Examples

(1) The ellipse $2x^2 + 2xy + y^2 - 2x - 2y = 0$ intersects the circle $x^2 + y^2 = 1$ in two points. To find them we compute a Gröbner basis for the ideal $I = (2x^2 + 2xy + y^2 - 2x - 2y, x^2 + y^2 - 1) \subset \mathbb{R}[x, y]$ using the lexicographic monomial order $x > y$ to eliminate x, obtaining $g_1 = 2x + y^2 + 5y^3 - 2$ and $g_2 = 5y^4 - 4y^3$. Hence $5y^4 = 4y^3$ and $y = 0$ or $y = 4/5$. Substituting these values into $g_1 = 0$ and solving for x we find the two intersection points are $(1, 0)$ and $(-3/5, 4/5)$.

Instead using the lexicographic monomial order $y > x$ to eliminate y results in the Gröbner basis $\{y^2 + x^2 - 1, 2yx - 2y + x^2 - 2x + 1, 5x^3 - 7x^2 - x + 3\}$. Then $5x^3 - 7x^2 - x + 3 = (x - 1)^2(5x + 3)$ shows that x is 1 or $-3/5$ and we obtain the same solutions as before, although with more effort.

(2) In the previous example the solutions could also have been found by elementary means. Consider now the solutions in $\mathbb{C}$ to the system of two equations

$$x^3 - 2xy + y^3 = 0 \quad \text{and} \quad x^5 - 2x^2y^2 + y^5 = 0.$$

Computing a Gröbner basis for the ideal generated by $f_1 = x^3 - 2xy + y^3$ and $f_2 = x^5 - 2x^2y^2 + y^5$ with respect to the lexicographic monomial order $x > y$ we obtain the basis

$$g_1 = x^3 - 2xy + y^3$$
$$g_2 = 200xy^2 + 193y^9 + 158y^8 - 45y^7 - 456y^6 + 50y^5 - 100y^4$$
$$g_3 = y^{10} - y^8 - 2y^7 + 2y^6.$$

Any solution to our original equations would satisfy $g_1 = g_2 = g_3 = 0$. Since $g_3 = y^6(y - 1)^2(y^2 + 2y + 2)$, we have $y = 0$, $y = 1$ or $y = -1 \pm i$. Since $g_1(x, 0) = x^3$ and $g_2(x, 0) = 0$, we see that $(0, 0)$ is the only solution with $y = 0$. Since $g_1(x, 1) = x^3 - 2x + 1$ and $g_2(x, 1) = 200(x - 1)$ have only $x = 1$ as a common zero, the only solution with $y = 1$ is $(1, 1)$. Finally,

$$g_1(x, -1 \pm i) = x^3 + (2 \mp 2i)x + (2 \pm 2i)$$
$$g_2(x, -1 \pm i) = -400i(x + 1 \pm i),$$

and a quick check shows the common zero $x = -1 \mp i$ when $y = -1 \pm i$, respectively. Hence, there are precisely four solutions to the original pair of equations, namely

$$(x, y) = (0, 0), \quad (1, 1), \quad (-1 + i, -1 - i), \quad \text{or} \quad (-1 - i, -1 + i).$$

(3) Consider the solutions in $\mathbb{C}$ to the system of equations

$$x + y + z = 1$$
$$x^2 + y^2 + z^2 = 2$$
$$x^3 + y^3 + z^3 = 3.$$

The reduced Gröbner basis with respect to the lexicographic ordering $x > y > z$ is

$$\{x + y + z - 1, \ y^2 + yz - y + z^2 - z - (1/2), \ z^3 - z^2 - (1/2)z - (1/6)\}$$

and so z is a root of the polynomial $t^3 - t^2 - (1/2)t - (1/6)$ (by symmetry, also x and y are roots of this same polynomial). For each of the three roots of this polynomial, there are two values of y and one corresponding value of x making the first two polynomials in the Gröbner basis equal to 0. The resulting six solutions are quickly checked to be the three distinct roots of the polynomial $t^3 - t^2 - (1/2)t - (1/6)$ (which is irreducible over $\mathbb{Q}$) in some order.

As the previous examples show, the study of solutions to systems of polynomial equations $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ is intimately related to the study of the ideal $I = (f_1, f_2, \ldots, f_m)$ the polynomials generate in $F[x_1, \ldots, x_n]$. This fundamental connection is the starting point for the important and active branch of mathematics called "algebraic geometry", introduced in Chapter 15, where additional applications of Gröbner bases are given.

