i \in k[x_1, \ldots, x_n]$ such that

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2}$$

From Lemma 8 of §2, it follows that

$$\mathrm{multideg}(f) \leq \max(\mathrm{multideg}(h_i g_i)). \tag{3}$$

If equality does not occur, then some cancellation must occur among the leading terms of (2). Lemma 5 will enable us to rewrite this in terms of S-polynomials. Then our assumption that S-polynomials have zero remainders will allow us to replace the S-polynomials by expressions that involve less cancellation. Thus, we will get an expression for f that has less cancellation of leading terms. Continuing in this way, we will eventually find an expression (2) for f where equality occurs in (3). Then $\mathrm{multideg}(f) = \mathrm{multideg}(h_i g_i)$ for some i, and it will follow that $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$. This will show that $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$, which is what we want to prove.

We now give the details of the proof. Given an expression (2) for f, let $m(i) = \mathrm{multideg}(h_i g_i)$, and define $\delta = \max(m(1), \ldots, m(t))$. Then inequality (3) becomes

$$\mathrm{multideg}(f) \leq \delta.$$

Now consider *all* possible ways that f can be written in the form (2). For each such expression, we get a possibly different δ. Since a monomial order is a well-ordering, we can select an expression (2) for f such that δ is *minimal*.

We will show that once this minimal δ is chosen, we have $\mathrm{multideg}(f) = \delta$. Then equality occurs in (3), and as we observed, it follows that $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$. This will prove the theorem.

It remains to show $\mathrm{multideg}(f) = \delta$. We will prove this by contradiction. Equality can fail only when $\mathrm{multideg}(f) < \delta$. To isolate the terms of multidegree δ, let us write

f in the following form:

$$
\begin{aligned}
f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\
&= \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i
\end{aligned} \tag{4}
$$

The monomials appearing in the second and third sums on the second line all have multidegree $< \delta$. Thus, the assumption $\mathrm{multideg}(f) < \delta$ means that the first sum also has multidegree $< \delta$.

Let $\mathrm{LT}(h_i) = c_i x^{\alpha(i)}$. Then the first sum $\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ has exactly the form described in Lemma 5 with $f_i = x^{\alpha(i)} g_i$. Thus Lemma 5 implies that this sum is a linear combination of the S-polynomials $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$. However,

$$
\begin{aligned}
S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) &= \frac{x^\delta}{x^{\alpha(j)} \mathrm{LT}(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)} \mathrm{LT}(g_k)} x^{\alpha(k)} g_k \\
&= x^{\delta - \gamma_{jk}} S(g_j, g_k),
\end{aligned}
$$

where $x^{\gamma_{jk}} = \mathrm{LCM}(\mathrm{LM}(g_j), \mathrm{LM}(g_k))$. Thus there are constants $c_{jk} \in k$ such that

$$
\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k). \tag{5}
$$

The next step is to use our hypothesis that the remainder of $S(g_j, g_k)$ on division by $g_1, \ldots, g_t$ is zero. Using the division algorithm, this means that each S-polynomial can be written in the form

$$
S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{6}
$$

where $a_{ijk} \in k[x_1, \ldots, x_n]$. The division algorithm also tells us that

$$
\mathrm{multideg}(a_{ijk} g_i) \leq \mathrm{multideg}(S(g_j, g_k)) \tag{7}
$$

for all i, j, k (see Theorem 3 of §3). Intuitively, this says that when the remainder is zero, we can find an expression for $S(g_j, g_k)$ in terms of G where the leading terms do not all cancel.

To exploit this, multiply the expression for $S(g_j, g_k)$ by $x^{\delta - \gamma_{jk}}$ to obtain

$$
x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i,
$$

where $b_{ijk} = x^{\delta - \gamma_{jk}} a_{ijk}$. Then (7) and Lemma 5 imply that

$$
\mathrm{multideg}(b_{ijk} g_i) \leq \mathrm{multideg}(x^{\delta - \gamma_{jk}} S(g_j, g_k)) < \delta. \tag{8}
$$

If we substitute the above expression for $x^{\delta - \gamma_{jk}} S(g_j, g_k)$ into (5), we get an equation

$$
\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_i b_{ijk} g_i \right) = \sum_i \tilde{h}_i g_i
$$

which by (8) has the property that for all i,

$$\text{multideg}(\tilde{h}_i g_i) < \delta.$$

For the final step in the proof, substitute $\sum_{m(i)=\delta} \text{LT}(h_i)g_i = \sum_i \tilde{h}_i g_i$ into equation (4) to obtain an expression for f as a polynomial combination of the g_i's where *all* terms have multidegree $< \delta$. This contradicts the minimality of δ and completes the proof of the theorem. □

The Buchberger Criterion given in Theorem 6 is one of the key results about Groebner bases. We have seen that Groebner bases have many nice properties, but, so far, it has been difficult to determine if a basis of an ideal is a Groebner basis (the examples we gave in §5 were rather trivial). Using the S-pair criterion, however, it is now easy to show whether a given basis is a Groebner basis. Furthermore, in §7, we will see that the S-pair criterion also leads naturally to an algorithm for computing Groebner bases.

As an example of how to use Theorem 6, consider the ideal $I = \langle y - x^2, z - x^3 \rangle$ of the twisted cubic in $\mathbb{R}^3$. We claim that $G = \{y - x^2, z - x^3\}$ is a Groebner basis for lex order with $y > z > x$. To prove this, consider the S-polynomial

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Using the division algorithm, one finds

$$-zx^2 + yx^3 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0,$$

so that $\overline{S(y - x^2, z - x^3)}^G = 0$. Thus, by Theorem 6, G is a Groebner basis for I. You can also check that G is *not* a Groebner basis for lex order with $x > y > z$ (see Exercise 8).

EXERCISES FOR §6

1. Show that Proposition 1 can be strengthened slightly as follows. Fix a monomial ordering and let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Suppose that $f \in k[x_1, \ldots, x_n]$.
   a. Show that f can be written in the form $f = g + r$, where $g \in I$ and no term of r is divisible by any element of $\text{LT}(I)$.
   b. Given two expressions $f = g + r = g' + r'$ as in part (a), prove that $r = r'$. Thus, r is uniquely determined.

   This result shows once a monomial order is fixed, we can define a unique "remainder of f on division by I." We will exploit this idea in Chapter 5.
2. In §5, we showed that $G = \{x + z, y - z\}$ is a Groebner basis for lex order. Let us use this basis to study the uniqueness of the division algorithm.
   a. Divide xy by $x + z, y - z$.
   b. Now reverse the order and divide xy by $y - z, x + z$.

   You should get the same remainder (as predicted by Proposition 1), but the "quotients" should be different for the two divisions. This shows that the uniqueness of the remainder is the best one can hope for.
3. In Corollary 2, we showed that if $I = \langle g_1, \ldots, g_t \rangle$ and if $G = \{g_1, \ldots, g_t\}$ is a Groebner basis for I, then $\overline{f}^G = 0$ for all $f \in I$. Prove the converse of this statement. Namely, show that if G is a basis for I with the property that $\overline{f}^G = 0$ for all $f \in I$, then G is a Groebner basis for I.

4. Let G and G' be Groebner bases for an ideal I with respect to the same monomial order in $k[x_1, \ldots, x_n]$. Show that $\overline{f}^G = \overline{f}^{G'}$ for all $f \in k[x_1, \ldots, x_n]$. Hence, the remainder on division by a Groebner basis is even independent of which Groebner basis we use, as long as we use one particular monomial order. Hint: See Exercise 1.
5. Compute $S(f, g)$ using the lex order.
   a. $f = 4x^2z - 7y^2, \quad g = xyz^2 + 3xz^4$.
   b. $f = x^4y - z^2, \quad g = 3xz^2 - y$.
   c. $f = x^7y^2z + 2ixyz, \quad g = 2x^7y^2z + 4$.
   d. $f = xy + z^3, \quad g = z^2 - 3z$.
6. Does $S(f, g)$ depend on which monomial order is used? Illustrate your assertion with examples.
7. Prove that $\text{multideg}(S(f, g)) < \gamma$, where $x^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$. Explain why this inequality is a precise version of the claim that S-polynomials are designed to produce cancellation.
8. Show that $\{y - x^2, z - x^3\}$ is not a Groebner basis for lex order with $x > y > z$.
9. Using Theorem 6, determine whether the following sets G are Groebner bases for the ideal they generate. You may want to use a computer algebra system to compute the S-polynomials and remainders.
   a. $G = \{x^2 - y, x^3 - z\}$ grlex order.
   b. $G = \{x^2 - y, x^3 - z\}$ invlex order (see Exercise 6 of §2).
   c. $G = \{xy^2 - xz + y, xy - z^2, x - yz^4\}$ lex order.
10. Let $f, g \in k[x_1, \ldots, x_n]$ be polynomials such that $\text{LM}(f)$ and $\text{LM}(g)$ are *relatively prime* monomials and $\text{LC}(f) = \text{LC}(g) = 1$.
    a. Show that $S(f, g) = -(g - \text{LT}(g))f + (f - \text{LT}(f))g$.
    b. Deduce that the leading monomial of $S(f, g)$ is a multiple of either $\text{LM}(f)$ or $\text{LM}(g)$ in this case.
11. Let $f, g \in k[x_1, \ldots, x_n]$ and x^α, x^β be monomials. Verify that
$$S(x^\alpha f, x^\beta g) = x^\gamma S(f, g)$$
where
$$x^\gamma = \frac{\text{LCM}(x^\alpha \text{LM}(f), x^\alpha \text{LM}(g))}{\text{LCM}(\text{LM}(f), \text{LM}(g))}.$$
Be sure to prove that x^γ is a monomial.
12. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let G be a Groebner basis of I.
    a. Show that $\overline{f}^G = \overline{g}^G$ if and only if $f - g \in I$. Hint: See Exercise 1.
    b. Deduce that
$$\overline{f + g}^G = \overline{f}^G + \overline{g}^G.$$
    Hint: Use part (a).
    c. Deduce that
$$\overline{fg}^G = \overline{\overline{f}^G \cdot \overline{g}^G}^G.$$

We will return to an interesting consequence of these facts in Chapter 5.

