Advanced Algebra

Final Version, September, 2007
For Publication by Birkhäuser Boston
Along with a Companion Volume *Basic Algebra*
In the Series

Cornerstones

Selected Pages from Chapter VIII: pp. 447–450, 491–510

Anthony W. Knapp

CHAPTER VIII

Background for Algebraic Geometry

Abstract. This chapter introduces aspects of the algebraic theory of systems of polynomial equations in several variables.

Section 1 gives a brief history of the subject, treating it as one of two early sources of questions to be addressed in algebraic geometry.

Section 2 introduces the resultant as a tool for eliminating one of the variables in a system of two such equations. A first form of Bezout's Theorem is an application, saying that if $f(X, Y)$ and $g(X, Y)$ are polynomials of respective degrees m and n whose locus of common zeros has more than mn points, then f and g have a nontrivial common factor. This version of the theorem may be regarded as pertaining to a pair of affine plane curves.

Section 3 passes to projective plane curves, which are nonconstant homogeneous polynomials in three variables, two such being regarded as the same if they are multiples of one another. Versions of the resultant and Bezout's Theorem are valid in this context, and two projective plane curves defined over an algebraically closed field always have a common zero.

Sections 4–5 introduce intersection multiplicity for projective plane curves. Section 4 treats a line and a curve, and Section 5 treats the general case of two curves. The theory in Section 4 is completely elementary, and a version of Bezout's Theorem is proved that says that a line and a curve of degree d have exactly d common zeros, provided the underlying field is algebraically closed, the zeros are counted as often as their intersection multiplicities, and the line does not divide the curve. Section 5 makes more serious use of algebraic background, particularly localizations and the Nullstellensatz. It gives an indication that ostensibly simple phenomena in the subject can require sophisticated tools to analyze.

Section 6 proves a version of Bezout's Theorem appropriate for the context of Section 5: if F and G are two projective plane curves of respective degrees m and n over an algebraically closed field, then either they have a nontrivial common factor or they have exactly mn common zeros when the intersection multiplicities of the zeros are taken into account.

Sections 7–10 concern Gröbner bases, which are finite generating sets of a special kind for ideals in a polynomial algebra over a field. Section 7 sets the stage, introducing monomial orders and defining Gröbner bases. Section 8 establishes a several-variable analog of the division algorithm for polynomials in one variable and derives from it a usable criterion for a finite set of generators to be a Gröbner basis. From this it is easy to give a constructive proof of the existence of Gröbner bases and to obtain as consequences solutions of the ideal-membership problem and the proper-ideal problem. Section 9 obtains a uniqueness theorem under the condition that the Gröbner basis be reduced. Adjusting a Gröbner basis to make it reduced is an easy matter. A consequence of the uniqueness result is a solution of the ideal-equality problem. Section 10 gives two theorems concerning solutions of systems of polynomial equations. The Elimination Theorem identifies in terms of Gröbner bases those members of the ideal that depend only on a certain subset of the variables. The Extension Theorem, proved under the additional assumption that the underlying field is algebraically closed,

gives conditions under which a solution to the subsystem of equations that depend on all but one variable can be extended to a solution of the whole system. The latter theorem makes use of the theory of resultants.

1. Historical Origins and Overview

Modern algebraic geometry grew out of early attempts to solve simultaneous polynomial equations in several variables and out of the theory of Riemann surfaces. We shall discuss the first of these sources in the present chapter and the second of the sources in Chapter IX.

Serious consideration of simultaneous polynomial equations of degree > 2 dates to a 1750 book[1] by Gabriel Cramer (1704–1752), who may be better known for Cramer's rule in connection with determinants. Cramer was interested in various aspects of the zero loci of polynomials in two variables with real coefficients. Thinking of the zero locus, we refer to a nonconstant polynomial in two variables as a plane curve.

One of the problems of interest to Cramer was to find the number of points in the plane that would uniquely determine a plane curve of degree n up to a constant multiple. Cramer gave the answer $\frac{1}{2}n(n+3)$ to this problem. For example, when $n = 2$, if we normalize matters by taking the coefficient of x^2 to be 1, then the possible quadratic polynomials

$$f(x, y) = x^2 + bxy + cy^2 + dx + ey + f$$

involve five unknown coefficients. Each condition $f(x_i, y_i) = 0$ gives a linear condition on the coefficients, and Cramer was able to write down explicitly a plane curve through the given points in question by introducing determinants and applying his rule to solve the problem.

Already with this much description the reader will see a certain subtlety—that there will be special choices of the five points for which existence or uniqueness will fail. We could also ask about the effect of multiplicities: what does it mean geometrically to take two or more of the points to be equal, and how does such an occurrence affect the number of points that can be specified?

Cramer noticed a subtlety that is less easy to resolve, even in hindsight. If we are given any two plane curves of degree 3, then Cardan's formula says that we can solve one equation for y in terms of x, obtaining three expressions in x; then we can substitute for y in the other equation each of the three expressions in x and obtain a cubic equation in x each time. In other words, we should expect up to 9 points of intersection for two cubics, and 9 should sometimes occur. (The various

[1] G. Cramer, *Introduction à l'Analyse des Lignes courbes algébriques*, Chez les Frères Cramer & Cl. Philibert, Geneva, 1750.

forms of Bezout's Theorem, which came a little later, confirm this argument.) The number of points that determine a cubic completely is $\frac{1}{2}n(n+3)$ for $n = 3$, i.e., is 9. Thus we have 9 points determining a unique cubic, and yet the second cubic goes through these 9 points as well. What is happening? This question has come to be known as **Cramer's paradox**.

Explaining this kind of mystery became an early impetus for the development of algebraic geometry.

The question of the number of points of intersection had been the subject of conjecture for some time earlier, and it was expected that two plane curves of respective total degrees m and n in some sense had mn points of intersection. Étienne Bezout (1730–1783) took up this question and dealt with parts of it rigorously. The quadratic case can be solved by finding one variable in terms of the other and by substituting, but let us handle it by the method that Bezout used. If we view each polynomial as quadratic in y and having coefficients that depend on x, then we have a system

$$\begin{aligned} a_0 + a_1 y + a_2 y^2 &= 0, \\ b_0 + b_1 y + b_2 y^2 &= 0. \end{aligned}$$

Instead of regarding this as a system of two equations for y, we regard it as a system of two homogeneous linear equations for variables x_0, x_1, x_2, where $x_0 = 1, x_1 = y, x_2 = y^2$. We can get two further equations by multiplying each equation by y:

$$\begin{aligned} a_0 y + a_1 y^2 + a_2 y^3 &= 0, \\ b_0 y + b_1 y^2 + b_2 y^3 &= 0, \end{aligned}$$

and then we have four homogeneous linear equations for $x_0 = 1, x_1 = y, x_2 = y^2, x_3 = y^3$. Since the system has the nonzero solution $(1, y, y^2, y^3)$, the determinant of the coefficient matrix must be 0. Remembering that the coefficients depend on x, we see that we have eliminated the variable y and obtained a polynomial equation for x without using any solution formula for polynomials in one variable. The device that Bezout introduced for this purpose—the determinant of the coefficient matrix—is called the **resultant** of the system and is a fundamental tool in handling simultaneous polynomial equations. With it Bezout went on in 1779 to give a rigorous proof that when two polynomials in (x, y) are set equal to 0 simultaneously, one of degree m and the other of degree n, then there cannot be more than mn solutions unless the two polynomials have a common factor. This is a first form of Bezout's Theorem and is proved in Section 2.

In order to have a chance of obtaining a full complement of mn solutions, we make three adjustments—allow complex solutions instead of just real solutions (even in the case $(m, n) = (2, 1)$), consider "projective plane curves" instead of ordinary plane curves to allow for solutions at infinity (even in the case $(m, n) =$

$(1,1)$), and introduce a suitable notion of intersection number of two plane curves at a point in order to take multiplicities into account (even in the case $(m,n) = (2,1)$). We shall allow complex solutions already in Section 2, and we shall make an adjustment for projective plane curves in Section 3. The issue of intersection multiplicity is more complicated. The beginnings of a classical approach to it are indicated in Section 4, and a somewhat more modern approach appears in Section 5. With the full theory of intersection multiplicities of projective plane curves in place, we obtain a general form of Bezout's Theorem[2] in Section 6.

The theory of the resultant can be extended in various ways, but we shall largely not pursue this matter. Studies of zero loci of systems of equations took a more geometric turn in the first part of the nineteenth century through the work of Julius Plücker (1801–1858) and others, but these matters will be left for an implicit discussion in Chapter X. Instead, we skip to a development that began with the doctoral thesis of Bruno Buchberger in 1965. Buchberger was interested in being able to decide when a polynomial is a member of an ideal that is specified by a finite list of generators. For this purpose he learned that each ideal has a special finite set of generators that is unique once certain declarations are made. He devised an algorithm for determining such a set of generators,[3] and he gave the name "Gröbner basis" to the set, in honor of his thesis advisor.[4] The special unique such basis is called a "reduced Gröbner basis."

An unfortunate feature of the algorithm (and even of later improved algorithms) is that Gröbner bases are extraordinarily complicated to calculate. The timing of Buchberger's discovery was therefore especially fortuitous, coming when computers were becoming more common, more economical, and more powerful.

Buchberger was able to give a test for membership in an ideal in terms of a multivariable division algorithm involving any Gröbner basis. Other general problems involving ideals were solvable as well. Because of the uniqueness of the reduced Gröbner basis, two ideals are identical if and only if their reduced Gröbner bases are equal. When some of the theory of resultants was incorporated into the theory of Gröbner bases, these bases could also be used to address various questions of identifying zero loci. Other problems involving ideals could be addressed by similar methods. The theory has flowered tremendously since its initial discovery and by the present day has found many imaginative applications to applied problems. Sections 7–10 give an introductory account of this important theory.

[2] A correct proof of the general form of the theorem seems to have been published for the first time by Georges-Henri Halphen (1844–1889) in 1873.