We close this section by showing how to compute the basic set-theoretic operations of sums, products and intersections of ideals in polynomial rings. Suppose $I = (f_1, \ldots, f_s)$ and $J = (h_1, \ldots, h_t)$ are two ideals in $F[x_1, \ldots, x_n]$. Then $I + J = (f_1, \ldots, f_s, h_1, \ldots, h_t)$ and $IJ = (f_1h_1, \ldots, f_ih_j, \ldots, f_sh_t)$. The following proposition shows how to compute the intersection of any two ideals.

Proposition 30. If I and J are any two ideals in $F[x_1, \ldots, x_n]$ then $tI + (1 - t)J$ is an ideal in $F[t, x_1, \ldots, x_n]$ and $I \cap J = (tI + (1 - t)J) \cap F[x_1, \ldots, x_n]$. In particular, $I \cap J$ is the first elimination ideal of $tI + (1 - t)J$ with respect to the ordering $t > x_1 > \cdots > x_n$.

Proof: First, tI and $(1-t)J$ are clearly ideals in $F[x_1, \ldots, x_n, t]$, so also their sum $tI + (1-t)J$ is an ideal in $F[x_1, \ldots, x_n, t]$. If $f \in I \cap J$, then $f = tf + (1-t)f$ shows $I \cap J \subseteq (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$. Conversely, suppose $f = tf_1 + (1-t)f_2$ is an element of $F[x_1, \ldots, x_n]$, where $f_1 \in I$ and $f_2 \in J$. Then $t(f_1 - f_2) = f - f_2 \in F[x_1, \ldots, x_n]$ shows that $f_1 - f_2 = 0$ and $f = f_2$, so $f = f_1 = f_2 \in I \cap J$. Since $I \cap J = (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$, $I \cap J$ is the first elimination ideal of $tI + (1-t)J$ with respect to the ordering $t > x_1 > \cdots > x_n$.

We have $tI + (1-t)J = (tf_1, \ldots, tf_s, (1-t)h_1, \ldots, (1-t)h_t)$ if $I = (f_1, \ldots, f_s)$ and $J = (h_1, \ldots, h_t)$. By Proposition 29, the elements not involving t in a Gröbner basis for this ideal in $F[t, x_1, \ldots, x_n]$, computed for the lexicographic monomial ordering $t > x_1 > \cdots > x_n$, give a Gröbner basis for the ideal $I \cap J$ in $F[x_1, \ldots, x_n]$.

Example

Let $I = (x, y)^2 = (x^2, xy, y^2)$ and let $J = (x)$. For the lexicographic monomial ordering $t > x > y$ the reduced Gröbner basis for $tI + (1-t)J$ in $F[t, x, y]$ is $\{tx - x, ty^2, x^2, xy\}$ and so $I \cap J = (x^2, xy)$.

EXERCISES

1. Suppose I is an ideal in $F[x_1, \ldots, x_n]$ generated by a (possibly infinite) set $\mathcal{S}$ of polynomials. Prove that a finite subset of the polynomials in $\mathcal{S}$ suffice to generate I. [Use Theorem 21 to write $I = (f_1, \ldots, f_m)$ and then write each $f_i \in I$ using polynomials in $\mathcal{S}$.]
2. Let $\geq$ be any monomial ordering.
   (a) Prove that $LT(fg) = LT(f)LT(g)$ and $\partial(fg) = \partial(f) + \partial(g)$ for any nonzero polynomials f and g.
   (b) Prove that $\partial(f + g) \leq \max(\partial(f), \partial(g))$ with equality if $\partial(f) \neq \partial(g)$.

(c) Prove that $m \geq 1$ for every monomial m.
(d) Prove that if m_1 divides m_2 then $m_2 \geq m_1$. Deduce that the leading term of a polynomial does not divide any of its lower order terms.

3. Prove that if $\geq$ is any total or partial ordering on a nonempty set then the following are equivalent:
(i) Every nonempty subset contains a minimum element.
(ii) There is no infinite strictly decreasing sequence $a_1 > a_2 > a_3 > \cdots$ (this is called the *descending chain condition* or *D.C.C.*).
Deduce that General Polynomial Division always terminates in finitely many steps.