§7 Buchberger's Algorithm

In Corollary 6 of §5, we saw that every ideal in $k[x_1, \ldots, x_n]$ other than 0 has a Groebner basis. Unfortunately, the proof given was nonconstructive in the sense that it did not

tell us how to produce the Groebner basis. So we now turn to the question: given an ideal $I \subset k[x_1, \ldots, x_n]$, how can we actually construct a Groebner basis for I? To see the main ideas behind the method we will use, we return to the ideal of Example 2 from §5 and proceed as follows.

Example 1. Consider the ring $k[x, y]$ with grlex order, and let $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Recall that $\{f_1, f_2\}$ is not a Groebner basis for I since $\text{LT}(S(f_1, f_2)) = -x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2)\rangle$.

To produce a Groebner basis, one natural idea is to try first to extend the original generating set to a Groebner basis by adding more polynomials in I. In one sense, this adds nothing new, and even introduces an element of redundancy. However, the extra information we get from a Groebner basis more than makes up for this.

What new generators should we add? By what we have said about the S-polynomials in §6, the following should come as no surprise. We have $S(f_1, f_2) = -x^2 \in I$, and its remainder on division by $F = (f_1, f_2)$ is $-x^2$, which is nonzero. Hence, we should include that remainder in our generating set, as a new generator $f_3 = -x^2$. If we set $F = (f_1, f_2, f_3)$, we can use Theorem 6 of §6 to test if this new set is a Groebner basis for I. We compute

$$\begin{aligned}
&S(f_1, f_2) = f_3, \text{ so}\\
&\overline{S(f_1, f_2)}^F = 0,\\
&S(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy, \text{ but}\\
&\overline{S(f_1, f_3)}^F = -2xy \neq 0.
\end{aligned}$$

Hence, we must add $f_4 = -2xy$ to our generating set. If we let $F = (f_1, f_2, f_3, f_4)$, then by Exercise 12 we have

$$\begin{aligned}
&\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0,\\
&S(f_1, f_4) = y(x^3 - 2xy) - (-1/2)x^2(-2xy) = -2xy^2 = yf_4, \text{ so}\\
&\overline{S(f_1, f_4)}^F = 0,\\
&S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \text{ but}\\
&\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0.
\end{aligned}$$

Thus, we must also add $f_5 = -2y^2 + x$ to our generating set. Setting $F = \{f_1, f_2, f_3, f_4, f_5\}$, one can compute that

$$\overline{S(f_i, f_j)}^F = 0 \text{ for all } 1 \leq i \leq j \leq 5.$$

By Theorem 6 of §6, it follows that a grlex Groebner basis for I is given by

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

The above example suggests that in general, one should try to extend a basis F to a Groebner basis by successively adding nonzero remainders $\overline{S(f_i, f_j)}^F$ to F. This idea is a natural consequence of the S-pair criterion from §6 and leads to the following algorithm due to Buchberger for computing a Groebner basis.

Theorem 2 (Buchberger's Algorithm). *Let $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm:*

Input: $F = (f_1, \ldots, f_s)$
Output: a Groebner basis $G = (g_1, \ldots, g_t)$ for I, with $F \subset G$

$G := F$
REPEAT
  $G' := G$
  FOR each pair $\{p, q\}$, $p \neq q$ in G' DO
    $S := \overline{S(p,q)}^{G'}$
    IF $S \neq 0$ THEN $G := G \cup \{S\}$
UNTIL $G = G'$

Proof. We begin with some frequently used notation. If $G = \{g_1, \ldots, g_t\}$, then $\langle G \rangle$ and $\langle \text{LT}(G) \rangle$ will denote the following ideals:

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle$$
$$\langle \text{LT}(G) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle.$$

Turning to the proof of the theorem, we first show that $G \subset I$ holds at every stage of the algorithm. This is true initially, and whenever we enlarge G, we do so by adding the remainder $S = \overline{S(p,q)}^{G'}$ for $p, q \in G$. Thus, if $G \subset I$, then p, q and, hence, $S(p, q)$ are in I, and since we are dividing by $G' \subset I$, we get $G \cup \{S\} \subset I$. We also note that G contains the given basis F of I so that G is actually a basis of I.

The algorithm terminates when $G = G'$, which means that $S = \overline{S(p,q)}^{G'} = 0$ for all $p, q \in G$. Hence G is a Groebner basis of $\langle G \rangle = I$ by Theorem 6 of §6.

It remains to prove that the algorithm terminates. We need to consider what happens after each pass through the main loop. The set G consists of G' (the old G) together with the nonzero remainders of S-polynomials of elements of G'. Then

$$\langle \text{LT}(G') \rangle \subset \langle \text{LT}(G) \rangle \tag{1}$$

since $G' \subset G$. Furthermore, if $G' \neq G$, we claim that $\langle \text{LT}(G') \rangle$ is strictly smaller than $\langle \text{LT}(G) \rangle$. To see this, suppose that a nonzero remainder r of an S-polynomial has been adjoined to G. Since r is a remainder on division by G', $\text{LT}(r)$ is not divisible by the leading terms of elements of G', and thus $\text{LT}(r) \notin \langle \text{LT}(G') \rangle$. Yet $\text{LT}(r) \in \langle \text{LT}(G) \rangle$, which proves our claim.

By (1), the ideals $\langle \text{LT}(G') \rangle$ from successive iterations of the loop form an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Thus, the ACC (Theorem 7 of §5) implies that after a finite number of iterations the chain will stabilize, so that $\langle \text{LT}(G') \rangle = \langle \text{LT}(G) \rangle$ must happen eventually. By the previous paragraph, this implies that $G' = G$, so that the algorithm must terminate after a finite number of steps. □

Taken together, the Buchberger criterion (Theorem 6 of §6) and the Buchberger algorithm (Theorem 2 above) provide an algorithmic basis for the theory of Groebner bases. These contributions of Buchberger are central to the development of the subject. In §8, we will get our first hints of what can be done with these methods, and a large part of the rest of the book will be devoted to exploring their ramifications.

We should also point out the algorithm presented in Theorem 2 is only a rudimentary version of the Buchberger algorithm. It was chosen for what we hope will be its clarity for the reader, but it is not a very practical way to do the computation. Note (as a first improvement) that once a remainder $\overline{S(p,q)}^{G'} = 0$, that remainder will stay zero even if we adjoin further elements to the generating set G'. Thus, there is no reason to recompute those remainders on subsequent passes through the main loop. Indeed, if we add our new generators f_j one at a time, the only remainders that need to be checked are $\overline{S(f_i, f_j)}^{G'}$, where $i \leq j-1$. It is a good exercise to revise the algorithm to take this observation into account. Other improvements of a deeper nature can also be made, but we will postpone considering them until §9.

Groebner bases computed using the algorithm of Theorem 2 are often bigger than necessary. We can eliminate some unneeded generators by using the following fact.

Lemma 3. *Let G be a Groebner basis for the polynomial ideal I. Let $p \in G$ be a polynomial such that $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$. Then $G - \{p\}$ is also a Groebner basis for I.*

Proof. We know that $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. If $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$, then we have $\langle \mathrm{LT}(G - \{p\})\rangle = \langle \mathrm{LT}(G)\rangle$. By definition, it follows that $G - \{p\}$ is also a Groebner basis for I. □

By adjusting constants to make all leading coefficients 1 and removing any p with $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$ from G, we arrive at what we will call a **minimal** Groebner basis.

Definition 4. *A* **minimal Groebner basis** *for a polynomial ideal I is a Groebner basis G for I such that:*
(i) $\mathrm{LC}(p) = 1$ *for all* $p \in G$.
(ii) *For all* $p \in G$, $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle$.

We can construct a minimal Groebner basis for a given nonzero ideal by applying the algorithm of Theorem 2 and then using Lemma 3 to eliminate any unneeded generators that might have been included. To illustrate this procedure, we return once again to the ideal I studied in Example 1. Using grlex order, we found the Groebner basis

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2y - 2y^2 + x, \\ f_3 &= -x^2, \\ f_4 &= -2xy, \\ f_5 &= -2y^2 + x. \end{aligned}$$

Since some of the leading coefficients are different from 1, the first step is to multiply the generators by suitable constants to make this true. Then note that $\text{LT}(f_1) = x^3 = -x \cdot \text{LT}(f_3)$. By Lemma 3, we can dispense with f_1 in the minimal Groebner basis. Similarly, since $\text{LT}(f_2) = x^2y = -(1/2)x \cdot \text{LT}(f_4)$, we can also eliminate f_2. There are no further cases where the leading term of a generator divides the leading term of another generator. Hence,

$$\tilde{f}_3 = x^2, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - (1/2)x$$

is a minimal Groebner basis for I.

Unfortunately, a given ideal may have many minimal Groebner bases. For example, in the ideal I considered above, it is easy to check that

$$\hat{f}_3 = x^2 + axy, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - (1/2)x \tag{2}$$

is also a minimal Groebner basis, where $a \in k$ is any constant. Thus, we can produce infinitely many minimal Groebner bases (assuming k is infinite). Fortunately, we can single out one minimal basis that is better than the others. The definition is as follows.

Definition 5. A reduced Groebner basis *for a polynomial ideal I is a Groebner basis G for I such that:*
(i) $\text{LC}(p) = 1$ *for all* $p \in G$.
(ii) *For all* $p \in G$, *no monomial of* p *lies in* $\langle \text{LT}(G - \{p\}) \rangle$.

Note that for the Groebner bases given in (2), only the one with $a = 0$ is reduced. In general, reduced Groebner bases have the following nice property.

Proposition 6. *Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has a unique reduced Groebner basis.*

Proof. Let G be a minimal Groebner basis for I. We say that $g \in G$ is *reduced for G* provided that no monomial of g is in $\langle \text{LT}(G - \{g\}) \rangle$. Our goal is to modify G until all of its elements are reduced.

A first observation is that if g is reduced for G, then g is also reduced for any other minimal Groebner basis of I that contains g and has the same set of leading terms. This follows because the definition of reduced only involves the leading terms.

Next, given $g \in G$, let $g' = \overline{g}^{G-\{g\}}$ and set $G' = (G - \{g\}) \cup \{g'\}$. We claim that G' is a minimal Groebner basis for I. To see this, first note that $\text{LT}(g') = \text{LT}(g)$, for when we divide g by $G - \{g\}$, $\text{LT}(g)$ goes to the remainder since it is not divisible by any element of $\text{LT}(G - \{g\})$. This shows that $\langle \text{LT}(G') \rangle = \langle \text{LT}(G) \rangle$. Since G' is clearly contained in I, we see that G' is a Groebner basis, and minimality follows. Finally, note that g' is reduced for G' by construction.

