$P_i < P_j$. In Exercise 28, we ask you to show by a counterexample that $P_i < P_j$ does not imply that P_i divides P_j.

Properties for an Ordering of Power Products

1. $1 < P$ for all power products $P \neq 1$.
2. For any two power products P_i and P_j, exactly one of $P_i < P_j, P_i = P_j, P_j < P_i$ holds.
3. If $P_i < P_j$ and $P_j < P_k$, then $P_i < P_k$.
4. If $P_i < P_j$, then $PP_i < PP_j$ for any power product P.

It can also be shown that these properties guarantee that any step-by-step process for modifying a finite ideal basis that does not increase the size of any maximal power product in a basis element and replaces at least one by something smaller at each step will terminate in a finite number of steps.

In $F[x]$ with x the only indeterminate, there is only one power product ordering, for by Property 1, we must have $1 < x$. Multiplying repeatedly by x and using Property 4, we have $x < x^2, x^2 < x^3$, etc. Property 3 then shows that $1 < x < x^2 < x^3 < \cdots$ is the only possible order. Notice that in Example 37.9, we modified a basis by replacing basis polynomials by polynomials containing smaller power products.

There are a number of possible orderings for power products in $F[\mathbf{x}]$ with n indeterminates. We present just one, the *lexicographical order* (denoted by "lex"). In lex, we define

$$x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n} < x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n} \tag{2}$$

if and only if $s_i < t_i$ for the first subscript i, reading from left to right, such that $s_i \neq t_i$. Thus in $F[x, y]$, if we write power products in the order $x^n y^m$, we have $y = x^0y^1 < x^1y^0 = x$ and $xy < xy^2$. Using lex, the order of n indeterminates is given by $1 < x_n < x_{n-1} < \cdots < x_2 < x_1$. Our reduction in Example 37.8, where we first got rid of all "big" x's that we could and then the "smaller" y's, corresponded to the lex order $z < y < x$, that is, to writing all power products in the $x^m y^n z^s$ order. For the two-indeterminate case with $y < x$, the total lex term order schematically is

$$1 < y < y^2 < y^3 \cdots < x < xy < xy^2 < xy^3 < \cdots < x^2 < x^2y < x^2y^2 < \cdots .$$

In all the examples that follow we will use lexicographic ordering using a specified ordering of the indeterminates.

An ordering of power products P induces an obvious ordering of terms aP of a polynomial in $F[\mathbf{x}]$, which we will refer to as a **term order.** From now on, given an ordering of power products, we consider every polynomial f in $F[\mathbf{x}]$ to be written in decreasing order of terms, so that the leading (first) term has the highest order. We denote by $\mathrm{lt}(f)$ the leading term of f and by $\mathrm{lp}(f)$ the power product of the leading term. If f and g are polynomials in $F[\mathbf{x}]$ such that $\mathrm{lp}(g)$ divides $\mathrm{lp}(f)$, then we can execute a division of f by g, as illustrated by the linear and one-indeterminate cases, in Section 37 to obtain $f(\mathbf{x}) = g(\mathbf{x})q(\mathbf{x}) + r(\mathbf{x})$ where $\mathrm{lp}(r) < \mathrm{lp}(f)$. Note that we did not say that $\mathrm{lp}(r) < \mathrm{lp}(g)$. We illustrate with an example.

38.1 Example By division, reduce the basis $\{xy^2, y^2 - y\}$ for the ideal $I = \langle xy^2, y^2 - y\rangle$ in $\mathbb{R}[x, y]$ to one with smaller maximum term size, assuming the order lex with $y < x$.