[3] Devising the algorithm was Buchberger's real contribution, since the abstract existence of the special set of generators is an easy consequence of the Hilbert Basis Theorem and had already been used in papers of H. Hironaka in 1964.

[4] Wolfgang Gröbner (1899–1980). The name is often spelled out as "Groebner," particularly when it is used in connection with computer algorithms.

Pages 451–490 do not appear in this file.

of $\big(K[X,Y,W]/(F,G)\big)_{d+r}$ for every $r \geq 0$.

To prove that (‡) spans $K[X,Y]/(f,g)$, let h be in $K[X,Y]$. Let H be a homogeneous polynomial in $K[X,Y,W]$ with $h(X,Y) = H(X,Y,1)$, and choose an integer s such that $W^s H$ lies in $K[X,Y,W]_{d+r}$ for some $r \geq 0$. Then we can write $W^s H = \sum_{j=1}^{mn} c_j W^r V_j + AF + BG$ for suitable scalars c_j and homogeneous polynomials A and B. Restricting the domain to points $(X,Y,1)$ gives $h = \sum_{j=1}^{mn} c_j v_j + af + bg$, and therefore $h + (f,g) = \sum_{j=1}^{mn} c_j v_j + (f,g)$. This proves that (‡) spans $K[X,Y]/(f,g)$.

To prove that (‡) is linearly independent, suppose that $\sum_{j=1}^{mn} c_j v_j = af + bg$ with a and b in $K[X,Y]$. If A and B are homogeneous polynomials such that $a(X,Y) = A(X,Y,1)$ and $b(X,Y) = B(X,Y,1)$, then $W^r \sum_{j=1}^{mn} c_j V_j = W^s AF + W^t BG$, provided the exponents r, s, t are chosen to make the degrees of the terms $W^r \sum_{j=1}^{mn} c_j V_j$, $W^s AF$, and $W^t BG$ match. Consequently $W^r \sum_{j=1}^{mn} c_j V_j$ lies in $(F,G)_{d+r}$, and (§) shows that the coefficients are all 0. This proves that (‡) is linearly independent. □

7. Gröbner Bases

The remainder of the chapter returns to the main question introduced in Section 1, that of how to get information about the set of simultaneous solutions of polynomial equations in several variables. The resultant introduced in Section 2 gave us one tool, but the tool is of most use when there are only two equations. Beyond two equations the number of cases to check quickly grows, and the resultant is of limited usefulness.[12]

The tool to be introduced in this section is of a completely different nature. Historically it was introduced in order to have a way of deciding whether an ideal in $K[X_1, \ldots, X_n]$ contains a given polynomial. We know from the Hilbert Basis Theorem that every such ideal is finitely generated, and it is assumed that the ideal to be tested is specified by such a set of generators.

The proof of the Hilbert Basis Theorem gives a clue how to start studying an ideal of polynomials. In the statement of the theorem, R is a Noetherian integral domain, and I is a nonzero ideal in $R[X]$. It is to be proved that I is finitely generated. The proof by Hilbert is longer than the proof given in *Basic Algebra*, but the idea is clearer. To each nonzero member $f(X)$ of I, we associate the coefficient of the highest power of X appearing in $f(X)$. These coefficients, together with 0, form an ideal $L(I)$ in R, and $L(I)$ is finitely generated because R is Noetherian. Let $a_1, \ldots, a_r$ be generators, let $f_1(X), \ldots, f_r(X)$ be members

[12] The nature of the extended theory can be found in Van der Waerden, Volume II, Chapter XI. Theorem 8.31 below in effect reproduces some of this extended theory in a context that is manageable because of the theory of Gröbner bases.

of I with respective highest coefficients $a_1, \dots, a_r$, and let q be the largest of the degrees of $f_1(X), \dots, f_r(X)$. If a general $g(X)$ in I is given and if $a \in R$ is its highest coefficient, then we know that $a = \sum_i c_i a_i$ with $c_i \in R$. The polynomial $h(X)$ given by $h(X) = g(X) - \sum_i c_i f_i(X) X^{\deg g - \deg f_i}$ has degree lower than $\deg g$, and $g(X)$ will be in $(f_1, \dots, f_r)$ if $h(X)$ is in $(f_1, \dots, f_r)$. Iterating this construction, we see that it is enough to account for all the members of I of degree $\le q - 1$. To handle these, one way to proceed is to enlarge the set $\{f_1, \dots, f_r\}$ a little. For each k with $0 \le k \le q - 1$, let $L_k(I)$ be the union of $\{0\}$ and the set of coefficients of X^k in members of I of degree k. Each of these is an ideal of R and hence is finitely generated, and we adjoin to $\{f_1, \dots, f_r\}$ a finite set of generators for each $L_k(I)$ with $0 \le k \le q - 1$. The result is a finite set $\{g_1, \dots, g_s\}$ of generators of I, as one easily checks.

In fact, the set $\{g_1, \dots, g_s\}$ is a special set of generators. For any member f of $R[X]$, let $\mathrm{LT}(f)$ be the complete term of $f(X)$ containing the highest power of X. What the argument shows is that $\{g_1, \dots, g_s\}$ is a subset of I such that $\mathrm{LT}(I) = \big(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\big)$, where $\mathrm{LT}(I)$ denotes the ideal given as the linear span of all polynomials $\mathrm{LT}(g)$ for g in I. One can show that this property of $\{g_1, \dots, g_s\}$ implies that $\{g_1, \dots, g_s\}$ generates I. In essence this property will be the defining property of a "Gröbner basis" of I. It is not automatically satisfied for just any finite generating set $\{f_1, \dots, f_r\}$, as the example below shows. We shall see that it is easy to use such a set of generators to test any polynomial in $R[X]$ for membership in I. Thus the original problem historically for introducing such sets is solved except for one little detail: the proof of the Hilbert Basis Theorem is not constructive, and we are left with no idea how actually to construct a Gröbner basis.[13]

EXAMPLE. Treat $K[X, Y]$ as an instance of the above setting by letting $R = K[Y]$ and regarding $K[X, Y]$ as $R[X]$. Consider the ideal $I = (f_1, f_2)$ in $R[X]$ with $f_1(X, Y) = X^2 + 2XY^2$ and $f_2(X, Y) = XY + 2Y^3 - 1$. Then $\big(\mathrm{LT}(f_1), \mathrm{LT}(f_2)\big) = (X^2, XY)$, and every monomial appearing with nonzero coefficient in a member of the latter ideal has total degree at least 2. On the other hand, I contains the polynomial

$$Yf_1(X, Y) - Xf_2(X, Y) = Y(X^2 + 2XY) - X(XY + 2Y^3 - 1) = X,$$

and its leading term is X, whose total degree is 1. Thus $\mathrm{LT}(I)$ properly contains $\big(\mathrm{LT}(f_1), \mathrm{LT}(f_2)\big)$.

Because of the nonconstructive nature of the proof of the Hilbert Basis Theorem, it is necessary to start afresh. One message to glean from the abstract proof

[13] The exposition in this section and the next three is based partly on the book of Cox–Little–O'Shea and the Web tutorial of Fabrizio listed in the Selected References.

is that the leading terms of the members of I are important and somewhat control the nature of I. To handle $K[X_1, \dots, X_n]$ when K is a field, it is of course necessary to use an additional induction that enumerates the variables. In the example above, we treated X as more significant than Y. For the inductive step for general $K[X_1, \dots, X_n]$, the ring R in the above argument is K with some number m of the indeterminates included, and X is the $(m+1)^{\text{st}}$ indeterminate. Putting all the steps of the induction together, we see that the order in which the variables are processed appears to be important.

The theory of Gröbner bases as it has evolved allows a healthy extra measure of generality. Instead of defining leading terms by insisting on an ordering of the indeterminates, it defines them by using a suitable kind of ordering of monomials, and that is where we begin. Let $K[X_1, \dots, X_n]$ be given, K being a field. Let $\mathcal{M}$ be the set of all monomials in $K[X_1, \dots, X_n]$. A **monomial ordering** $\leq$ on $\mathcal{M}$ is a total ordering[14] with the two additional properties that

(i) $M_1 \leq M_2$ implies $M_1M_3 \leq M_2M_3$ for all M_1, M_2, M_3 in $\mathcal{M}$,
(ii) $1 \leq M$ for all M in $\mathcal{M}$.

We write $M_2 \geq M_1$ to mean $M_1 \leq M_2$. Also, $M_1 < M_2$ means $M_1 \leq M_2$ with $M_1 \neq M_2$, and $M_1 > M_2$ means $M_1 \geq M_2$ with $M_1 \neq M_2$.

EXAMPLES OF MONOMIAL ORDERINGS. Each ordering assumes that the variables are enumerated in some way. In these examples we take this enumeration to be $X_1, \dots, X_n$. The first four examples all have the property that the largest X_j is X_1 and the smallest is X_n.

(1) **Lexicographic ordering**, abbreviated as "lex" by many authors and written as $\leq_{\text{LEX}}$ in this list of examples. This, the most important monomial ordering, is already suggested by the proof of the Hilbert Basis Theorem. In principle it can be used for all purposes in Sections 7–10, but one application in Chapter X will require a different monomial ordering. Its disadvantage is that it sometimes makes lengthy computations take longer than necessary; this matter will be discussed more in Section 9. The definition is that $X_1^{i_1} \cdots X_n^{i_n} \leq_{\text{LEX}} X_1^{j_1} \cdots X_n^{j_n}$ if either the two monomials are equal or else the first k for which $i_k \neq j_k$ has $i_k < j_k$. Thus for example, $X_1X_2^2X_3^3 \leq_{\text{LEX}} X_1^2$. The word "lexicographic" refers to the dictionary system for alphabetizing in which a first word comes before a second word if for the first position in which the two words differ, the letter of the first word in that position precedes alphabetically the letter of the second word in that position.