Now, take the elements of G and apply the above process until they are all reduced. The Groebner basis may change each time we do the process, but our earlier observation shows that once an element is reduced, it stays reduced since we never change the leading terms. Thus, we end up with a reduced Groebner basis.

Finally, to prove uniqueness, suppose that G and $\widetilde{G}$ are reduced Groebner bases for I. Then in particular, G and $\widetilde{G}$ are minimal Groebner bases, and in Exercise 7, we will show that this implies they have the same leading terms, i.e.,

$$\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G}).$$

Thus, given $g \in G$, there is $\tilde{g} \in \widetilde{G}$ such that $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. If we can show that $g = \tilde{g}$, it will follow that $G = \widetilde{G}$, and uniqueness will be proved.

To show $g = \tilde{g}$, consider $g - \tilde{g}$. This is in I, and since G is a Groebner basis, it follows that $\overline{g - \tilde{g}}^{G} = 0$. But we also know $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. Hence, these terms cancel in $g - \tilde{g}$, and the remaining terms are divisible by none of $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$ since G and $\widetilde{G}$ are reduced. This shows that $\overline{g - \tilde{g}}^{G} = g - \tilde{g}$, and then $g - \tilde{g} = 0$ follows. This completes the proof. □

Many computer algebra systems implement a version of Buchberger's algorithm for computing Groebner bases. These systems always compute a Groebner basis whose elements are constant multiples of the elements in a reduced Groebner basis. This means that they will give essentially the same answers for a given problem. Thus, answers can be easily checked from one system to the next.

Another consequence of the uniqueness in Proposition 6 is that we have an **ideal equality algorithm** for seeing when two sets of polynomials $\{f_1, \dots, f_s\}$ and $\{g_1, \dots, g_t\}$ generate the same ideal: simply fix a monomial order and compute a reduced Groebner basis for $\langle f_1, \dots, f_s \rangle$ and $\langle g_1, \dots, g_t \rangle$. Then the ideals are equal if and only if the Groebner bases are the same.

To conclude this section, we will indicate briefly some of the connections between Buchberger's algorithm and the row-reduction (Gaussian elimination) algorithm for systems of linear equations. The interesting fact here is that the row-reduction algorithm is essentially a special case of the general algorithm we have discussed. For concreteness, we will discuss the special case corresponding to the system of linear equations

$$\begin{array}{rcrcrcrcl} 3x & - & 6y & - & 2z & & & = & 0, \\ 2x & - & 4y & & & + & 4w & = & 0, \\ x & - & 2y & - & z & - & w & = & 0. \end{array}$$

If we use row operations on the coefficient matrix to put it in row echelon form (which means that the leading 1's have been identified), then we get the matrix

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{3}$$

To get a *reduced* row echelon matrix, we need to make sure that each leading 1 is the only nonzero entry in its column. This leads to the matrix

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4}$$

To translate these computations into algebra, let I be the ideal

$$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w \rangle \subset k[x, y, z, w]$$

corresponding to the original system of equations. We will use lex order with $x > y > z > w$. Then, in the exercises, you will verify that the linear forms determined by the row echelon matrix (3) give a minimal Groebner basis

$$I = \langle x - 2y - z - w, z + 3w \rangle,$$

and you will also check that the reduced row echelon matrix (4) gives the reduced Groebner basis

$$I = \langle x - 2y + 2w, z + 3w \rangle.$$

Recall from linear algebra that every matrix can be put in reduced row echelon form in a unique way. This can be viewed as a special case of the uniqueness of reduced Groebner bases.

In the exercises, you will also examine the relation between Buchberger's algorithm and the Euclidean Algorithm for finding the generator for the ideal $\langle f, g \rangle \subset k[x]$.

EXERCISES FOR §7

1. Check that $\overline{S(f_i, f_j)}^F = 0$ for all pairs $1 \leq i < j \leq 5$ in Example 1.
2. Use the algorithm given in Theorem 2 to find a Groebner basis for each of the following ideals. You may wish to use a computer algebra system to compute the S-polynomials and remainders. Use the lex, then the grlex order in each case, and then compare your results.
   a. $I = \langle x^2 y - 1, xy^2 - x \rangle$.
   b. $I = \langle x^2 + y, x^4 + 2x^2 y + y^2 + 3 \rangle$. [What does your result indicate about the variety $\mathbf{V}(I)$?]
   c. $I = \langle x - z^4, y - z^5 \rangle$.
3. Find reduced Groebner bases for the ideals in Exercise 2 with respect to the lex and the grlex orders.
4. Use the result of Exercise 7 of §4 to give an alternate proof that Buchberger's algorithm will always terminate after a finite number of steps.
5. Let G be a Groebner basis of an ideal I with the property that $\mathrm{LC}(g) = 1$ for all $g \in G$. Prove that G is a minimal Groebner basis if and only if no proper subset of G is a Groebner basis of I.
6. Recall the notion of a *minimal* basis for a monomial ideal introduced in Exercise 8 of §4. Show that a Groebner basis G of I is minimal if and only if $\mathrm{LC}(g) = 1$ for all $g \in G$ and $\mathrm{LT}(G)$ is a minimal basis of the monomial ideal $\langle \mathrm{LT}(I) \rangle$.
7. Fix a monomial order, and let G and $\widetilde{G}$ be minimal Groebner bases for the ideal I.
   a. Prove that $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$.
   b. Conclude that G and $\widetilde{G}$ have the same number of elements.
8. Develop an algorithm that produces a reduced Groebner basis (see Definition 5) for an ideal I, given as input an arbitrary Groebner basis for I. Prove that your algorithm works.
9. Consider the ideal

   $$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w \rangle \subset k[x, y, z, w]$$

   mentioned in the text. We will use lex order with $x > y > z > w$.
   a. Show that the linear polynomials determined by the row echelon matrix (3) give a minimal Groebner basis $I = \langle x - 2y - z - w, z + 3w \rangle$. Hint: Use Theorem 6 of §6.

b. Show that the linear polynomials from the reduced row echelon matrix (4) give the reduced Groebner basis $I = \langle x - 2y + 2w, z + 3w \rangle$.

10. Let $A = (a_{ij})$ be an $n \times m$ matrix with entries in k and let $f_i = a_{i1}x_1 + \cdots + a_{im}x_m$ be the linear polynomials in $k[x_1, \ldots, x_m]$ determined by the rows of A. Then we get the ideal $I = \langle f_1, \ldots, f_n \rangle$. We will use lex order with $x_1 > \cdots > x_m$. Now let $B = (b_{ij})$ be the reduced row echelon matrix determined by A and let $g_1, \ldots, g_t$ be the linear polynomials coming from the nonzero rows of B (so that $t \leq n$). We want to prove that $g_i, \ldots, g_t$ form the reduced Groebner basis of I.
    a. Show that $I = \langle g_1, \ldots, g_t \rangle$. Hint: Show that the result of applying a row operation to A gives a matrix whose rows generate the same ideal.
    b. Use Theorem 6 of §6 to show that $g_i, \ldots, g_t$ form a Groebner basis of I. Hint: If the leading 1 in the ith row of B is in the kth column, we can write $g_i = x_k + A$, where A is a linear polynomial involving none of the variables corresponding to leading 1's. If $g_j = x_l + B$ is written similarly, then you need to divide $S(g_i, g_j) = x_l A - x_k B$ by $g_1, \ldots, g_t$. Note that you will use only g_i and g_j in the division.
    c. Explain why $g_1, \ldots, g_t$ is the reduced Groebner basis.
11. Show that the result of applying the Euclidean Algorithm in $k[x]$ to any pair of polynomials f, g is a reduced Groebner basis for $\langle f, g \rangle$ (after dividing by a constant to make the leading coefficient equal to 1). Explain how the steps of the Euclidean Algorithm can be seen as special cases of the operations used in Buchberger's algorithm.
12. Fix $F = \{f_1, \ldots, f_s\}$ and let $r = \overline{f}^F$. Since dividing f by F gives r as remainder, adding r to the polynomials we divide by should reduce the remainder to zero. In other words, we should have $\overline{f}^{F \cup \{r\}} = 0$ when r comes last. Prove this as follows.
    a. When you divide f by $F \cup \{r\}$, consider the first place in the division algorithm where the intermediate dividend p is not divisible by any $\mathrm{LT}(f_i)$. Explain why $\mathrm{LT}(p) = \mathrm{LT}(r)$ and why the next intermediate dividend is $p - r$.
    b. From here on in the division algorithm, explain why the leading term of the intermediate dividend is always divisible by one of the $\mathrm{LT}(f_i)$. Hint: If this were false, consider the first time it fails. Remember that the terms of r are not divisible by any $\mathrm{LT}(f_i)$.
    c. Conclude that the remainder is zero, as desired.
    d. (For readers who did Exercise 11 of §3.) Give an alternate proof of $\overline{f}^{F \cup \{r\}} = 0$ using Exercise 11 of §3.
13. In the discussion following the proof of Theorem 2, we commented that if $\overline{S(f,g)}^{G'} = 0$, then remainder stays zero when we enlarge G'. More generally, if $\overline{f}^F = 0$ and F' is obtained from F by adding elements at the end, then $\overline{f}^{F'} = 0$. Prove this.

§8 First Applications of Groebner Bases

In §1, we posed four problems concerning ideals and varieties. The first was the ideal description problem, which was solved by the Hilbert Basis Theorem in §5. Let us now consider the three remaining problems and see to what extent we can solve them using Groebner bases.

The Ideal Membership Problem

If we combine Groebner bases with the division algorithm, we get the following **ideal membership algorithm**: given an ideal $I = \langle f_1, \ldots, f_s \rangle$, we can decide whether a

given polynomial f lies in I as follows. First, using an algorithm similar to Theorem 2 of §7, find a Groebner basis $G = \{g_1, \dots, g_t\}$ for I. Then Corollary 2 of §6 implies that

$$f \in I \text{ if and only if } \overline{f}^G = 0.$$

Example 1. Let $I = \langle f_1, f_2\rangle = \langle xz - y^2, x^3 - z^2\rangle \in \mathbb{C}[x, y, z]$, and use the grlex order. Let $f = -4x^2y^2z^2 + y^6 + 3z^5$. We want to know if $f \in I$.