Solution We see that y^2 divides xy^2 and compute

$$\begin{array}{r|l} & x \\ \hline y^2 - y & xy^2 \\ & xy^2 - xy \\ \hline & xy \end{array}$$

Because y^2 does not divide xy, we cannot continue the division. Note that $1\mathrm{p}(xy) = xy$ is not less than $1\mathrm{p}(y^2 - y) = y^2$. However, we do have $1\mathrm{p}(xy) < 1\mathrm{p}(xy^2)$. Our new basis for I is $\{xy, y^2 - y\}$. ▲

When dealing with more than one indeterminate, it is often easier to perform basis reduction by multiplying a basis polynomial $g(\mathbf{x})$ by a polynomial $-q(\mathbf{x})$ and adding it to a polynomial $f(\mathbf{x})$ to obtain $r(\mathbf{x})$, as we perform matrix reduction in linear algebra, rather than writing out the division display as we did in the preceding example. Starting with basis polynomials xy^2 and $y^2 - y$, we can reduce the xy^2 by multiplying $y^2 - y$ by $-x$ and adding the resulting $-xy^2 + xy$ to xy^2, obtaining the replacement xy for xy^2. We can do that in our head, and write down the result directly.

Referring again to Example 38.1, it will follow from what we state later that given any polynomial $f(x, y) = c_1(x, y)(xy) + c_2(x, y)(y^2 - y)$ in $\langle xy, y^2 - y\rangle$, either xy or y^2 will divide $1\mathrm{p}(f)$. (See Exercise 32.) This illustrates the defining property of a *Gröbner basis*.

38.2 Definition A set $\{g_1, g_2, \cdots, g_r\}$ of nonzero polynomials in $F[x_1, x_2, \cdots, x_n]$, with term ordering $<$, is a **Gröbner basis** for the ideal $I = \langle g_1, g_2, \cdots, g_r\rangle$ if and only if, for each nonzero $f \in I$, there exists some i where $1 \leq i \leq r$ such that $1\mathrm{p}(g_i)$ divides $1\mathrm{p}(f)$. ■

While we have illustrated the computation of a Gröbner basis from a given basis for an ideal in Examples 37.8, 37.9, and 38.1, we have not given a specific algorithm. We refer the reader to Adams and Loustaunau [23]. The method consists of multiplying some polynomial in the basis by any polynomial in $F[\mathbf{x}]$ and adding the result to another polynomial in the basis in a manner that reduces the size of power products. In our illustrations, we have treated the case involving division of $f(\mathbf{x})$ by $g(\mathbf{x})$ where $1\mathrm{p}(g)$ divides $1\mathrm{p}(f)$, but we can also use the process if $1\mathrm{p}(g)$ only divides some other power product in f. For example, if two elements in a basis are $xy - y^3$ and $y^2 - 1$, we can multiply $y^2 - 1$ by y and add it to $xy - y^3$, reducing $xy - y^3$ to $xy - y$. Theorem 37.7 shows that this is a valid computation.

You may wonder how any basis $\{g_1, g_2, \cdots, g_r\}$ can fail to be a Gröbner basis for $I = \langle g_1, g_2, \cdots, g_r\rangle$ because, when we form an element $c_1g_1 + c_2g_2 + \cdots + c_rg_r$ in I, we see that $1\mathrm{p}(g_i)$ is a divisor of $1\mathrm{p}(c_ig_i)$ for $i = 1, 2, \cdots, r$. However, cancellation of power products can occur in the addition. We illustrate with an example.

38.3 Example Consider the ideal $I = \langle x^2y - 2, xy^2 - y\rangle$ in $\mathbb{R}[x, y]$. The polynomials in the basis shown cannot be reduced further. However, the ideal I contains $y(x^2y - 2) - x(xy^2 - y) = xy - 2y$, whose leading power product xy is not divisible by either of the leading power products x^2y or xy^2 of the given basis. Thus $\{x^2y - 2, xy^2 - y\}$ is not a Gröbner basis for I, according to Definition 38.2. ▲

When we run into a situation like that in Example 38.3, we realize that a Gröbner basis must contain some polynomial with a smaller leading power product than those in the given basis. Let f and g be polynomials in the given basis. Just as we did in Example 38.3, we can multiply f and g by as small power products as possible so that the resulting two leading power products will be the same, the *least common multiple*

(lcm) of 1p(f) and 1p(g), and then subtract or add with suitable coefficients from F so cancellation results. We denote a polynomial formed in this fashion by $S(f, g)$. We state without proof a theorem that can be used to test whether a basis is a Gröbner basis.