(2) **Graded lexicographic ordering**, abbreviated as "glex" or "grlex" by many authors. As in Section 3 the **total degree** of a monomial $X_1^{i_1} \cdots X_n^{i_n}$ is

[14] This means a partial ordering with the properties that each pair a, b has $a \leq b$ or $b \leq a$ and that both hold only if $a = b$.

$\deg(X_1^{i_1}\cdots X_n^{i_n}) = \sum_{k=1}^n i_k$. The definition of the ordering is that $M \leq_{\text{GLEX}} N$ if either $\deg M < \deg N$ or else if $\deg M = \deg N$ and $M \leq_{\text{LEX}} N$. Thus for example, $X_1^2 \leq_{\text{GLEX}} X_1X_2^2X_3^3$ because the total degree 2 of the first monomial is less than the total degree 6 of the second monomial. But $X_1X_2^2X_3^3 \leq_{\text{GLEX}} X_1^2X_3^4$ because both monomials have the same total degree 6 and the second monomial involves a higher power of X_1 than does the first. This monomial ordering is not much used; more common is the variant of it in the next example.

(3) **Graded reverse lexicographic ordering**, abbreviated as "grevlex" by many authors. The definition is that $M \leq_{\text{GREVLEX}} N$ if either $\deg M < \deg N$ or else if $\deg M = \deg N$ and $N^t \leq_{\text{LEX}} M^t$, where M^t is M but with the exponents of X_j and X_{n-j} interchanged for each j, and where N^t is defined similarly. This ordering takes some getting used to. For example, $X_1^2X_3^4 \leq_{\text{GREVLEX}} X_1X_2^2X_3^3$ when $n = 3$ because both monomials have the same total degree and $X_1^3X_2^2X_3 = (X_1X_2^2X_3^3)^t \leq_{\text{LEX}} (X_1^2X_3^4)^t = X_1^4X_3^2$. By contrast, $X_1X_2^2X_3^3 \leq_{\text{GLEX}} X_1^2X_3^4$.

(4) Orderings of k-**elimination type**, where $1 \leq k \leq n-1$. These are orderings such that any monomial containing one of $X_1, \dots, X_k$ to a positive power exceeds any monomial in $X_{k+1}, \dots, X_n$ alone. These will be discussed in Section 10. Of them, one of particular importance is the **Bayer–Stillman ordering** of k-elimination type. Here a monomial M is $\leq$ a monomial N if the sum of the exponents of $X_1, \dots, X_k$ for M is less than the corresponding sum for N or else the two sums are equal and $M \leq_{\text{GREVLEX}} N$. This ordering is commonly used for making computations in the context of Section 10.

(5) Ordering from a tuple of **weight vectors**. For $1 \leq i \leq n$, let $w^{(i)}$ be a vector in $\mathbb{R}^n$ of the form $w^{(i)} = (w_1^{(i)}, \dots, w_n^{(i)})$, and assume that $w^{(1)}, \dots, w^{(n)}$ are linearly independent over $\mathbb{R}$. Identify the monomial X^α with the vector of individual exponents $\alpha = (\alpha_1, \dots, \alpha_n)$. The ordering given by the weight vectors $w_j^{(i)}$ is defined by saying that $X^\alpha \leq X^\beta$ if $X^\alpha = X^\beta$ or if the first i such that $w^{(i)} \cdot \alpha \neq w^{(i)} \cdot \beta$ has $w^{(i)} \cdot \alpha < w^{(i)} \cdot \beta$. Here the dot refers to the ordinary dot product. A condition is needed on the $w^{(i)}$'s to ensure that $1 \leq X^\alpha$ for all α. (See Problem 14 at the end of the chapter.) Here are two specific examples for which the condition is satisfied. Let $e^{(i)}$ be the i^{th} standard basis vector of $\mathbb{R}^n$. The lexicographic ordering in Example 1 is determined by the tuple of weight vectors $(e^{(1)}, \dots, e^{(n)})$. The Bayer–Stillman ordering in Example 4 is determined by the tuple of weight vectors

$$\big(e^{(1)} + \cdots + e^{(k)}, e^{(k+1)} + \cdots + e^{(n)}, -e^{(n)}, \dots, -e^{(k+2)}, -e^{(k)}, \dots, -e^{(2)}\big).$$

Further discussion of monomial orderings determined by weight vectors occurs in Problems 14–15 at the end of the chapter.

Property (i) of monomial orderings insists that the ordering respect multiplication of monomials in the natural way. Property (ii), according to the next proposition, is a well-ordering property. The proof of the proposition will be preceded by a lemma.

Proposition 8.16. In any monomial ordering for $K[X_1, \ldots, X_n]$, any decreasing sequence $M_1 \geq M_2 \geq M_3 \geq \cdots$ is eventually constant. Consequently each nonempty subset of $\mathcal{M}$ has a smallest element in the ordering.

Lemma 8.17. If I is an ideal in $K[X_1, \ldots, X_n]$ generated by monomials and if $f(X_1, \ldots, X_n)$ is in I, then each monomial appearing in the expansion of f with nonzero coefficient lies in I. Consequently I has a finite set of monomials as generators. Moreover, if $\{M_1, \ldots, M_s\}$ is a set of monomials that generate I and if M is any monomial in I, then some M_j divides M.

PROOF. Let $\{M_\alpha\}$ be the set of monomials that generates I. If f is in I, then we can write $f = \sum_{j=1}^{k} h_j M_{\alpha_j}$ for polynomials h_j. Let $h_j = \sum_{i=1}^{l_j} c_{ij} M_{ij}$ be the expansion of h_j in terms of monomials. If M_0 is a monomial appearing in f with nonzero coefficient c, then the only possible monomial M_{ij} in h_j that can contribute toward c is one with $M_{ij} M_{\alpha_j} = M_0$ if such a monomial exists. For some j, such a monomial must exist, or c would be 0; thus M_0 lies in I.

For the second conclusion, write $\{f_1, \ldots, f_l\}$ by the Hilbert Basis Theorem. The first conclusion shows that each monomial contributing to each f_j lies in I, and the set of all these monomials, as j varies, is therefore a finite set of monomials generating I.

For the third conclusion, write $M = \sum_{i=1}^{s} a_i M_i$ for polynomials a_i. Expanding each a_i in terms of monomials, we see that some a_i contains with nonzero coefficient a monomial M' such that $M = M' M_i$. The divisibility follows. □

PROOF OF PROPOSITION 8.16. Let M be a monomial, and let I be the linear span of all monomials M' with $M' \geq M$. If M' is a such a monomial and N is any monomial, then $NM' \geq NM$ by (i), and $NM \geq 1M = M$ by (i) and (ii). Therefore NM' lies in I, and I is an ideal.

From such an ideal I, we can recover M as the unique monomial M_0 in I such that $M_0 \leq M'$ for every monomial M' in I, since any such M_0 has $M_0 \leq M$ as well as $M \leq M_0$.

With $M_1, M_2, \ldots$ given as in the proposition, let I_k be the linear span of all monomials $M' \geq M_k$. We have just seen that I_k is an ideal, and the I_k's are increasing in k. Then $I = \bigcup_{k=1}^{\infty} I_k$ is an ideal generated by monomials, and Lemma 8.17 shows that it has a finite set of monomials as a set of generators. Each such monomial generator lies in some I_k. Since the I_k's are nested, all the generators lie in some I_{k_0}, and we conclude that $I = I_{k_0}$. The previous paragraph of the proof shows that I_{k_0} determines M_{k_0}, and therefore $M_k = M_{k_0}$ for all $k \geq k_0$.

For the last statement of the proposition, if there were no least element, then for any element in the subset, we could always find a smaller element in the subset. In this way, we would be able to construct a strictly decreasing infinite sequence in $\mathcal{M}$, in contradiction to what has just been proved. $\square$

Fix a monomial ordering for $K[X_1, \dots, X_n]$. If f is any nonzero member of $K[X_1, \dots, X_n]$ and if f is expanded as a K linear combination of monomials, then we define the leading monomial, leading coefficient, and leading term of f by

$$\begin{aligned} \text{LM}(f) &= \text{largest monomial with nonzero coefficient in expansion of } f, \\ \text{LC}(f) &= \text{coefficient of } \text{LM}(f) \text{ in } f, \\ \text{LT}(f) &= \text{LC}(f)\,\text{LM}(f). \end{aligned}$$

It will be convenient to be able to use these definitions without having to distinguish the cases $f \neq 0$ and $f = 0$. Accordingly, let us adjoin 0 to the set $\mathcal{M}$, agreeing that $0 < M$ and $0M = 0$ for every monomial M. We adopt the convention that $\text{LM}(0) = 0$, $\text{LT}(0) = 0$, and $\text{LC}(0) = 0$.

Since any monomial that occurs in a sum of two polynomials occurs in one or the other of them, it is immediate from the definition that

$$\text{LM}(f_1 + f_2) \le \max(\text{LM}(f_1), \text{LM}(f_2))$$

if f_1, f_2, and $f_1 + f_2$ are nonzero. Checking the various cases, we see that this inequality persists if one or more of f_1, f_2, and $f_1 + f_2$ are 0.

The comparable results concerning multiplication are contained in the next proposition.

Proposition 8.18. If f_1 and f_2 are two nonzero members of $K[X_1, \dots, X_n]$, then

$$\text{LM}(f_1 f_2) = \text{LM}(f_1)\,\text{LM}(f_2) \qquad \text{and} \qquad \text{LC}(f_1 f_2) = \text{LC}(f_1)\,\text{LC}(f_2);$$

hence

$$\text{LT}(f_1 f_2) = \text{LT}(f_1)\,\text{LT}(f_2).$$

These equalities persist if one or both of f_1 and f_2 are 0. Moreover, if f_1 and f_2 are nonzero and have $\text{LT}(f_1) = \text{LT}(f_2)$, then $\text{LM}(f_1 - f_2) < \text{LM}(f_1)$.