The generating set given is not a Groebner basis of I because $\mathrm{LT}(I)$ also contains polynomials such as $\mathrm{LT}(S(f_1, f_2)) = \mathrm{LT}(-x^2y^2 + z^3) = -x^2y^2$ that are not in the ideal $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2)\rangle = \langle xz, x^3\rangle$. Hence, we begin by computing a Groebner basis for I. Using a computer algebra system, we find a Groebner basis

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

Note that this is a reduced Groebner basis.

We may now test polynomials for membership in I. For example, dividing f above by G, we find

$$f = (-4xy^2z - 4y^4) \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + (-3) \cdot f_5 + 0\cdot$$

Since the remainder is zero, we have $f \in I$.

For another example, consider $f = xy - 5z^2 + x$. Even without completely computing the remainder on division by G, we can see from the form of the elements in G that $f \notin I$. The reason is that $\mathrm{LT}(f) = xy$ is clearly not in the ideal $\langle \mathrm{LT}(G)\rangle = \langle xz, x^3, x^2y^2, xy^4, y^6\rangle$. Hence, $\overline{f}^G \neq 0$, so that $f \notin I$.

This last observation illustrates the way the properties of an ideal are revealed by the form of the elements of a Groebner basis.

The Problem of Solving Polynomial Equations

Next, we will investigate how the Groebner basis technique can be applied to solve systems of polynomial equations in several variables. Let us begin by looking at some specific examples.

Example 2. Consider the equations

$$\begin{aligned} x^2 + y^2 + z^2 &= 1, \\ x^2 + z^2 &= y, \\ x &= z \end{aligned} \tag{1}$$

in $\mathbb{C}^3$. These equations determine $I = \langle x^2+y^2+z^2-1, x^2+z^2-y, x-z\rangle \subset \mathbb{C}[x, y, z]$, and we want to find all points in $\mathbf{V}(I)$. Proposition 9 of §5 implies that we can compute $\mathbf{V}(I)$ using *any* basis of I. So let us see what happens when we use a Groebner basis.

Though we have no compelling reason as of yet to do so, we will compute a Groebner basis on I with respect to the lex order. The basis is

$$\begin{aligned} g_1 &= x - z, \\ g_2 &= -y + 2z^2, \\ g_3 &= z^4 + (1/2)z^2 - 1/4. \end{aligned}$$

If we examine these polynomials closely, we find something remarkable. First, the polynomial g_3 depends on z alone, and its roots can be found by first using the quadratic formula to solve for z^2, then, taking square roots,

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5} - 1}.$$

This gives us four values of z. Next, when these values of z are substituted into the equations $g_2 = 0$ and $g_1 = 0$, those two equations can be solved uniquely for y and x, respectively. Thus, there are four solutions altogether of $g_1 = g_2 = g_3 = 0$, two real and two complex. Since $\mathbf{V}(I) = \mathbf{V}(g_1, g_2, g_3)$ by Proposition 9 of §5, we have found *all* solutions of the original equations (1).

Example 3. Next, we will consider the system of polynomial equations (2) from Chapter 1, §2, obtained by applying Lagrange multipliers to find the minimum and maximum values of $x^3 + 2xyz - z^2$ subject to the constraint $x^2 + y^2 + z^2 = 1$:

$$\begin{aligned} 3x^2 + 2yz - 2x\lambda &= 0, \\ 2xz - 2y\lambda &= 0, \\ 2x^2 - 2z - 2z\lambda &= 0, \\ x^2 + y^2 + z^2 - 1 &= 0. \end{aligned}$$

Again, we follow our general hunch and begin by computing a Groebner basis for the ideal in $\mathbb{R}[x, y, z, \lambda]$ generated by the left-hand sides of the four equations, using the lex order with $\lambda > x > y > z$. We find a Groebner basis:

$$\begin{aligned} &\lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2, \\ &x^2 + y^2 + z^2 - 1, \\ &xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z, \\ &xz + yz^2 - \frac{1152}{3835}z^5 + \frac{108}{295}z^3 + \frac{2556}{3835}z, \\ &y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z, \\ &y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z, \\ &yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2, \\ &z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z. \end{aligned} \tag{2}$$

At first glance, this collection of polynomials looks horrendous. (The coefficients of the elements of Groebner basis can be significantly messier than the coefficients of the original generating set.) However, on further observation, we see that once again the last polynomial depends only on the variable z. We have "eliminated" the other variables in the process of finding the Groebner basis. (Miraculously) the equation obtained by setting this polynomial equal to zero has the roots

$$z = 0, \quad \pm 1, \quad \pm 2/3, \quad \pm\sqrt{11}/8\sqrt{2}.$$

If we set z equal to each of these values in turn, the remaining equations can then be solved for y, x (and λ, though its values are essentially irrelevant for our purposes). We obtain the following solutions:

$$\begin{aligned}
&z = 0; \quad y = 0; \quad x = \pm 1.\\
&z = 0; \quad y = \pm 1; \quad x = 0.\\
&z = \pm 1; \quad y = 0; \quad x = 0.\\
&z = 2/3; \quad y = 1/3; \quad x = -2/3.\\
&z = -2/3; \quad y = -1/3; \quad x = -2/3.\\
&z = \sqrt{11}/\sqrt{2}; \quad y = -3\sqrt{11}/8\sqrt{2}; \quad x = -3/8.\\
&z = -\sqrt{11}/8\sqrt{2}; \quad y = 3\sqrt{11}/8\sqrt{2}; \quad x = -3/8.
\end{aligned}$$

From here, it is easy to determine the minimum and maximum values.

Examples 2 and 3 indicate that finding a Groebner basis for an ideal with respect to the lex order simplifies the form of the equations considerably. In particular, we seem to get equations where the variables are eliminated successively. Also, note that the *order* of elimination seems to correspond to the ordering of the variables. For instance, in Example 3, we had variables $\lambda > x > y > z$, and if you look back at the Groebner basis (2), you will see that λ is eliminated first, x second, and so on.

A system of equations in this form is easy to solve, especially when the last equation contains only one variable. We can apply one-variable techniques to try and find its roots, then substitute back into the other equations in the system and solve for the other variables, using a procedure similar to the above examples. The reader should note the analogy between this procedure for solving polynomial systems and the method of "back-substitution" used to solve a linear system in triangular form.

We will study the process of elimination of variables from systems of polynomial equations intensively in Chapter 3. In particular, we will see why lex order gives a Groebner basis that successively eliminates the variables.

The Implicitization Problem

Suppose that the parametric equations

$$\begin{aligned}
x_1 &= f_1(t_1, \ldots, t_m),\\
&\vdots\\
x_n &= f_n(t_1, \ldots, t_m),
\end{aligned} \tag{3}$$

define a subset of an algebraic variety V in k^n. For instance, this will always be the case if the f_i are rational functions in $t_i, \ldots, t_m$, as we will show in Chapter 3. How can we find polynomial equations in the x_i that define V? This problem can be solved using Groebner bases, though a complete proof that this is the case will come only with the results of Chapter 3.

For simplicity, we will restrict our attention for now to cases in which the f_i are actually *polynomials.* We can study the affine variety in k^{m+n} defined by equations (3) or

$$\begin{aligned} x_1 - f_1(t_1, \ldots, t_m) &= 0, \\ &\vdots \\ x_n - f_n(t_1, \ldots, t_m) &= 0. \end{aligned}$$

The basic idea is to eliminate the variables $t_1, \ldots, t_m$ from these equations. This should give us the equations for V.

Given what we saw in Examples 2 and 3, it makes sense to use a Groebner basis to eliminate variables. We will take the lex order in $k[t_1, \ldots, t_m, x_1, \ldots, x_n]$ defined by the variable ordering

$$t_1 > \cdots > t_m > x_1 > \cdots > x_n.$$

Now suppose we have a Groebner basis of the ideal $\tilde{I} = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$. Since we are using lex order, we expect the Groebner basis to have polynomials that eliminate variables, and $t_1, \ldots, t_m$ should be eliminated first since they are biggest in our monomial order. Thus, the Groebner basis for $\tilde{I}$ should contain polynomials that only involve $x_1, \ldots, x_n$. These are our candidates for the equations of V.

The ideas just described will be explored in detail when we study elimination theory in Chapter 3. For now, we will content ourselves with some examples to see how this process works.

Example 4. Consider the parametric curve V:

$$\begin{aligned} x &= t^4, \\ y &= t^3, \\ z &= t^2 \end{aligned}$$

in $\mathbb{C}^3$. We compute a Groebner basis G of $I = \langle t^4 - x, t^3 - y, t^2 - z \rangle$ with respect to the lex order in $\mathbb{C}[t, x, y, z]$, and we find

$$G = \{-t^2 + z, ty - z^2, tz - y, x - z^2, y^2 - z^3\}.$$

The last two polynomials depend only on x, y, z, so they define an affine variety of $\mathbb{C}^3$ containing our curve V. By the intuition on dimensions that we developed in Chapter 1, we would guess that two equations in $\mathbb{C}^3$ would define a curve (a 1-dimensional variety). The remaining question to answer is whether V is the entire intersection of the two surfaces

$$x - z^2 = 0, \quad y^2 - z^3 = 0.$$

Might there be other curves (or even surfaces) in the intersection? We will be able to show that the answer is no when we have established the general results in Chapter 3.

Example 5. Now consider the tangent surface of the twisted cubic in $\mathbb{R}^3$, which we studied in Chapter 1. This surface is parametrized by

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned}$$

We compute a Groebner basis G for this ideal relative to the lex order defined by $t > u > x > y > z$, and we find that G has 6 elements altogether. If you make the calculation, you will see that only one contains only x, y, z terms:

$$-(4/3)x^3z + x^2y^2 + 2xyz - (4/3)y^3 - (1/3)z^2 = 0. \tag{4}$$

The variety defined by this equation is a surface containing the tangent surface to the twisted cubic. However, it is possible that the surface given by (4) is strictly bigger than the tangent surface: there may be solutions of (4) that do not correspond to points on the tangent surface. We will return to this example in Chapter 3.