4. Let $\geq$ be a monomial ordering, and for monomials m_1, m_2 define $m_1 \geq_g m_2$ if either $\deg m_1 > \deg m_2$, or $\deg m_1 = \deg m_2$ and $m_1 \geq m_2$.
(a) Prove that $\geq_g$ is also a monomial ordering. (The relation $\geq_g$ is called the *grading* of $\geq$. An ordering in which the most important criterion for comparison is degree is sometimes called a *graded* or a *degree* ordering, so this exercise gives a method for constructing graded orderings.)
(b) The grading of the lexicographic ordering $x_1 > \cdots > x_n$ is called the *grlex* monomial ordering. Show that $x_2^4 > x_1^2x_2 > x_1x_2^2 > x_2^2 > x_1$ with respect to the grlex ordering and $x_1^2x_2 > x_1x_2^2 > x_1 > x_2^4 > x_2^2$ with respect to the lexicographic ordering.

5. The *grevlex* monomial ordering is defined by first choosing an ordering of the variables $\{x_1, x_2, \ldots, x_n\}$, then defining $m_1 \geq m_2$ for monomials m_1, m_2 if either $\deg m_1 > \deg m_2$ or $\deg m_1 = \deg m_2$ and the first exponent of $x_n, x_{n-1}, \ldots, x_1$ (in that order) where m_1 and m_2 differ is *smaller* in m_1.
(a) Prove that grevlex is a monomial ordering that satisfies $x_1 > x_2 > \cdots > x_n$.
(b) Prove that the grevlex ordering on $F[x_1, x_2]$ with respect to $\{x_1, x_2\}$ is the graded lexicographic ordering with $x_1 > x_2$, but that the grevlex ordering on $F[x_1, x_2, x_3]$ is not the grading of any lexicographic ordering.
(c) Show that $x_1x_2^2x_3 > x_1^2x_3^2 > x_2^2x_3^2 > x_2x_3^2 > x_1x_2 > x_2^2 > x_1x_3 > x_3^2 > x_1 > x_2$ for the grevlex monomial ordering with respect to $\{x_1, x_2, x_3\}$.

6. Show that $x^3y > x^3z^2 > x^3z > x^2y^2z > x^2y > xz^2 > y^2z^2 > y^2z$ with respect to the lexicographic monomial ordering $x > y > z$. Show that for the corresponding grlex monomial ordering $x^3z^2 > x^2y^2z > x^3y > x^3z > y^2z^2 > x^2y > xz^2 > y^2z$, and that $x^2y^2z > x^3z^2 > x^3y > x^3z > y^2z^2 > x^2y > y^2z > xz^2$ for the grevlex monomial ordering with respect to $\{x, y, z\}$.

7. Order the monomials $x^2z, x^2y^2z, xy^2z, x^3y, x^3z^2, x^2, x^2yz^2, x^2z^2$ for the lexicographic monomial ordering $x > y > z$, for the corresponding grlex monomial order, and for the grevlex monomial ordering with respect to $\{x, y, z\}$.

8. Show there are $n!$ distinct lexicographic monomial orderings on $F[x_1, \ldots, x_n]$. Show similarly that there are $n!$ distinct grlex and grevlex monomial orderings.

9. It can be shown that any monomial ordering on $F[x_1, \ldots, x_n]$ may be obtained as follows. For $k \leq n$ let $v_1, v_2, \ldots, v_k$ be nonzero vectors in Euclidean n-space, $\mathbb{R}^n$, that are pairwise orthogonal: $v_i \cdot v_j = 0$ for all $i \neq j$, where $\cdot$ is the usual dot product, and suppose also that all the coordinates of v_1 are nonnegative. Define an order, $\geq$, on monomials by $m_1 > m_2$ if and only if for some $t \leq k$ we have $v_i \cdot \partial(m_1) = v_i \cdot \partial(m_2)$ for all $i \in \{1, 2, \ldots, t-1\}$ and $v_t \cdot \partial(m_1) > v_t \cdot \partial(m_2)$.
(a) Let $k = n$ and let $v_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the i^{th} position. Show that $\geq$ defines the lexicographic order with $x_1 > x_2 > \cdots > x_n$.
(b) Let $k = n$ and define $v_1 = (1, 1, \ldots, 1)$ and $v_i = (1, 1, \ldots, 1, -n+i-1, 0, \ldots, 0)$,