38.4 Theorem A basis $G = \{g_1, g_2, \cdots, g_r\}$ is a Gröbner basis for the ideal $\langle g_1, g_2, \cdots, g_r\rangle$ if and only if, for all $i \neq j$, the polynomial $S(g_i, g_j)$ can be reduced to zero by repeatedly dividing remainders by elements of G, as in the division algorithm.

As we mentioned before, we may prefer to think of reducing $S(g_i, g_j)$ by a sequence of operations consisting of adding (or subtracting) multiples of polynomials in G, rather than writing out division.

We can now indicate how we can obtain a Gröbner basis from a given basis. First, reduce the polynomials in the basis as far as possible among themselves. Then choose polynomials g_i and g_j in the basis, and form the polynomial $S(g_i, g_j)$. See if $S(g_i, g_j)$ can be reduced to zero as just described. If so, choose a different pair of polynomials, and repeat the procedure with them. If $S(g_i, g_j)$ cannot be reduced to zero as described above, augment the given basis with this $S(g_i, g_j)$, and start all over, reducing this basis as much as possible. By Theorem 38.4, when every polynomial $S(g_i, g_j)$ for all $i \neq j$ can be reduced to zero using polynomials from the latest basis, we have arrived at a Gröbner basis. We conclude with a continuation of Example 38.3.

38.5 Example Continuing Example 38.3, let $g_1 = x^2y - 2$, $g_2 = xy^2 - y$, and $I = \langle g_1, g_2\rangle$ in $\mathbb{R}^2$. In Example 38.3, we obtained the polynomial $S(g_1, g_2) = xy - 2y$, which cannot be reduced to zero using g_1 and g_2. We now reduce the basis $\{x^2y - 2, xy^2 - y, xy - 2y\}$, indicating each step.

$\{x^2y - 2, xy^2 - y, xy - 2y\}$	augmented basis
$\{2xy - 2, xy^2 - y, xy - 2y\}$	by adding $(-x)$ (third) to first
$\{2xy - 2, 2y^2 - y, xy - 2y\}$	by adding $(-y)$ (third) to second
$\{4y - 2, 2y^2 - y, xy - 2y\}$	by adding (-2) (third) to first
$\{4y - 2, 0, xy - 2y\}$	by adding $(-\frac{y}{2})$ (first) to second
$\{4y - 2, 0, \frac{1}{2}x - 2y\}$	by adding $(-\frac{x}{4})$ (first) to third
$\{4y - 2, 0, \frac{1}{2}x - 1\}$	by adding $(\frac{1}{2})$ (first) to third

Clearly, $\{y - \frac{1}{2}, x - 2\}$ is a Gröbner basis. Note that if $f = y - \frac{1}{2}$ and $g = x - 2$, then $S(f, g) = xf - yg = (xy - \frac{x}{2}) - (xy - 2y) = -\frac{x}{2} + 2y$, which can readily be reduced to zero by adding $\frac{1}{2}(x - 2)$ and $-2(y - \frac{1}{2})$.

From the Gröbner basis, we see that the algebraic variety $V(I)$ contains only one point, $(2, \frac{1}{2})$, in $\mathbb{R}^2$. ▲

Applications

Here we give a simple example of how a Gröbner basis can be used to derive a geometric formula.

38.6 Example Using a Gröbner basis, derive the standard formula for a parabola.

Solution Recall that a parabola is the set of all points in the plane that are equidistant from a fixed line (directrix) and a fixed point (focus). In standard form, the directrix is the line $y = -p$ and the focus is the point $(0, p)$ where $p > 0$. The algebraic variety defined by the ideal $\langle x^2 + (y - p)^2 - d^2, y + p - d\rangle$ gives the set of all points $(x_0, y_0, p_0, d_0) \in \mathbb{R}^4$