To summarize our findings in this section, we have seen that Groebner bases and the division algorithm give a complete solution of the ideal membership problem. Furthermore, we have seen ways to produce solutions of systems of polynomial equations and to produce equations of parametrically given subsets of affine space. Our success in the examples given earlier depended on the fact that Groebner bases, when computed using lex order, seem to eliminate variables in a very nice fashion. In Chapter 3, we will prove that this is always the case, and we will explore other aspects of what is called elimination theory.

EXERCISES FOR §8

In all of the following exercises, a computer algebra system should be used to perform the necessary calculations. (Most of the calculations would be very arduous if carried out by hand.)

1. Determine whether $f = xy^3 - z^2 + y^5 - z^3$ is in the ideal $I = \langle -x^3 + y, x^2y - z \rangle$.
2. Repeat Exercise 1 for $f = x^3z - 2y^2$ and $I = \langle xz - y, xy + 2z^2, y - z \rangle$.
3. By the method of Examples 2 and 3, find the points in $\mathbb{C}^3$ on the variety
$$\mathbf{V}(x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z).$$
4. Repeat Exercise 3 for $\mathbf{V}(x^2y - z^3, 2xy - 4z - 1, z - y^2, x^3 - 4zy)$.
5. Recall from calculus that a *critical point* of a differentiable function $f(x, y)$ is a point where the partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish simultaneously. When $f \in \mathbb{R}[x, y]$, it follows that the critical points can be found by applying our techniques to the system of polynomial equations
$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

To see how this works, consider the function

$$f(x, y) = (x^2 + y^2 - 4)(x^2 + y^2 - 1) + (x - 3/2)^2 + (y - 3/2)^2.$$

a. Find all critical points of $f(x, y)$.
b. Classify your critical points as local maxima, local minima, or saddle points. Hint: Use the second derivative test.

6. Fill in the details of Example 5. In particular, compute the required Groebner basis, and verify that this gives us (up to a constant multiple) the polynomial appearing on the left-hand side of equation (4).
7. Let the surface S in $\mathbb{R}^3$ be formed by taking the *union* of the straight lines joining pairs of points on the lines

$$\begin{Bmatrix} x = t \\ y = 0 \\ z = 1 \end{Bmatrix}, \quad \begin{Bmatrix} x = 0 \\ y = 1 \\ z = t \end{Bmatrix}$$

with the *same parameter* (i.e., t) *value*. (This is a special example of a class of surfaces called *ruled surfaces*.)

a. Show that the surface S can be given in the parametric form:

$$\begin{aligned} x &= ut, \\ y &= 1 - u, \\ z &= u + t - ut. \end{aligned}$$

b. Using the method of Examples 4 and 5, find an (implicit) equation of a variety V containing the surface S.
c. Show $V = S$ (that is, show that every point of the variety V can be obtained by substituting some values for t, u in the equations of part a). Hint: Try to "solve" the implicit equation of V for one variable as a function of the other two.

8. Some parametric curves and surfaces are algebraic varieties even when the given parametrizations involve transcendental functions such as sin and cos. In this problem, we will see that that the parametric surface T,

$$\begin{aligned} x &= (2 + \cos(t))\cos(u), \\ y &= (2 + \cos(t))\sin(u), \\ z &= \sin(t), \end{aligned}$$

lies on an affine variety in $\mathbb{R}^3$.

a. Draw a picture of T. Hint: Use cylindrical coordinates.
b. Let $a = \cos(t), b = \sin(t), c = \cos(u), d = \sin(u)$, and rewrite the above equations as polynomial equations in a, b, c, d, x, y, z.
c. The pairs a, b and c, d in part b are not *independent* since there are additional polynomial identities

$$a^2 + b^2 - 1 = 0, \quad c^2 + d^2 - 1 = 0$$

stemming from the basic trigonometric identity. Form a system of five equations by adjoining the above equations to those from part b and compute a Groebner basis for the corresponding ideal. Use the lex monomial ordering and the variable order

$$a > b > c > d > x > y > z.$$

There should be exactly one polynomial in your basis that depends only on x, y, z. This is the equation of a variety containing T.

9. Consider the parametric curve $K \subset \mathbb{R}^3$ given by

$$\begin{aligned} x &= (2 + \cos(2s))\cos(3s), \\ y &= (2 + \cos(2s))\sin(3s), \\ z &= \sin(2s). \end{aligned}$$

   a. Express the equations of K as polynomial equations in $x, y, z, a = \cos(s), b = \sin(s)$. Hint: Trig identities.
   b. By computing a Groebner basis for the ideal generated by the equations from part a and $a^2 + b^2 - 1$ as in Exercise 8, show that K is (a subset of) an affine algebraic curve. Find implicit equations for a curve containing K.
   c. Show that the equation of the surface from Exercise 8 is *contained in* the ideal generated by the equations from part b. What does this result mean geometrically? (You can actually reach the same conclusion by comparing the parametrizations of T and K, without calculations.)

10. Use the method of Lagrange Multipliers to find the point(s) on the surface $x^4+y^2+z^2-1=0$ closest to the point (1, 1, 1) in $\mathbb{R}^3$. Hint: Proceed as in Example 3. (You may need to "fall back" on a *numerical* method to solve the equations you get.)
11. Suppose we have numbers a, b, c which satisfy the equations

$$\begin{aligned} a + b + c &= 3, \\ a^2 + b^2 + c^2 &= 5, \\ a^3 + b^3 + c^3 &= 7. \end{aligned}$$

   a. Prove that $a^4 + b^4 + c^4 = 9$. Hint: Regard a, b, c as variables and show carefully that $a^4 + b^4 + c^4 - 9 \in \langle a + b + c - 3, a^2 + b^2 + c^2 - 5, a^3 + b^3 + c^3 - 7\rangle$.
   b. Show that $a^5 + b^5 + c^5 \neq 11$.
   c. What are $a^5 + b^5 + c^5$ and $a^6 + b^6 + c^6$? Hint: Compute remainders.

§9 (Optional) Improvements on Buchberger's Algorithm

In designing useful mathematical software, attention must be paid not only to the *correctness* of the algorithms employed, but also to their *efficiency*. In this section, we will discuss some improvements on the basic Buchberger algorithm for computing Groebner bases that can greatly speed up the calculations. Some version of these improvements has been built into most of the computer algebra systems that offer Groebner basis packages. The section will conclude with a brief discussion of the complexity of Buchberger's algorithm. This is still an active area of research though, and there are as yet no definitive results in this direction.

The first class of modifications we will consider concern Theorem 6 of §6, which states that an ideal basis G is a Groebner basis provided that $\overline{S(f,g)}^G = 0$ for all $f, g \in G$. If you look back at §7, you will see that this criterion is the driving force behind Buchberger's algorithm. Hence, a good way to improve the efficiency of the algorithm would be to show that fewer S-polynomials $S(f, g)$ need to be considered. As you learned from doing examples by hand, the polynomial divisions involved are the

most computationally intensive part of Buchberger's algorithm. Thus, any reduction of the number of divisions that need to be performed is all to the good.

To identify S-polynomials that can be ignored in Theorem 6 of §6, we first need to give a more general view of what it means to have zero remainder. The definition is as follows.

Definition 1. *Fix a monomial order and let* $G = \{g_1, \ldots, g_t\} \subset k[x_1, \ldots, x_n]$. *Given* $f \in k[x_1, \ldots, x_n]$, *we say that* f **reduces to zero modulo** G, *written*

$$f \to_G 0,$$

if f *can be written in the form*

$$f = a_1 g_1 + \cdots + a_t g_t,$$

such that whenever $a_i g_i \neq 0$, *we have*

$$\text{multideg}(f) \geq \text{multideg}(a_i g_i).$$

To understand the relation between Definition 1 and the division algorithm, we have the following lemma.

Lemma 2. *Let* $G = \{g_1, \ldots, g_t\}$ *be an ordered set of elements of* $k[x_1, \ldots, x_n]$ *and fix* $f \in k[x_1, \ldots, x_n]$. *Then* $\overline{f}^G = 0$ *implies* $f \to_G 0$, *though the converse is false in general.*

Proof. If $\overline{f}^G = 0$, then the division algorithm implies

$$f = a_1 g_1 + \cdots + a_t g_t + 0,$$

and by Theorem 3 of §3, whenever $a_i g_i \neq 0$, we have

$$\text{multideg}(f) \geq \text{multideg}(a_i g_i).$$

This shows that $f \to_G 0$. To see that the converse may fail, consider Example 5 from §3. If we divide $f = xy^2 - x$ by $G = (xy + 1, y^2 - 1)$, the division algorithm gives

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y),$$

so that $\overline{f}^G = -x - y \neq 0$. Yet we can also write

$$xy^2 - x = 0 \cdot (xy + 1) + x \cdot (y^2 - 1),$$

and since

$$\text{multideg}(xy^2 - x) \geq \text{multideg}(x \cdot (y^2 - 1))$$

(in fact, they are equal), it follows that $f \to_G 0$. □

As an example of how Definition 1 can be used, let us state a more general version of the Groebner basis criterion from §6.

Theorem 3. *A basis $G = \{g_1, \ldots, g_t\}$ for an ideal I is a Groebner basis if and only if $S(g_i, g_j) \to_G 0$ for all $i \neq j$.*

Proof. In Theorem 6 of §6, we proved this result under the hypothesis that $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$. But if you examine the proof, you will see that all we used was

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i,$$

where

$$\text{multideg}(a_{ijk} g_i) \geq \text{multideg}(S(g_j, g_k))$$

[see (6) and (7) from §6]. This is exactly what $S(g_i, g_j) \to_G 0$ means, and the theorem follows. □

By Lemma 2, notice that Theorem 6 of §6 is a special case of Theorem 3. To exploit the freedom given by Theorem 3, we next show that certain S-polynomials are guaranteed to reduce to zero.

Proposition 4. *Given a finite set $G \subset k[x_1, \ldots, x_n]$, suppose that we have $f, g \in G$ such that*

$$\text{LCM}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f) \cdot \text{LM}(g).$$

This means that the leading monomials of f and g are relatively prime. Then $S(f, g) \to_G 0$.