PROOF. For the first statement, let the expansions of f_1 and f_2 as linear combinations of distinct monomials be $f_1 = a_1\,\text{LM}(f_1) + \sum_i c_i M_i$ and $f_2 = a_2\,\text{LM}(f_2) + \sum_j d_j N_j$ with $M_i < \text{LM}(f_1)$ for all i and $N_j < \text{LM}(f_2)$ for all j. Then $f_1 f_2$ equals

$$a_1 a_2\,\text{LM}(f_1)\,\text{LM}(f_2) + a_2 \sum_i c_i M_i\,\text{LM}(f_2) + a_1 \sum_j d_j\,\text{LM}(f_1) N_j + \sum_{i,j} c_i d_j M_i N_j,$$

and the conclusions in the first sentence of the proposition will follow if it is shown that $M_i\,\mathrm{LM}(f_2) < \mathrm{LM}(f_1)\,\mathrm{LM}(f_2)$, that $\mathrm{LM}(f_1)N_j < \mathrm{LM}(f_1)\,\mathrm{LM}(f_2)$, and that $M_iN_j < \mathrm{LM}(f_1)\,\mathrm{LM}(f_2)$. The first inequality follows from (i) because $M_i < \mathrm{LM}(f_1)$, and the second inequality is similar. For the third we apply (i) twice to obtain $M_iN_j \le M_i\,\mathrm{LM}(f_2) \le \mathrm{LM}(f_1)\,\mathrm{LM}(f_2)$ and observe that the end expressions can be equal only if equality holds in both instances. The latter is impossible because $K[X_1, \dots, X_n]$ is an integral domain, and thus $M_iN_j < \mathrm{LM}(f_1)\,\mathrm{LM}(f_2)$.

The three displayed equalities persist if one or both of f_1 and f_2 are 0 because $\mathrm{LM}(f)$, $\mathrm{LT}(f)$, and $\mathrm{LC}(f)$ can be 0 only if $f = 0$.

Finally if f_1 and f_2 are nonzero and have expansions as in the first paragraph of the proof with $\mathrm{LT}(f_1) = \mathrm{LT}(f_2)$, then $\mathrm{LC}(f_1) = a_1$ and $\mathrm{LC}(f_2) = a_2$. Hence $f_1 - f_2$ has an expansion involving only the monomials M_i and N_j. Consequently if $f_1 - f_2 \ne 0$, then the largest of the M_i's and N_j's is $< \mathrm{LM}(f_1)$. Thus $\mathrm{LM}(f_1 - f_2) < \mathrm{LM}(f_1)$. This inequality holds also if $f_1 - f_2 = 0$. □

If I is a nonzero ideal in $K[X_1, \dots, X_n]$, we define $\mathrm{LT}(I)$ to be the vector space of all K linear combinations of polynomials $\mathrm{LT}(f)$ with f in I. It follows from Proposition 8.18 that $K[X_1, \dots, X_n]\,\mathrm{LT}(I) \subseteq \mathrm{LT}(I)$, and therefore $\mathrm{LT}(I)$ is an ideal in $K[X_1, \dots, X_n]$. A finite unordered subset $\{g_1, \dots, g_k\}$ of nonzero elements of the ideal I is called a **Gröbner basis** of I if $\mathrm{LT}(I) = \big(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_k)\big)$. The inclusion $\supseteq$ follows from the definition, and the question is whether $\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_k)$ generate $\mathrm{LT}(I)$.

Among the examples below, Example 3 is particularly suggestive of the utility of a Gröbner basis. The idea is that an ordinary set of generators may have the property that certain "small" elements of I can be expanded in terms of the generators only using "large" coefficients and that this property is reflected in the failure of $(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_k))$ to exhaust $\mathrm{LT}(I)$.

EXAMPLES WITH LEXICOGRAPHIC ORDERING.

(1) Principal ideal. If $I = (f(X_1, \dots, X_n))$, then $\{f\}$ is a Gröbner basis. In fact, the most general member of I is of the form hf with h in $K[X_1, \dots, X_n]$, and Proposition 8.18 gives $\mathrm{LT}(hf) = \mathrm{LT}(h)\,\mathrm{LT}(f)$. Therefore $\mathrm{LT}(I) = (\mathrm{LT}(f))$, as required.

(2) Ideal generated by members of $K[X_1, \dots, X_n]_1$. Suppose that $I = (L_1, \dots, L_k)$, where each L_j is a homogeneous linear polynomial of degree 1. For example, I could be $(X_1 + X_2 + X_3, X_1 - X_3)$. Let us form the corresponding k-by-n coefficient matrix, specifically $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$ in the 3-variable example. If we perform row operations to transform this matrix into reduced row-echelon form and let $L'_1, \dots, L'_{k'}$ be the members of $K[X_1, \dots, X_n]_1$ corresponding to the reduced matrix, specifically $X_1 - X_3$ and $X_2 + 2X_3$ for the reduced form

$\left(\begin{smallmatrix}1&0&-1\\0&1&2\end{smallmatrix}\right)$ of $\left(\begin{smallmatrix}1&1&1\\1&0&-1\end{smallmatrix}\right)$, then $I = (L'_1, \dots, L'_{k'})$ and moreover $\{L'_1, \dots, L'_{k'}\}$ is a Gröbner basis of I. This fact is not particularly obvious in the full generality of this example, but it will be shown to be an easy consequence of Theorem 8.23 in the next section.

(3) Earlier example in this section. In $K[X, Y]$, let $I = (f_1, f_2)$ with $f_1(X, Y) = X^2 + 2XY^2$ and $f_2(X, Y) = XY + 2Y^3 - 1$. Then $\big(\mathrm{LT}(f_1), \mathrm{LT}(f_2)\big) = (X^2, XY)$. We saw that X is a member of I and that $\mathrm{LT}(X) = X$ is not in $\big(\mathrm{LT}(f_1), \mathrm{LT}(f_2)\big)$. So $\{f_1, f_2\}$ is not a Gröbner basis. If we enlarge the set of generators of I to $\{f_1, f_2, X\}$, then we still do not have a Gröbner basis because $f_2 - YX = 2Y^3 - 1$ is in I and $\mathrm{LT}(f_2 - YX) = 2Y^3$ does not lie in $\big(\mathrm{LT}(f_1), \mathrm{LT}(f_2), \mathrm{LT}(X)\big) = (X^2, XY, X) = (X)$. We can enlarge the set of generators still further to $\{f_1, f_2, X, 2Y^3 - 1\}$. Is this a Gröbner basis? Here we have $\big(\mathrm{LT}(f_1), \mathrm{LT}(f_2), \mathrm{LT}(X), \mathrm{LT}(2Y^3 - 1)\big) = (X, Y^3)$, and it seems as if this equals $\mathrm{LT}(I)$. But we need a way of checking easily. We shall obtain a way of checking in Theorem 8.23 in the next section.

The question of existence–uniqueness of a Gröbner basis will be addressed constructively in Sections 8–9; however, we did observe at the beginning of this section that Hilbert's proof of the Hilbert Basis Theorem essentially handles existence when the monomial ordering is the usual lexicographic ordering. Actually, the argument at the beginning of the section had two parts to it—a nonconstructive argument producing a certain finite set of leading terms and a verification that those leading terms lead to a set of generators of the ideal. The first part, being a nonconstructive existence proof, does not help us in our current efforts, and we defer to Problem 13 at the end of the chapter the question of adapting it to a general monomial order. The second part, on the other hand, is a useful kind of verification in our current efforts. It shows that a certain kind of finite subset of an ideal is necessarily a set of generators, and it generalizes as follows. The generalization will play a role in Section 9.

Proposition 8.19. If K is a field, if a monomial ordering is specified for $K[X_1, \dots, X_n]$, and if $\{g_1, \dots, g_k\}$ is a Gröbner basis for a nonzero ideal I of $K[X_1, \dots, X_n]$, then $\{g_1, \dots, g_k\}$ generates I.

PROOF. First we prove that if $f \neq 0$ is in I, then there exist a g_j, a monomial M_0, and a nonzero scalar c such that $\mathrm{LM}(f - cM_0 g_j) < \mathrm{LM}(f)$. To see this, we use the hypothesis that $\{g_1, \dots, g_k\}$ is a Gröbner basis to find polynomials $h_1, \dots, h_k$ such that $\mathrm{LM}(f) = \sum_{i=1}^k h_i \,\mathrm{LM}(g_i)$. Then it must be true for i equal to some index j that $\mathrm{LM}(f) = M_0 \,\mathrm{LM}(g_j)$ for one of the monomials M_0 that appears in h_j with nonzero coefficient. Since $M_0 \,\mathrm{LM}(g_j) = \mathrm{LM}(M_0)\,\mathrm{LM}(g_j) = \mathrm{LM}(M_0 g_j)$, we can rewrite this equality as $\mathrm{LT}(f) = c\,\mathrm{LT}(M_0 g_j)$ for some scalar $c \neq 0$. Then

$\text{LT}(f) = \text{LT}(cM_0g_j)$, and Proposition 8.18 shows that $\text{LM}(f - cM_0g_j) < \text{LM}(f)$, as asserted.

Iterating this construction and assuming that we never get 0, we can find successively nonzero scalars c_i, monomials M_i, and members g_{j_i} of the Gröbner basis such that the sequence $\text{LM}\big(f - \sum_{i=1}^{l} c_j M_j g_{j_i}\big)$ indexed by l is strictly decreasing, in contradiction to Proposition 8.16. To avoid the contradiction, we must have $f - \sum_{i=1}^{l} c_j M_j g_{j_i} = 0$ for some l, and then f is exhibited as in the ideal $(g_1, \dots, g_k)$. Hence the Gröbner basis generates I. □

8. Constructive Existence

Throughout this section, K denotes a field, and we work with a fixed monomial ordering on $K[X_1, \dots, X_n]$. Ideals in $K[X_1, \dots, X_n]$ will always be specified by giving finite sets of generators. Our objective is to obtain a constructive proof of the existence of a Gröbner basis for each nonzero ideal in $K[X_1, \dots, X_n]$, along with a useful test procedure for deciding whether a given finite set of generators of I is a Gröbner basis. As is often the case with existence proofs, the motivation for the proof comes from a certain amount of deduction of properties that a Gröbner basis must satisfy if its exists. It was mentioned in the previous section that the failure of a set of generators to be a Gröbner basis has something to do with its failure to be able to represent all "small" elements of the ideal by means of expansions in terms of the generators that use "small" coefficients. The first part of this section will explore this idea, seeking to make it precise. The main step will be a checkable text for a set to be a Gröbner basis; this is Theorem 8.23. The existence argument will be an easy corollary. A by-product of the existence argument will be a way of testing a polynomial for membership in I.