Proof. For simplicity, we assume that f, g have been multiplied by appropriate constants to make $\text{LC}(f) = \text{LC}(g) = 1$. Write $f = \text{LM}(f) + p$, $g = \text{LM}(g) + q$. Then, since $\text{LCM}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f) \cdot \text{LM}(g)$, we have

$$\begin{aligned} S(f, g) &= \text{LM}(g) \cdot f - \text{LM}(f) \cdot g \\ &= (g - q) \cdot f - (f - p) \cdot g \\ &= g \cdot f - q \cdot f - f \cdot g + p \cdot g \\ &= p \cdot g - q \cdot f. \end{aligned} \tag{1}$$

We claim that

$$\text{multideg}(S(f, g)) = \max(\text{multideg}(p \cdot g), \text{multideg}(q \cdot f)). \tag{2}$$

Note that (1) and (2) imply $S(f, g) \to_G 0$ since $f, g \in G$. To prove (2), observe that in the last polynomial of (1), the leading monomials of $p \cdot g$ and $q \cdot f$ are distinct and, hence, cannot cancel. For if the leading monomials were the same, we would have

$$\text{LM}(p) \cdot \text{LM}(g) = \text{LM}(q) \cdot \text{LM}(f).$$

However this is impossible if $\text{LM}(f), \text{LM}(g)$ are relatively prime: from the last equation, $\text{LM}(g)$ would have to divide $\text{LM}(q)$, which is absurd since $\text{LM}(g) > \text{LM}(q)$. □

For an example of how this proposition works, let $G = (yz + y, x^3 + y, z^4)$ and use grlex order on $k[x, y, z]$. Then

$$S(x^3 + y, z^4) \to_G 0$$

by Proposition 4. However, using the division algorithm, it is easy to check that

$$S(x^3 + y, z^4) = yz^4 = (z^3 - z^2 + z - 1)(yz + y) + y.$$

so that

$$\overline{S(x^3 + y, z^4)}^G = y \neq 0.$$

This explains why we need Definition 1: Proposition 4 is false if we use the notion of zero remainder coming from the division algorithm.

Note that Proposition 4 gives a more efficient version of Theorem 3: to test for a Groebner basis, we need only have $S(g_i, g_j) \to_G 0$ for those $i < j$ where $\text{LM}(g_i)$ and $\text{LM}(g_j)$ are not relatively prime. But before we apply this to improving Buchberger's algorithm, let us explore a second way to improve Theorem 3.

The basic idea is to better understand the role played by S-polynomials in the proof of Theorem 6 of §6. Since S-polynomials were constructed to cancel leading terms, this means we should study cancellation in greater generality. Hence, we will introduce the notion of a *syzygy* on the leading terms of a set $F = \{f_1, \ldots, f_s\}$. This word is used in astronomy to indicate an *alignment* of three planets or other heavenly bodies. The root is a Greek word meaning "yoke." In an astronomical syzygy, planets are "yoked together"; in a mathematical syzygy, it is polynomials that are "yoked."

Definition 5. *Let $F = (f_1, \ldots, f_s)$. A* **syzygy** *on the leading terms $\text{LT}(f_1), \ldots, \text{LT}(f_s)$ of F is an s-tuple of polynomials $S = (h_1, \ldots, h_s) \in (k[x_1, \ldots, x_n])^s$ such that*

$$\sum_{i=1}^{s} h_i \cdot \text{LT}(f_i) = 0.$$

We let $S(F)$ be the subset of $(k[x_1, \ldots, x_n])^s$ consisting of all syzygies on the leading terms of F.

For an example of a syzygy, consider $F = (x, x^2 + z, y + z)$. Then using the lex order, $S = (-x + y, 1, -x) \in (k[x, y, z])^3$ defines a syzygy in $S(F)$ since

$$(-x + y) \cdot \text{LT}(x) + 1 \cdot \text{LT}(x^2 + z) + (-x) \cdot \text{LT}(y + z) = 0.$$

Let $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in (k[x_1, \ldots, x_n])^s$, where the 1 is in the ith place. Then a syzygy $S \in S(F)$ can be written as $S = \sum_{i=1}^{s} h_i \mathbf{e}_i$. For an example of how to use this notation, consider the syzygies that come from S-polynomials. Namely, given a pair $\{f_i, f_j\} \subset F$ where $i < j$, let x^γ be the least common multiple of the leading monomials of f_i and f_j. Then

$$S_{ij} = \frac{x^\gamma}{\text{LT}(f_i)}\mathbf{e}_i - \frac{x^\gamma}{\text{LT}(f_j)}\mathbf{e}_j \tag{3}$$

gives a syzygy on the leading terms of F. In fact, the name S-polynomial is actually an abbreviation for "syzygy polynomial."

It is straightforward to check that the set of syzygies is closed under coordinate-wise sums, and under coordinate-wise multiplication by polynomials (see Exercise 1). An especially nice fact about $S(F)$ is that it has a finite *basis*—there is a finite collection of syzygies such that every other syzygy is a linear combination with polynomial coefficients of the basis syzygies.

However, before we can prove this, we need to learn a bit more about the structure of $S(F)$. We first define the notion of a *homogeneous* syzygy.

Definition 6. *An element $S \in S(F)$ is* **homogeneous of multidegree** α*, where $\alpha \in \mathbb{Z}^n_{\geq 0}$, provided that*

$$S = (c_1 x^{\alpha(1)}, \ldots, c_s x^{\alpha(s)}),$$

where $c_i \in k$ and $\alpha(i) + \text{multideg}(f_i) = \alpha$ whenever $c_i \neq 0$.

You should check that the syzygy S_{ij} given in (3) is homogeneous of multidegree γ (see Exercise 4). We can decompose syzygies into homogeneous ones as follows.

Lemma 7. *Every element of S(F) can be written uniquely as a sum of homogeneous elements of S(F).*

Proof. Let $S=(h_1, \ldots, h_s) \in S(F)$. Fix an exponent $\alpha \in \mathbb{Z}^n_{\geq 0}$, and let $h_{i\alpha}$ be the term of h_i, (if any) such that $h_{i\alpha} f_i$ has multidegree α. Then we must have $\sum_{i=1}^s h_{i\alpha} \text{LT}(f_i) = 0$ since the $h_{i\alpha}\text{LT}(f_i)$ are the terms of multidegree α in the sum $\sum_{i=1}^s h_i \text{LT}(f_i) = 0$. Then $S_\alpha = (h_{1\alpha}, \ldots, h_{s\alpha})$ is a homogeneous element of $S(F)$ of degree α and $S = \sum_\alpha S_\alpha$.

The proof of uniqueness will be left to the reader (see Exercise 5). □

We can now prove that the S_{ij}'s form a basis of all syzygies on the leading terms.

Proposition 8. *Given $F = (f_1, \ldots, f_s)$, every syzygy $S \in S(F)$ can be written as*

$$S = \sum_{i<j} u_{ij} S_{ij},$$

where $u_{ij} \in k[x_1, \ldots, x_n]$ and the syzygy S_{ij} is defined as in (3)*.*

Proof. By Lemma 7, we can assume that S is homogeneous of multidegree α. Then S must have at least two nonzero components, say $c_i x^{\alpha(i)}$ and $c_j x^{\alpha(j)}$, where $i < j$. Then $\alpha(i) + \text{multideg}(f_i) = \alpha(j) + \text{multideg}(f_j) = \alpha$, which implies that $x^\gamma = \text{LCM}(\text{LM}(f_i), \text{LM}(f_j))$ divides x^α. Since

$$S_{ij} = \frac{x^\gamma}{\text{LM}(f_i)} \mathbf{e}_i - \frac{x^\gamma}{\text{LM}(f_j)} \mathbf{e}_j,$$

an easy calculation shows that the ith component of

$$S - c_i \text{LC}(f_i) x^{\alpha-\gamma} S_{ij}$$

must be zero, and the only other component affected is the jth. It follows that from S, we have produced a homogeneous syzygy with fewer nonzero components. Since a nonzero syzygy must have at least two nonzero components, continuing in this way will eventually enable us to write S as a combination of the S_{ij}'s, and we are done. □

This proposition explains our observation in §6 that S-polynomials account for all possible cancellation of leading terms.

An interesting observation is that we do not always need *all* of the S_{ij}'s to generate the syzygies in $S(F)$. For example, let $F = (x^2y^2 + z,\ xy^2 - y,\ x^2y + yz)$ and use lex order in $k[x, y, z]$. The three syzygies corresponding to the S-polynomials are

$$\begin{aligned} S_{12} &= (1, -x, 0), \\ S_{13} &= (1, 0, -y), \\ S_{23} &= (0, x, -y), \end{aligned}$$

However, we see that $S_{23} = S_{13} - S_{12}$. Then, S_{23} is *redundant* in the sense that it can be obtained from S_{12}, S_{13} by a linear combination. (In this case, the coefficients are constants; in more general examples, we might find relations between syzygies with polynomial coefficients.) In this case, $\{S_{12}, S_{13}\}$ forms a basis for the syzygies. Later in the section, we will give a systematic method for making smaller bases of $S(F)$.

We are now ready to state a more refined version of our algorithmic criterion for Groebner bases.

Theorem 9. *A basis $G = (g_1, \ldots, g_t)$ for an ideal I is a Groebner basis if and only if for every element $S = (h_1, \ldots, h_t)$ in a homogeneous basis for the syzygies $S(G)$, we have*

$$S \cdot G = \sum_{i=1}^{t} h_i g_i \to_G 0.$$

Proof. We will use the strategy (and notation) of the proof of Theorem 6 of §6. We start with $f = \sum_{i=1}^{t} h_i g_i$, where $m(i) = \text{multideg}(h_i g_i)$ and $\delta = \max(m(i))$ is minimal among all ways of writing f in terms of $g_1, \ldots, g_t$. As before, we need to show that $\text{multideg}(f) < \delta$ leads to a contradiction.

From (4) in §6, we know that $\text{multideg}(f) < \delta$ implies that $\sum_{m(i)=\delta} \text{LT}(h_i)g_i$ has strictly smaller multidegree. This therefore means that $\sum_{m(i)=\delta} \text{LT}(h_i)\text{LT}(g_i) = 0$, so that

$$S = \sum_{m(i)=\delta} \text{LT}(h_i)\mathbf{e}_i$$

is a syzygy in $S(G)$. Note also that S is homogeneous of degree δ. Our hypothesis then gives us a homogeneous basis $S_1, \ldots, S_m$ of $S(G)$ with the property that $S_j \cdot G \to_G 0$ for all j. We can write S in the form

$$S = u_1 S_1 + \cdots + u_m S_m. \tag{4}$$

By writing the u_j's as sums of terms and expanding, we see that (4) expresses S as a sum of homogeneous syzygies. Since S is homogeneous of multidegree δ, it follows from the uniqueness of Lemma 7 that we can discard all syzygies not of multidegree δ. Thus, in (4), we can assume that, for each j, either

$$u_j = 0 \quad \text{or} \quad u_j S_j \text{ is homogeneous of multidegree } \delta.$$

Suppose that S_j has multidegree γ_j. If $u_j \neq 0$, then it follows that u_j can be written in the form $u_j = c_j x^{\delta-\gamma_j}$ for some $c_j \in k$. Thus, (4) can be written

$$S = \sum_j c_j x^{\delta-\gamma_j} S_j,$$

where the sum is over those j's with $u_j \neq 0$. If we take the dot product of each side with G, we obtain

$$\sum_{m(i)=\delta} \text{LT}(h_i) g_i = S \cdot G = \sum_i c_j x^{\delta-\gamma_j} S_j \cdot G. \tag{5}$$

By hypothesis, $S_j \cdot G \to_G 0$, which means that

$$S_j \cdot G = \sum_{i=1}^{t} a_{ij} g_i, \tag{6}$$

where

$$\text{multideg}(a_{ij} g_i) \leq \text{multideg}(S_j \cdot G) \tag{7}$$

for all i, j. Note that (5), (6), and (7) are similar to the corresponding (5), (6), and (7) from §6. In fact, the remainder of the proof of the theorem is identical to what we did in §6. The only detail you will need to check is that $x^{\delta-\gamma_j} S_j \cdot G$ has multidegree $< \delta$ (see Exercise 6). The theorem is now proved. □

Note that Theorem 6 of §6 is a special case of this result. Namely, if we use the basis $\{S_{ij}\}$ for the syzygies $S(G)$, then the polynomials $S_{ij} \cdot G$ to be tested are precisely the S-polynomials $S(g_i, g_j)$.

To exploit the power of Theorem 9, we need to learn how to make smaller bases of $S(G)$. We will show next that starting with the basis $\{S_{ij} : i < j\}$, there is a systematic way to predict when elements can be omitted.

Proposition 10. *Given $G = (g_1, \ldots, g_t)$, suppose that $\mathcal{S} \subset \{S_{ij} : 1 \leq i < j \leq t\}$ is a basis of $S(G)$. In addition, suppose we have distinct elements $g_i, g_j, g_k \in G$ such that*

$$\text{LT}(g_k) \textit{ divides } \text{LCM}(\text{LT}(g_i), \text{LT}(g_j)).$$

If $S_{ik}, S_{jk} \in \mathcal{S}$, then $\mathcal{S} - \{S_{ij}\}$ is also a basis of $S(G)$. (Note: If $i > j$, we set $S_{ij} = S_{ji}$.)

Proof. For simplicity, we will assume that $i < j < k$. Set $x^{\gamma_{ij}} = \text{LCM}(\text{LM}(g_i), \text{LM}(g_j))$ and let $x^{\gamma_{ik}}$ and $x^{\gamma_{jk}}$ be defined similarly. Then our hypothesis implies that $x^{\gamma_{ik}}$ and $x^{\gamma_{jk}}$

both divide $x^{\gamma_{ij}}$. We leave it as an exercise to verify that

$$S_{ij} = \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}} S_{ik} - \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}} S_{jk},$$

and the proposition is proved. □

To incorporate this proposition into an algorithm for creating Groebner bases, we will use the ordered pairs (i, j) with $i < j$ to keep track of which syzygies we want. Since we sometimes will have an $i \neq j$ where we do not know which is larger, we will use the following notation: given $i \neq j$, define

$$[i, j] = \begin{cases} (i, j) & \text{if } i < j \\ (j, i) & \text{if } i > j. \end{cases}$$

We can now state an improved version of Buchberger's algorithm that takes into account the results proved so far.

Theorem 11. *Let $I = \langle f_1, \ldots, f_s \rangle$ be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm:*

Input : $F = (f_1, \ldots, f_s)$
Output : G, a Groebner basis for $I = \langle f_1, \ldots, f_s \rangle$

{*initialization*}
$B := \{(i, j) : 1 \leq i < j \leq s\}$
$G := F$
$t := s$
{*iteration*}
WHILE $B \neq \emptyset$ DO
Select $(i, j) \in B$
IF $\text{LCM}(\text{LT}(f_i), \text{LT}(f_j)) \neq \text{LT}(f_i)\text{LT}(f_j)$ AND
Criterion (f_i, f_j, B) is false THEN
$S := \overline{S(f_i, f_j)}^G$
IF $S \neq 0$ THEN
$t := t + 1$; $f_t := S$
$G := G \cup \{f_t\}$
$B := B \cup \{(i, t) : 1 \leq i \leq t - 1\}$
$B := B - \{(i, j)\}$,

where Criterion(f_i, f_j, B) *is true provided that there is some $k \notin \{i, j\}$ for which the pairs $[i, k]$ and $[j, k]$ are* **not** *in B and* $\text{LT}(f_k)$ *divides* $\text{LCM}(\text{LT}(f_i), \text{LT}(f_j))$. *(Note that this criterion is based on Proposition 10.)*

Proof. The basic idea of the algorithm is that B records the pairs (i, j) that remain to be considered. Furthermore, we only compute the remainder of those S-polynomials $S(g_i, g_j)$ for which neither Proposition 4 nor Proposition 10 apply.

To prove that the algorithm works, we first observe that at every stage of the algorithm, B has the property that if $1 \le i < j \le t$ and $(i, j) \notin B$, then

$$S(f_i, f_j) \to_G 0 \quad \text{or} \quad \text{Criterion}(f_i, f_j, B) \text{ holds.} \tag{8}$$

Initially, this is true since B starts off as the set of all possible pairs. We must show that if (8) holds for some intermediate value of B, then it continues to hold when B changes, say to B'.

To prove this, assume that $(i, j) \notin B'$. If $(i, j) \in B$, then an examination of the algorithm shows that $B' = B - \{(i, j)\}$. Now look at the step before we remove (i, j) from B. If $\text{LCM}(\text{LT}(f_i)), \text{LT}(f_j)) = \text{LT}(f_i)\text{LT}(f_j)$, then $S(f_i, f_j) \to_G 0$ by Proposition 4, and (8) holds. Also if Criterion (f_i, f_j, B) is true, then (8) clearly holds. Now suppose that both of these fail. In this case, the algorithm computes the remainder $S = \overline{S(f_i, f_j)}^G$. If $S = 0$, then $S(f_i, f_j) \to_G 0$ by Lemma 2, as desired. Finally, if $S \neq 0$, then we enlarge G to be $G' = G \cup \{S\}$, and we leave it as an exercise to show that $S(f_i, f_j) \to_{G'} 0$.

It remains to study the case when $(i, j) \notin B$. Here, (8) holds for B, and we leave it as an exercise to show that this implies that (8) also holds for B'.

Next, we need to show that G is a Groebner basis when $B = \emptyset$. To prove this, let t be the length of G, and consider the set $\mathcal{I}$ consisting of all pairs (i, j) for $1 \le i < j \le t$ where Criterion(f_i, f_j, B) was *false* when (i, j) was selected in the algorithm. We claim that $\mathcal{S} = \{S_{ij} : (i, j) \in \mathcal{I}\}$ is a basis of $S(G)$ with the property that $S_{ij} \cdot G = S(f_i, f_j) \to_G 0$ for all $S_{ij} \in \mathcal{S}$. This claim and Theorem 9 will prove that G is a Groebner basis.

To prove our claim, note that $B = \emptyset$ implies that (8) holds for *all* pairs (i, j) for $1 \le i < j \le t$. It follows that $S(f_i, f_j) \to_G 0$ for all $(i, j) \in \mathcal{I}$. It remains to show that S is a basis of $S(G)$. To prove this, first notice that we can *order* the pairs (i, j) according to when they were removed from B in the algorithm (see Exercise 10 for the details of this ordering). Now go through the pairs in reverse order, starting with the last removed, and delete the pairs (i, j) for which Criterion(f_i, f_j, B) was true at that point in the algorithm. After going through all pairs, those that remain are precisely the elements of $\mathcal{I}$. Let us show that at every stage of this process, the syzygies corresponding to the pairs (i, j) not yet deleted form a basis of $S(G)$. This is true initially because we started with all of the S_{ij}'s, which we know to be a basis. Further, if at some point we delete (i, j), then the definition of Criterion(f_i, f_j, B) implies that there is some k where $\text{LT}(f_k)$ satisfies the LCM condition and $[i, k], [j, k] \notin B$. Thus, $[i, k]$ and $[j, k]$ were removed earlier from B, and hence S_{ik} and S_{ik} are still in the set we are creating because we are going in reverse order. If follows from Proposition 10 that we still have a basis even after deleting S_{ij}.

Finally, we need to show that the algorithm terminates. As in the proof of the original algorithm (Theorem 2 of §7), G is always a basis of our ideal, and each time we enlarge G, the monomial ideal $\langle \text{LT}(G) \rangle$ gets strictly larger. By the ACC, it follows that at some point, G must stop growing, and thus, we eventually stop adding elements to B. Since every pass through the WHILE ... DO loop removes an element of B, we must eventually get $B = \emptyset$, and the algorithm comes to an end. □

The algorithm given above is still not optimal, and several strategies have been found to improve its efficiency further. For example, our discussion of the division algorithm in $k[x_1, \ldots, x_n]$ (Theorem 3 of §3), we allowed the divisors $f_1, \ldots, f_s$ to be listed in any order. In practice, some effort could be saved on average if we arranged the f_i so that their leading terms are listed in increasing order with respect to the chosen monomial ordering. Since the smaller $\text{LT}(f_i)$ are more likely to be used during the division algorithm, listing them earlier means that fewer comparisons will be required. A second strategy concerns the step where we choose $(i, j) \in B$ in the algorithm of Theorem 11. BUCHBERGER (1985) suggests that there will often be some savings if we pick $(i, j) \in B$ such that $\text{LCM}(\text{LM}(f_i), \text{LM}(f_j))$ is as *small* as possible. The corresponding S-polynomials will tend to yield any nonzero remainders (and new elements of the Groebner basis) sooner in the process, so there will be more of a chance that subsequent remainders $\overline{S(f_i, f_j)}^{G}$ will be zero. This *normal selection strategy* is discussed in more detail in BECKER and WEISPFENNING (1993), BUCHBERGER (1985) and GEBAUER and MÖLLER (1988). Finally, there is the idea of *sugar*, which is a refinement of the normal selection strategy. Sugar and its variant *double sugar* can be found in GIOVINI, MORA, NIESI, ROBBIANO and TRAVERSO (1991).