In the one-variable case any ideal is principal, necessarily of the form $(g(X))$, and the test for membership of a polynomial f in the ideal is to apply the division algorithm, writing $f(X) = q(X)g(X) + r(X)$ with $r = 0$ or $\deg r < \deg g$. Then f is a member of the ideal if and only if $r = 0$. The starting point for the several-variable theory is to do the best we can to generalize the division algorithm to several variables, recognizing that we cannot expect too much because of the complicated ideal structure in several variables.

Proposition 8.20 (generalized division algorithm). Let $(f_1, \dots, f_s)$ be a fixed enumeration of a set of nonzero members of $K[X_1, \dots, X_n]$, and let f be an arbitrary nonzero member of $K[X_1, \dots, X_n]$. Then there exist polynomials $a_1, \dots, a_s$ and r such that

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

such that $\mathrm{LM}(a_j f_j) \leq \mathrm{LM}(f)$ for all j, and such that no monomial appearing in r with nonzero coefficient is divisible by $\mathrm{LM}(f_j)$ for any j.

REMARK. The proof below will stop short of giving an algorithm, because omitting the details of the algorithm will make the invariant of the construction clearer. To make the proof into an algorithm, one merely needs to be systematic about the choices in the proof. There is no claim of any uniqueness of $a_1, \dots, a_s$ or r in the statement; in fact, Problem 16 at the end of the chapter shows that more than one kind of nonuniqueness is possible. Corollary 8.21 below, however, will show that if the given $f_1, \dots, f_s$ form a Gröbner basis of an ideal I, then r is independent of the enumeration of the Gröbner basis, even without the requirement that $\mathrm{LM}(a_j f_j) \leq \mathrm{LM}(f)$ for all j.

PROOF. We shall do a kind of induction involving decompositions of f of the form

$$f = (a_1 f_1 + \cdots + a_s f_s) + p + r, \qquad (*)$$

where $a_1, \dots, a_s, p, r$ are polynomials with the properties that

(i) $\mathrm{LM}(p) \leq \mathrm{LM}(f)$,
(ii) $\mathrm{LM}(a_i f_i) \leq \mathrm{LM}(f)$ for all i,
(iii) no monomial M appearing in r with nonzero coefficient has M divisible by any $\mathrm{LM}(f_i)$,

and we shall demonstrate that $\mathrm{LM}(p)$ decreases at every step of the induction as long as $p \neq 0$. Initially we take all $a_i = 0$, $p = f$, and $r = 0$. Then $(*)$ and the three properties hold at the start. Let us describe the inductive step.

If $\mathrm{LT}(f_j)$ divides $\mathrm{LT}(p)$ for some j, then we replace a_j by $a_j + \mathrm{LT}(p)/\mathrm{LT}(f_j)$, we change p to $p - \big(\mathrm{LT}(p)/\mathrm{LT}(f_j)\big) f_j$, and we leave r alone. The equality $(*)$ is maintained, and (iii) continues to hold. Since

$$\begin{aligned} \mathrm{LT}\Big(\big(\mathrm{LT}(p)/\mathrm{LT}(f_j)\big) f_j\Big) &= \mathrm{LT}\big(\mathrm{LT}(p)/\mathrm{LT}(f_j)\big)\,\mathrm{LT}(f_j) \\ &= \big(\mathrm{LT}(p)/\mathrm{LT}(f_j)\big)\,\mathrm{LT}(f_j) = \mathrm{LT}(p), \end{aligned} \qquad (**)$$

Proposition 8.18 shows that $\mathrm{LM}(p)$ strictly decreases. Consequently (i) continues to hold. By the same kind of computation as for $(**)$,

$$\begin{aligned} \mathrm{LM}\Big(\big(a_j + \mathrm{LT}(p)/\mathrm{LT}(f_j)\big) f_j\Big) &\leq \max\Big(\mathrm{LM}(a_j f_j), \mathrm{LM}\big(\mathrm{LT}(p)/\mathrm{LT}(f_j)\big) f_j\Big) \\ &\leq \max(\mathrm{LM}(f), \mathrm{LM}(p)) = \mathrm{LM}(f), \end{aligned}$$

and therefore (ii) continues to hold. This completes the inductive step if $\mathrm{LT}(f_j)$ divides $\mathrm{LT}(p)$ for some j.

The contrary case is that $\mathrm{LT}(p)$ is divisible by $\mathrm{LT}(f_i)$ for no i. Then we replace p by $p - \mathrm{LT}(p)$, we change r to $r + \mathrm{LT}(p)$, and we leave all a_i alone. The equality $(*)$ is maintained, and (ii) continues to hold. Since $\mathrm{LM}(p) = \mathrm{LM}(\mathrm{LT}(p))$, Proposition 8.18 shows that $\mathrm{LM}(p)$ strictly decreases. Consequently (i) continues to hold. Also, (iii) continues to hold because of the assumption that $\mathrm{LT}(p)$ is divisible by $\mathrm{LT}(f_i)$ for no i. This completes the inductive step if $\mathrm{LT}(p)$ is divisible by $\mathrm{LT}(f_i)$ for no i.

Proposition 8.16 shows that the induction can continue for only finitely many steps. Since it must continue as long as $p \neq 0$, the conclusion is that $p = 0$ after some stage, and then the decomposition of the proposition has been proved. □

Corollary 8.21. If $\{g_1, \dots, g_s\}$ is a Gröbner basis of a nonzero ideal I of $K[X_1, \dots, X_n]$ and if f is any nonzero member of $K[X_1, \dots, X_n]$, then there exist polynomials g and r such that $f = g + r$, g is in I, and no monomial appearing in r with nonzero coefficient is divisible by $\mathrm{LM}(g_j)$ for any j. Moreover, r is uniquely determined by these properties, and g has an expansion $g = \sum_{i=1}^{s} a_i g_i$ with $\mathrm{LM}(a_i g_i) \leq \mathrm{LM}(f)$ for all i.

REMARKS. The uniqueness statement implies in particular that r is independent of the enumeration of the set $\{g_1, \dots, g_s\}$. This corollary will give us some insight into the way a Gröbner basis can resolve cancellation. Shortly we shall introduce specific members of I that have cancellation built into their definition. Being in I, they have expansions with remainder term 0, according to this corollary. Since the remainder is unique, the corollary says that they can be rewritten in terms of the Gröbner basis in a way that eliminates the cancellation.

PROOF. For existence, let $\{g_1, \dots, g_s\}$ be a Gröbner basis of I, and apply Proposition 8.20 to f and the ordered set $(g_1, \dots, g_s)$. Then the existence follows immediately.

For uniqueness, suppose that $f = g_1 + r_1 = g_2 + r_2$. Then $r_1 - r_2 = g_2 - g_1$ exhibits $r_1 - r_2$ as in I. Arguing by contradiction, suppose that $r_1 \neq r_2$. The hypothesis on r_1 and r_2 shows that no monomial with nonzero coefficient in $r_1 - r_2$ is divisible by any $\mathrm{LM}(g_j)$, and in particular $\mathrm{LM}(r_1 - r_2)$ is not divisible by any of the generators of the monomial ideal $\big(\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)\big) = \mathrm{LM}(I)$. Since $\mathrm{LM}(r_1 - r_2)$ is a monomial in this ideal, this conclusion contradicts the last conclusion of Lemma 8.17. □

Suppose that $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ and $X^\beta = X_1^{\beta_1} \cdots X_n^{\beta_n}$ are two monomials in $K[X_1, \dots, X_n]$. Then we define their **least common multiple** $\mathrm{LCM}(X^\alpha, X^\beta)$ to be

$$\mathrm{LCM}(X^\alpha, X^\beta) = X^\gamma = X_1^{\gamma_1} \cdots X_n^{\gamma_n} \qquad \text{with } \gamma_j = \max(\alpha_j, \beta_j) \text{ for all } j.$$

This notion does not depend on the choice of a monomial ordering. Observe for any two monomials M and N that $\mathrm{LCM}(M, N)/M$ and $\mathrm{LCM}(M, N)/N$ are monomials.

If f_1 and f_2 are nonzero polynomials, then the expression

$$\frac{\mathrm{LCM}\big(\textsc{lm}(f_1),\textsc{lm}(f_2)\big)}{\textsc{lt}(f_1)}\,f_1=\frac{\mathrm{LCM}\big(\textsc{lm}(f_1),\textsc{lm}(f_2)\big)}{\textsc{lm}(f_1)}\,\frac{f_1}{\textsc{lc}(f_1)}$$

is a polynomial whose leading monomial is $\mathrm{LCM}\big(\textsc{lm}(f_1),\textsc{lm}(f_2)\big)$ and whose leading coefficient is 1. We define the S-**polynomial** of f_1 and f_2 to be

$$S(f_1,\,f_2)=\frac{\mathrm{LCM}\big(\textsc{lm}(f_1),\textsc{lm}(f_2)\big)}{\textsc{lt}(f_1)}\,f_1-\frac{\mathrm{LCM}\big(\textsc{lm}(f_1),\textsc{lm}(f_2)\big)}{\textsc{lt}(f_2)}\,f_2.$$

This is the difference of two polynomials with the same leading monomial $\mathrm{LCM}\big(\textsc{lm}(f_1),\textsc{lm}(f_2)\big)$ and with the same leading coefficient 1. Accordingly, Proposition 8.18 shows that

$$\textsc{lm}(S(f_1,\,f_2))<\mathrm{LCM}\big(\textsc{lm}(f_1),\textsc{lm}(f_2)\big).$$

The elements $S(f_1,\,f_2)$ are the elements mentioned in the remarks with Corollary 8.21; the above inequality is a precise formulation of their built-in cancellation.