In another direction, one can also modify the algorithm so that it will automatically produce a reduced Groebner basis (as defined in §7). The basic idea is to systematically reduce G each time it is enlarged. Incorporating this idea also generally lessens the number of S-polynomials that must be divided in the course of the algorithm. For a further discussion of this idea, consult BUCHBERGER (1985).

We will end this section with a short discussion of the complexity of Buchberger's algorithm. Even with the best currently known versions of the algorithm, it is still easy to generate examples of ideals for which the computation of a Groebner basis takes a tremendously long time and/or consumes a huge amount of storage space. There are several reasons for this:

- The total degrees of intermediate polynomials that must be generated as the algorithm proceeds can be quite large.
- The coefficients of the elements of a Groebner basis can be quite complicated rational numbers, even when the coefficients of the original ideal generators were small integers. See Example 3 of §8 or Exercise 13 of this section for some instances of this phenomenon.

For these reasons, a large amount of theoretical work has been done to try to establish uniform upper bounds on the degrees of the intermediate polynomials in Groebner basis calculations when the degrees of the original generators are given. For some specific results in this area, see DUBÉ (1990) and MÖLLER and MORA (1984). The idea is to measure to what extent the Groebner basis method will continue to be tractable as larger and larger problems are attacked.

The bounds on the degrees of the generators in a Groebner basis are quite large, and it has been shown that large bounds are necessary. For instance, MAYR and MEYER (1982) give examples where the construction of a Groebner basis for an ideal generated by polynomials of degree less than or equal to some d can involve polynomials of degree proportional to 2^{2^d}. As $d \to \infty$, 2^{2^d} grows *very* rapidly. Even when grevlex order is

used (which often gives the smallest Groebner bases—see below), the degrees can be quite large. For example, consider the polynomials

$$x^{n+1} - yz^{n-1}w, \quad xy^{n-1} - z^n, \quad x^n z - y^n w.$$

If we use grevlex order with $x > y > z > w$, then Mora [see LAZARD (1983)] showed that the reduced Groebner basis contains the polynomial

$$z^{n^2+1} - y^{n^2} w.$$

The results led for a time to some pessimism concerning the ultimate practicality of the Groebner basis method as a whole. Further work has shown, however, that for ideals in two and three variables, much more reasonable upper degree bounds are available [see, for example, LAZARD (1983) and WINKLER (1984)]. Furthermore, in any case the running time and storage space required by the algorithm seem to be much more manageable "on average" (and this tends to include most cases of geometric interest) than in the worst cases. There is also a growing realization that computing "algebraic" information (such as the primary decomposition of an ideal—see Chapter 4) should have greater complexity than computing "geometric" information (such as the dimension of a variety—see Chapter 9). A good reference for this is GIUSTI and HEINTZ (1993), and a discussion of a wide variety of complexity issues related to Groebner bases can be found in BAYER and MUMFORD (1993).

Finally, experimentation with changes of variables and varying the ordering of the variables often can reduce the difficulty of the computation drastically. BAYER and STILLMAN (1987a) have shown that in most cases, the grevlex order should produce a Groebner basis with polynomials of the smallest total degree. In a different direction, some versions of the algorithm will change the term ordering as the algorithm progresses in order to produce a more efficient Groebner basis. This is discussed by GRITZMANN and STURMFELS (1993).

For more recent developments concerning Bucherger's algorithm, we refer readers to the special issue of the Journal of Symbolic Computation devoted to efficient computation of Groebner bases, scheduled to appear in 2007.

EXERCISES FOR §9

1. Let $S = (c_1, \ldots, c_s)$ and $T = (d_1, \ldots, d_s) \in (k[x_1, \ldots, x_n])^s$ be syzygies on the leading terms of $F = (f_1, \ldots, f_s)$.
   a. Show that $S + T = (c_1 + d_1, \ldots, c_s + d_s)$ is also a syzygy.
   b. Show that if $g \in k[x_1, \ldots, x_n]$, then $g \cdot S = (gc_1, \ldots, gc_s)$ is also a syzygy.
2. Given any $G = (g_1, \ldots, g_s) \in (k[x_1, \ldots, x_n])^s$, we can define a syzygy on G to be an s-tuple $S = (h_1, \ldots, h_s) \in (k[x_1, \ldots, x_n])^s$ such that $\sum_i h_i g_i = 0$. [Note that the syzygies we studied in the text are syzygies on $\mathrm{LT}(G) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$.]
   a. Show that if $G = (x^2 - y, xy - z, y^2 - xz)$, then $(z, -y, x)$ defines a syzygy on G.
   b. Find another syzygy on G from partial
   c. Show that if S, T are syzygies on G, and $g \in k[x_1, \ldots, x_n]$, then $S + T$ and gS are also syzygies on G.

3. Let M be an $m \times (m+1)$ matrix of polynomials in $k[x_1, \ldots, x_n]$. Let I be the ideal generated by the determinants of all the $m \times m$ submatrices of M (such ideals are examples of *determinantal* ideals).
   a. Find a 2×3 matrix M such that the associated determinantal ideal of 2×2 submatrices is the ideal with generators G as in Exercise 2.
   b. Explain the syzygy given in part a of Exercise 2 in terms of your matrix.
   c. Give a general way to produce syzygies on the generators of a determinantal ideal. Hint: Find ways to produce $(m+1) \times (m+1)$ matrices containing M, whose determinants are automatically zero.
4. Prove that the syzygy S_{ij} defined in (3) is homogeneous of multidegree γ.
5. Complete the proof of Lemma 7 by showing that the decomposition into homogeneous components is unique. Hint: First show that if $S = \sum_\alpha S'_\alpha$, where S'_α has multidegree α, then, for a fixed i, the ith components of the S'_α are either 0 or have multidegree $\alpha - \text{multideg}(f_i)$ and, hence, give distinct terms as α varies.
6. Suppose that S_j is a homogeneous syzygy of multidegree γ_j in $S(G)$. Then show that $S_j \cdot G$ has multidegree $< \gamma_j$. This implies that $x^{\delta-\gamma_i} S_j \cdot G$ has multidegree $< \delta$, which is a fact we need for the proof of Theorem 9.
7. Complete the proof of Proposition 10 by proving the formula expressing S_{ij} in terms of S_{ik} and S_{jk}.
8. Let G be a finite subset of $k[x_1, \ldots, x_n]$ and let $f \in \langle G \rangle$. If $\overline{f}^G = r \neq 0$, then show that $F \to_{G'} 0$, where $G' = G \cup \{r\}$. This fact is used in the proof of Theorem 11.
9. In the proof of Theorem 11, we claimed that for every value of B, if $1 \leq i < j \leq t$ and $(i, j) \notin B$, then condition (8) was true. To prove this, we needed to show that if the claim held for B, then it held when B changed to some B'. The case when $(i, j) \notin B'$ but $(i, j) \in B$ was covered in the text. It remains to consider when $(i, j) \notin B' \cup B$. In this case, prove that (8) holds for B'. Hint: Note that (8) holds for B. There are two cases to consider, depending on whether B' is bigger or smaller than B. In the latter situation, $B' = B - \{(k, l)\}$ for some $(k, l) \neq (i, j)$.
10. In this exercise, we will study the ordering on the set $\{(i, j) : 1 \leq i < j \leq t\}$ described in the proof of Theorem 11. Assume that $B = \emptyset$, and recall that t is the length of G when the algorithm stops.
    a. Show that any pair (i, j) with $1 \leq i < j \leq t$ was a member of B at some point during the algorithm.
    b. Use part (a) and $B = \emptyset$ to explain how we can order the set of *all* pairs according to when a pair was removed from B.
11. Consider $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$ and use grlex order on $k[x, y]$. These polynomials are taken from Example 1 of §7, where we followed Buchberger's algorithm to show how a Groebner basis was produced. Redo this example using the algorithm of Theorem 11 and, in particular, keep track of how many times you have to use the division algorithm.
12. Consider the polynomials

$$x^{n+1} - yz^{n-1}w, \quad xy^{n-1} - z^n, \quad x^n z - y^n w,$$

and use grevlex order with $x > y > z > w$. Mora [see LAZARD (1983)] showed that the reduced Groebner basis contains the polynomial

$$z^{n^2+1} - y^{n^2} w.$$

Prove that this is true when n is 3, 4, or 5. How big are the Groebner bases?

13. In this exercise, we will look at some examples of how the term order can affect the length of a Groebner basis computation and the complexity of the answer.
    a. Compute a Groebner basis for $I = \langle x^5 + y^4 + z^3 - 1, x^3 + y^2 + z^2 - 1\rangle$ using lex and grevlex orders with $x > y > z$. You may not notice any difference in the computation time, but you will see that the Groebner basis is much simpler when using grevlex.
    b. Compute a Groebner basis for $I = \langle x^5 + y^4 + z^3 - 1, x^3 + y^3 + z^2 - 1\rangle$ using lex and grevlex orders with $x > y > z$. This differs from the previous example by a single exponent, but the Groebner basis for lex order is significantly nastier (one of its polynomials has 282 terms, total degree 25, and a largest coefficient of 170255391). Depending on the computer and how the algorithm was implemented, the computation for lex order may take dramatically longer.
    c. Let $I = \langle x^4 - yz^2w, xy^2 - z^3, x^3z - y^3w\rangle$ be the ideal generated by the polynomials of Exercise 12 with $n = 3$. Using lex and grevlex orders with $x > y > z > w$, show that the resulting Groebner bases are the same. So grevlex is not always better than lex, but in practice, it is usually a good idea to use grevlex whenever possible.