Lemma 8.22 below says that whenever cancellation of this kind occurs in any sum of products with functions $f_1,\dots,f_s$, then the sum of products can be rewritten in terms of the S-polynomials $S(f_j,\,f_k)$. In this way the nature of the cancellation has been made more transparent, partly being accounted for by the definitions of the individual polynomials $S(f_j,\,f_k)$.

Lemma 8.22. Let M and $M_1,\dots,M_s$ be monomials, let $f_1,\dots,f_s$ be nonzero polynomials, and suppose that $M_i\,\textsc{lm}(f_i)=M$ for all i. If $c_1,\dots,c_s$ are constants such that $\textsc{lm}\big(\sum_{i=1}^s c_iM_i f_i\big)<M$, then the sum $\sum_{i=1}^s c_iM_i f_i$ can be rewritten in the form

$$\sum_{i=1}^s c_iM_i f_i=\sum_{j<k}\frac{d_{jk}M}{\mathrm{LCM}\big(\textsc{lm}(f_j),\textsc{lm}(f_k)\big)}\,S(f_j,\,f_k)$$

for suitable constants d_{jk}. In the sum on the right side, each nonzero term has leading monomial $<M$.

PROOF. Let us write $L_{ij}=\mathrm{LCM}\big(\textsc{lm}(f_i),\textsc{lm}(f_j)\big)$ for $i\neq j$. We may assume that all the c_i are nonzero, and we proceed by induction on s. There is nothing to prove for $s=1$. The key step is $s=2$, for which we are given that the M term of $c_1M_1f_1+c_2M_2f_2$ is 0, i.e., that

$$c_1\,\textsc{lc}(f_1)+c_2\,\textsc{lc}(f_2)=0. \qquad (*)$$

Substituting for $\mathrm{LC}(f_2)$ from $(*)$ gives

$$\begin{aligned} ML_{12}^{-1}S(f_1,\, f_2) &= Mf_1/\,\mathrm{LT}(f_1) - Mf_2/\,\mathrm{LT}(f_2) \\ &= M_1 f_1/\,\mathrm{LC}(f_1) - M_2 f_2/\,\mathrm{LC}(f_2) \\ &= c_1^{-1}\,\mathrm{LC}(f_1)^{-1}(c_1 M_1 f_1 + c_2 M_2 f_2), \end{aligned}$$

and this proves the displayed formula of the lemma with $d_{12} = c_1\,\mathrm{LC}(f_1)$.

Assume the result for $s-1 \geq 2$. We are given that $\sum_{i=1}^{s} c_i\,\mathrm{LC}(f_i) = 0$, which we break into two parts as

$$\begin{aligned} c_1\,\mathrm{LC}(f_1) - \tfrac{c_1\,\mathrm{LC}(f_1)}{\mathrm{LC}(f_2)}\,\mathrm{LC}(f_2) &= 0, \\ \Big(c_2 + \tfrac{c_1\,\mathrm{LC}(f_1)}{\mathrm{LC}(f_2)}\Big)\,\mathrm{LC}(f_2) + \sum_{i=3}^{s} c_i\,\mathrm{LC}(f_i) &= 0. \end{aligned}$$

The inductive hypothesis gives

$$\begin{aligned} c_1 M_1 f_1 - \tfrac{c_1\,\mathrm{LC}(f_1)}{\mathrm{LC}(f_2)}\,M_2 f_2 &= d_{12} M L_{12}^{-1} S(f_1,\, f_2), \\ \Big(c_2 + \tfrac{c_1\,\mathrm{LC}(f_1)}{\mathrm{LC}(f_2)}\Big) M_2 f_2 + \sum_{i=3}^{s} c_i M_i f_i &= \sum_{2 \leq j < k} d_{jk} M L_{jk}^{-1} S(f_j,\, f_k). \end{aligned}$$

Adding these two formulas, we obtain the displayed formula of the lemma for the case s, and the induction is complete. □

Theorem 8.23. Let $\{g_1, \ldots, g_s\}$ be a set of generators of a nonzero ideal I of $K[X_1, \ldots, X_n]$, and assume that $g_i \neq 0$ for all i. Then the following conditions on $\{g_1, \ldots, g_s\}$ are equivalent:

(a) $\{g_1, \ldots, g_s\}$ is a Gröbner basis of I,

(b) for each pair (g_j, g_k) with $S(g_j, g_k) \neq 0$, every expansion of $S(g_j, g_k)$ as $S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i + r$ with the two properties that

 (i) $\mathrm{LM}(a_{ijk} g_i) \leq \mathrm{LM}(S(g_j, g_k))$ and

 (ii) no monomial appearing in r with nonzero coefficient is divisible by $\mathrm{LM}(g_j)$ for any j

has $r = 0$,

(c) for each pair (g_j, g_k) with $S(g_j, g_k) \neq 0$, there is an expansion of the form $S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i$ with $\mathrm{LM}(a_{ijk} g_i) \leq \mathrm{LM}(S(g_j, g_k))$.

REMARKS. Because of the equivalence of (b) and (c), the generalized division algorithm (Proposition 8.20) gives us a procedure for testing whether these conditions are satisfied by $\{g_1, \ldots, g_s\}$. Namely we follow through the steps in the proof of Proposition 8.20 in whatever fashion we please for each nonzero

$S(g_j, g_k)$. If we get remainder $r = 0$ for each pair (j, k), then the conditions are satisfied. If we get a nonzero remainder r for some pair, then the conditions are not satisfied. In view of the equivalence of (a) with these conditions, we have an effective (though somewhat tedious) way of checking whether $\{g_1, \dots, g_s\}$ is a Gröbner basis.

PROOF. We prove that (a) implies (b) and that (c) implies (a). Since (b) certainly implies (c), the proof will be complete.

Let (a) hold, i.e., let $\{g_1, \dots, g_s\}$ be a Gröbner basis. If $S(g_j, g_k) \neq 0$, then $S(g_j, g_k)$ is a nonzero member of I because each g_i lies in I, and $S(g_j, g_k)$ consequently has an expansion as $\sum_{i=1}^s a_i g_i + r$ with $r = 0$. By Corollary 8.21 it has a possibly different expansion with $r = 0$ and with $\mathrm{LM}(a_i g_i) \leq \mathrm{LM}(S(g_j, g_k))$ for each i. On the other hand, in any expansion of $S(g_j, g_k)$ as $\sum_{i=1}^s a_i g_i + r$ such that (ii) holds, whether or not $\mathrm{LM}(a_i g_i) \leq \mathrm{LM}(S(g_j, g_k))$, r must be 0 by Corollary 8.21. This proves (b).

To prove that (c) implies (a), we argue by contradiction. Among all expansions of members of I as $\sum_{i=1}^s b_i g_i$ such that $\mathrm{LT}\big(\sum_{i=1}^s b_i g_i\big)$ is not in the ideal $\big(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\big)$, choose one for which

$$M = \max_{1 \leq i \leq s} \mathrm{LM}(b_i g_i)$$

is as small as possible; this choice exists by Proposition 8.16. For this choice, let

$$f = \sum_{i=1}^s b_i g_i. \tag{$*$}$$

Define $M_i = \mathrm{LM}(b_i)$ for each i with $b_i \neq 0$. If i_0 is an index with $M = \mathrm{LM}(b_{i_0} g_{i_0})$, then $M = M_{i_0}\,\mathrm{LM}(g_{i_0})$ by Proposition 8.18, and hence M lies in $\big(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\big)$. Since $\mathrm{LT}\big(\sum_{i=1}^s b_i g_i\big)$ is not in $\big(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\big)$, it follows that $\mathrm{LT}\big(\sum_i b_i g_i\big) < M$. Within the set $\{1, \dots, s\}$, define a subset E to consist of those i for which $M_i\,\mathrm{LM}(g_i) = M$. This set contains i_0, and it has the property that all i not in E have $\mathrm{LM}(b_i g_i) < M$. We regroup f as

$$f = \sum_{i \in E} b_i g_i + \sum_{i \notin E} b_i g_i = \sum_{i \in E} \mathrm{LC}(b_i) M_i g_i + \sum_{i \in E} (b_i - \mathrm{LT}(b_i)) g_i + \sum_{i \notin E} b_i g_i.$$

Every term in the second and third sums on the right side has leading monomial $< M$, and so does f. Therefore $\mathrm{LM}\big(\sum_{i \in E} \mathrm{LC}(b_i) M_i g_i\big) < M$. It follows that the expression $\sum_{i \in E} \mathrm{LC}(b_i) M_i g_i$ is of the form considered in Lemma 8.22 with $c_i = \mathrm{LC}(b_i)$ for $i \in E$ (and $c_i = 0$ for $i \notin E$). The lemma tells us that

$$\sum_{i \in E} \mathrm{LC}(b_i) M_i g_i = \sum_{j,k} d_{jk} (M / L_{jk}) S(g_j, g_k)$$

for suitable scalars d_{jk}, where $L_{jk} = \mathrm{LCM}\big(\mathrm{LM}(g_j), \mathrm{LM}(g_k)\big)$.

Now we apply the hypothesis (c), expanding each $S(g_j, g_k)$ in some way as $S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i$ with the a_{ijk} equal to polynomials such that

$$\mathrm{LM}(a_{ijk} g_i) \le \mathrm{LM}(S(g_j, g_k)). \tag{$**$}$$

Substituting for $S(g_j, g_k)$, we obtain

$$f = \sum_{i,j,k} d_{jk}(M/L_{jk}) a_{ijk} g_i + \sum_{i \in E} (b_i - \mathrm{LT}(b_i)) g_i + \sum_{i \notin E} b_i g_i. \tag{$\dagger$}$$

We know that every term in the second and third sums on the right side of (†) has leading monomial $< M$, and we shall estimate the leading monomial of each term in the first sum. Multiplying the inequality

$$\mathrm{LM}(S(g_j, g_k)) < \mathrm{LCM}\big(\mathrm{LM}(g_j), \mathrm{LM}(g_k)\big) = L_{jk}$$

by the monomial M/L_{jk} yields

$$(M/L_{jk})\, \mathrm{LM}(S(g_j, g_k)) < M \tag{$\dagger\dagger$}$$

for every pair (j, k). Combining $(**)$ and (††) gives

$$\mathrm{LM}\big((M/L_{jk}) a_{ijk} g_i\big) = (M/L_{jk})\, \mathrm{LM}(a_{ijk} g_i) \le (M/L_{jk})\, \mathrm{LM}(S(g_j, g_k)) < M.$$

Since each d_{jk} is a scalar, every term in the first sum on the right side of (†) has leading monomial $< M$. Thus (†) is an expansion of a member of I that contradicts the minimality of $\max_i \mathrm{LM}(b_i g_i)$ in the expansion $(*)$. From this contradiction we conclude that (a) holds. □

EXAMPLE OF A VERIFICATION THAT A SET IS A GRÖBNER BASIS. This example continues Example 2 of "Examples with lexicographic ordering" in the previous section. A nonzero ideal I is generated by members of $K[X_1, \dots, X_n]_1$ of the form $(L_1, \dots, L_s)$, where each L_j is a linear combination of $X_1, \dots, X_n$. After initial manipulations we assume that the matrix of coefficients of $L_1, \dots, L_s$ is in reduced row-echelon form. The assertion is that $\{L_1, \dots, L_s\}$ is then a Gröbner basis of I. To prove this, we write $L_j = X_{n_j} + l_j$, where X_{n_j} is the associated corner variable and l_j is a linear combination of $X_{n_j+1}, \dots, X_n$ such that the coefficient of each corner variable is 0. If $j < k$, then

$$S(L_j, L_k) = -l_k X_{n_j} + l_j X_{n_k} = -l_k(X_{n_j} + l_j) + l_j(X_{n_k} + l_k) = -l_k L_j + l_j L_k.$$

The second term on the right side contains no variable $X_1, \dots, X_{n_j}$, but the first term on the right side contains X_{n_j}. Therefore, relative to the lexicographic ordering, we have $\mathrm{LM}\big(S(L_j, L_k)\big) = \mathrm{LM}(-l_k L_j) = \mathrm{LM}(l_k) X_{n_j}$. Consequently $\mathrm{LM}(l_j L_k) \le \mathrm{LM}\big(S(L_j, L_k)\big)$ (and actually strict inequality must hold). Thus the displayed formula shows that $S(L_j, L_k) = a_1 L_j + a_2 L_k$ in the form demanded by (c) of Theorem 8.23. Since (c) implies (a) in the theorem, $\{L_1, \dots, L_s\}$ is a Gröbner basis of I.

Corollary 8.24 (Buchberger's algorithm).[15] Each nonzero ideal in the polynomial ring $K[X_1, \dots, X_n]$ has a Gröbner basis. Such a basis can be obtained by the following procedure: Start from any set $\{f_1, \dots, f_t\}$ of nonzero generators, apply the generalized division algorithm in some fashion to each $S(f_j, f_k)$ and to the generating set $\{f_1, \dots, f_t\}$, and adjoin to the set of generators any nonzero remainders obtained from this process. Iterate this process for enlarging a set $\{f'_1, \dots, f'_{t'}\}$ of generators as long as a nonzero remainder is obtained for some $S(f'_j, f'_k)$. This process must terminate at some point with all remainders equal to 0, and the resulting generating set is a Gröbner basis.

PROOF. At the stage of the iteration that works with the set $\{f'_1, \dots, f'_{t'}\}$ of generators, any nonzero remainder r that arises has the property that no monomial occurring in r is divisible by any $\mathrm{LM}(f'_j)$. By Lemma 8.17, $\mathrm{LT}(r)$ is not a member of $\big(\mathrm{LT}(f'_1), \dots, \mathrm{LT}(f'_t)\big)$. However, at the next stage when r has been designated as one of the generators of I, $\mathrm{LT}(r)$ has become one of the generators of this ideal. Therefore the ideal $\big(\mathrm{LT}(f'_1), \dots, \mathrm{LT}(f'_t)\big)$ strictly increases as we pass from one stage to the next. Since $K[X_1, \dots, X_n]$ is Noetherian, its ideals satisfy the ascending chain condition, and this chain of ideals must stabilize. Consequently all the remainders must be 0 at some point, and then Theorem 8.23 shows that the set of generators is a Gröbner basis. □

EXAMPLE OF THE COMPUTATION OF A GRÖBNER BASIS. We return to Example 3 of "Examples with lexicographic ordering" in the previous section. In $K[X, Y]$, we let $f_1(X, Y) = X^2 + 2XY^2$ and $f_2(X, Y) = XY + 2Y^3 - 1$, and we define $I = (f_1, f_2)$. We seek a Gröbner basis of I, using the lexicographic ordering. Direct computation gives $S(f_1, f_2) = Y(X^2 + 2XY^2) - X(XY + 2Y^3 - 1) = X$. Since X is not divisible by $\mathrm{LM}(f_1)$ or by $\mathrm{LM}(f_2)$, $S(f_1, f_2) = 0 f_1 + 0 f_2 + X$ is an expansion of $S(f_1, f_2)$ as in Theorem 8.23c with $r = X$. The procedure of Corollary 8.24 says to adjoin $f_3 = X$ to the generating set and test again. Direct computation gives $S(f_1, f_3) = 1(X^2 + 2XY^2) - X \cdot X = 2XY$, and $S(f_1, f_3) = 0 f_1 + 0 F_2 + (2Y) f_3 + 0$ is an expansion of $S(f_1, f_3)$ as in (c), since $\mathrm{LM}(2Y f_3) \le \mathrm{LM}\big(S(f_1, f_3)\big)$. Thus $S(f_1, f_3)$ gives us a 0 remainder, hence nothing new to process. In addition, we have $S(f_2, f_3) = 1(XY + 2Y^3 - 1) - Y \cdot X = 2Y^3 - 1$. No term of this is divisible by any of the leading monomials of f_1, f_2, f_3, namely X^2, XY, X. Hence $2Y^3 - 1$ is a nonzero remainder.[16] Therefore we are to adjoin $f_4 = 2Y^3 - 1$ to our set. Computation gives $S(f_1, f_4) = 2XY^4 + X^2 = (2Y^4 + X) f_3$, $S(f_2, f_4) = 2Y^5 - Y^2 + \frac{1}{2}X = \frac{1}{2} f_3 + Y^2 f_4$,

[15] Computer programs typically use an improved version of this algorithm to compute Gröbner bases.

[16] It was not a bad choice of decomposition that led to a nonzero remainder when some other decomposition might have given us 0; the equivalence of (b) and (c) in Theorem 8.23 assures us of that fact.

and $S(f_3, f_4) = \frac{1}{2}X = \frac{1}{2}f_3$. In every case each term has leading monomial at most the leading monomial of the S-polynomial. Hence all remainders are 0, and Corollary 8.24 says that $\{f_1, f_2, f_3, f_4\}$ is a Gröbner basis of I.

Corollary 8.25 (solution of the ideal-membership problem). If I is a nonzero ideal in $K[X_1, \dots, X_n]$ and f is a polynomial, then a procedure for deciding whether f lies in I is as follows: introduce a monomial ordering, construct a Gröbner basis $\{g_1, \dots, g_s\}$ of I by means of Corollary 8.24, and apply the generalized division algorithm to write $f = \sum_{i=1}^{s} a_i g_i + r$ for polynomials $a_1, \dots, a_r, r$ such that no monomial appearing in r with nonzero coefficient is divisible by $\text{LM}(g_j)$ for any j. Then f lies in I if and only if $r = 0$.

PROOF. Corollary 8.24 produces the Gröbner basis, and Corollary 8.21 affirms that this procedure decides whether f lies in I. □

Corollary 8.26 (solution of the proper-ideal problem). If I is a nonzero ideal in $K[X_1, \dots, X_n]$, then a procedure for deciding whether $I = K[X_1, \dots, X_n]$ is to compute a Gröbner basis for I and to see whether one of its members is a nonzero scalar c.

PROOF. If I has a nonzero scalar as one of its generators, then 1 lies in I, and hence I certainly equals $K[X_1, \dots, X_n]$. Conversely if I is given, then Corollary 8.24 produces a Gröbner basis $\{g_1, \dots, g_s\}$. Since $\text{LT}(1) = 1$ and since $\text{LT}(I) = \big(\text{LT}(g_1), \dots, \text{LT}(g_s)\big)$, the monomial 1 must lie in $\big(\text{LT}(g_1), \dots, \text{LT}(g_s)\big)$. Since 1 is a monomial, Lemma 8.17 shows that it must be divisible by $\text{LM}(g_j)$ for some j. Therefore $\text{LM}(g_j) = 1$. Since 1 is the smallest monomial in any monomial ordering, it is the only monomial appearing with a nonzero coefficient in g_j. Therefore g_j is a nonzero scalar. □

In many applications of Gröbner bases, there is some flexibility in what monomial ordering to impose in obtaining the Gröbner basis. In Corollaries 8.25 and 8.26, for example, absolutely any monomial ordering works fine. The actual calculation of Gröbner bases is often computationally demanding, and thus it is worthwhile to use such a basis that takes relatively little time to compute. According to computer scientists,[17] Gröbner bases are the most widely useful when computed relative to the lexicographic ordering, but they are then also the most time-consuming to compute. The monomial orderings that make the computation of Gröbner bases proceed quickly tend to be ones that first bound

[17] The Web essay "Representation and monomial orders," `http://www.umich.edu/~gpcc/scs/magma/text835.htm`, within the publication of the Statistics and Computation Service listed in the Selected References contains a discussion of various monomial orders and their uses and advantages.

the total degree in one or two steps. One of the reasons that this kind of monomial ordering works so efficiently is that once the total degree is bounded, there are only finitely many monomials less than any given monomial M.

9. Uniqueness of Reduced Gröbner Bases

In this section, K continues to denote a field, and we work with a fixed monomial ordering on $K[X_1, \ldots, X_n]$. Ideals in $K[X_1, \ldots, X_n]$ will always be specified by giving finite sets of generators. Our objective in this section is to show how any Gröbner basis can be "reduced" and that a "reduced" Gröbner basis for an ideal is unique. A by-product of the uniqueness argument will be a way of testing two ideals for equality.

Any finite set of generators of I that contains a Gröbner basis is again a Gröbner basis. Thus a constructed Gröbner basis will often be unnecessarily large. One simple kind of redundance is addressed by Lemma 8.27 below.

Lemma 8.27. If $\{g_1, \ldots, g_s\}$ is a Gröbner basis for a nonzero ideal I in $K[X_1, \ldots, X_n]$ and if $\text{LM}(g_1)$ lies in the ideal $\big(\text{LT}(g_2), \ldots, \text{LT}(g_s)\big)$, then $\{g_2, \ldots, g_s\}$ is a Gröbner basis of I.

REMARK. Lemma 8.17 shows how to check whether $\text{LM}(g_1)$ lies in the ideal $\big(\text{LT}(g_2), \ldots, \text{LT}(g_s)\big)$; all we have to do is see whether some $\text{LM}(g_j)$ for $j \geq 1$ divides $\text{LM}(g_1)$.

PROOF. By hypothesis, $\big(\text{LT}(g_2), \ldots, \text{LT}(g_s)\big) = \big(\text{LT}(g_1), \ldots, \text{LT}(g_s)\big) = \text{LT}(I)$. Therefore $\{g_2, \ldots, g_s\}$ is a Gröbner basis of I. (Recall that the definition of Gröbner basis does not assume that the set generates the ideal; Proposition 8.19 deduces that it generates.) □

A Gröbner basis $\{g_1, \ldots, g_s\}$ of a nonzero ideal I is said to be **minimal** if $\text{LC}(g_j) = 1$ for all j and if no $\text{LM}(g_i)$ is divisible by $\text{LM}(g_j)$ for some $j \neq i$. Lemma 8.27 shows that in trying to transform a Gröbner basis into a form for which a uniqueness result will apply, there is no loss of generality in assuming that the given Gröbner basis is minimal.

EXAMPLE. As in the example following Corollary 8.24, let I be the ideal in $K[X, Y]$ given by $I = (f_1, f_2)$ with $f_1(X, Y) = X^2 + 2XY^2$ and $f_2(X, Y) = XY + 2Y^3 - 1$. Then we saw that $\{f_1, f_2, f_3, f_4\}$ is a Gröbner basis of I in the lexicographic ordering, where $f_3(X, Y) = X$ and $f_4(X, Y) = 2Y^3 - 1$. The leading monomials are $\text{LM}(f_1) = X^2$, $\text{LM}(f_2) = XY$, $\text{LM}(f_3) = X$, and $\text{LM}(f_4) = Y^3$. The first two are divisible by the third. Therefore $\{X, Y^3 - \frac{1}{2}\}$ is the corresponding minimal Gröbner basis.

Unfortunately an ideal can have more than one minimal Gröbner basis, as is shown in Problem 17 at the end of the chapter. A Gröbner basis $\{g_1, \dots, g_s\}$ of an ideal I is said to be **reduced** if it is minimal and if for each i, no monomial appearing in g_i with nonzero coefficient is divisible by $\mathrm{LM}(g_j)$ for some $j \neq i$.

Theorem 8.28 (uniqueness of reduced Gröbner basis). If I is a nonzero ideal in $K[X_1, \dots, X_n]$, then I has a unique reduced Gröbner basis, and this can be obtained algorithmically starting from any minimal Gröbner basis.

PROOF OF UNIQUENESS. Let $\{g_1, \dots, g_s\}$ be any Gröbner basis. Since $\mathrm{LT}(I) = \big(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\big)$, Lemma 8.17 shows that any $\mathrm{LM}(f)$ for $f \in I$ is divisible by $\mathrm{LM}(g_j)$ for some j. If $\{h_1, \dots, h_t\}$ is a second Gröbner basis, then this argument shows that each $\mathrm{LM}(h_i)$ is divisible by some $\mathrm{LM}(g_j)$. Turned around, the argument shows that $\mathrm{LM}(g_j)$ is divisible by some $\mathrm{LM}(h_k)$. Since $\{h_1, \dots, h_t\}$ is assumed minimal, $\mathrm{LM}(h_k)$ cannot be divisible by $\mathrm{LM}(h_i)$ if $i \neq k$. Thus $\mathrm{LM}(h_i) = \mathrm{LM}(h_k)$, and these equal $\mathrm{LM}(g_j)$. Then it follows that $s = t$ and that we may enumerate any two minimal Gröbner bases in such a way that the leading monomial of the i^{th} member of each basis is the same for each i with $1 \leq i \leq s$.

With this normalization in place, let us show that $g_i = h_i$. To do so, we expand $g_i - h_i$ as $g_i - h_i = \sum_{j=1}^{s} a_j h_j$ with $\mathrm{LM}(g_i - h_i) = \max_j \mathrm{LM}(a_j h_j)$ in accordance with (b) of Theorem 8.23. Choose k such that the maximum on the right side is attained at k, i.e., such that

$$\mathrm{LM}(a_k)\,\mathrm{LM}(h_k) = \mathrm{LM}(g_i - h_i). \qquad (*)$$

Arguing by contradiction, suppose that the right side of $(*)$ is nonzero. Then it must be a monomial occurring in either g_i or h_i. Since the two Gröbner bases are reduced, no monomial occurring in g_i is divisible by $\mathrm{LM}(g_k) = \mathrm{LM}(h_k)$ if $k \neq i$, and similarly for monomials occurring in h_i. We conclude that $k = i$ and that $\mathrm{LM}(h_i) = \mathrm{LM}(g_i - h_i)$. But this is impossible by Proposition 8.18 if $g_i - h_i \neq 0$, since $\mathrm{LM}(g_i) = \mathrm{LM}(h_i)$ and $\mathrm{LC}(g_i) = \mathrm{LC}(h_i) = 1$. Therefore the right side of $(*)$ is 0, and $g_i = h_i$. □

PROOF OF EXISTENCE. Let $\{g_1, \dots, g_s\}$ be a minimal Gröbner basis of I. As was shown in the proof of uniqueness, the leading monomials $\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)$ are independent of the choice of the actual minimal basis. Looking at the definition of "reduced," we see therefore that the property of being reduced is a property of each member g_i of the basis separately. That is, it is meaningful to say that g_i is reduced if no monomial appearing in g_i with nonzero coefficient is divisible by $\mathrm{LM}(g_j)$ for some $j \neq i$. We shall show how to replace g_i by an element g_i' with the same leading monomial in such a way that the new set is still a Gröbner basis and g_i' is reduced, and then the proof will be complete. There is no loss of generality in taking $i = 1$.

Applying the generalized division algorithm (Proposition 8.20), we write

$$g_1 = \sum_{j=2}^{s} a_j g_j + r \tag{$**$}$$

in such a way that

$$\mathrm{LM}(g_1) = \max_{2 \le j \le s} \mathrm{LM}(a_j g_j) \tag{$\dagger$}$$

and that no monomial appearing in r with nonzero coefficient is divisible by $\mathrm{LM}(g_j)$ for any $j \ge 2$. If we define g_1' to be this element r, then the element g_1' is reduced in the above sense, and the only question is whether $\{g_1', g_2, \dots, g_s\}$ is a Gröbner basis. Since $\{g_1, \dots, g_s\}$ is minimal, $\mathrm{LM}(g_1)$ is not divisible by any $\mathrm{LM}(g_j)$ for $j \ge 2$. Consequently $\mathrm{LM}(g_1)$ appears with nonzero coefficient on the left side of $(**)$, and it does not appear in any of the terms $a_j g_j$ with nonzero coefficient on the right side. Consequently it appears in $r = g_1'$, and $\mathrm{LM}(g_1) \le \mathrm{LM}(g_1')$. On the other hand, the equality $(\dagger)$ implies that $\mathrm{LM}(g_1') \le \mathrm{LM}(g_1)$. Therefore $\mathrm{LM}(g_1) = \mathrm{LM}(g_1')$, and $\mathrm{LT}(I) = \big(\mathrm{LT}(g_1), \mathrm{LT}(g_2) \dots, \mathrm{LT}(g_s)\big) = \big(\mathrm{LT}(g_1'), \mathrm{LT}(g_2) \dots, \mathrm{LT}(g_s)\big)$. Consequently $\{g_1', g_2, \dots, g_s\}$ is a Gröbner basis by definition. □

Corollary 8.29 (solution of the ideal-equality problem). Let I and J be two nonzero ideals in $K[X_1, \dots, X_n]$ specified in terms of finite sets of generators. Then $I = J$ if and only if the reduced Gröbner bases of I and J relative to a single monomial ordering are the same.

REMARK. As with the solution of problems listed in Corollaries 8.25 and 8.26, the desired end is independent of the monomial ordering, and in practice one might just as well start from a monomial ordering for which the computation of Gröbner bases is relatively easy.

PROOF. This result is immediate from Corollary 8.24 (constructive existence of Gröbner bases) and Theorem 8.28. □

10. Simultaneous Systems of Polynomial Equations

In this section we combine our techniques concerning the resultant and Gröbner bases to attack the original problem discussed in Section 1, that of solving systems of simultaneous polynomial equations in several variables. Our interest ultimately will be in the case that the underlying field is algebraically closed.

Corollary 8.26 and the Nullstellensatz already combine to give a criterion for such a system to have no solutions: We regard the system as the zero locus of an ideal, and we calculate a Gröbner basis for the ideal. Then the system has no