For (2), note that the ideal $LT(I)$ of leading terms of any ideal I is a monomial ideal generated by all the leading terms of the polynomials in I. By Exercise 1 a finite number of those leading terms suffice to generate $LT(I)$, say $LT(I) = (LT(h_1), \ldots, LT(h_k))$ for some $h_1, \ldots, h_k \in I$. By (1), the polynomials $h_1, \ldots, h_k$ are a Gröbner basis of I, completing the proof.

Proposition 24 proves that Gröbner bases always exist. We next prove a criterion that determines whether a given set of generators of an ideal I is a Gröbner basis, which we then use to provide an algorithm to find a Gröbner basis. The basic idea is very simple: additional elements in $LT(I)$ can arise by taking linear combinations of generators that cancel leading terms, as we saw in taking $yf_1 - xf_2$ in the first example in this section. We shall see that obtaining new leading terms from generators in this simple manner is the only obstruction to a set of generators being a Gröbner basis.

In general, if f_1, f_2 are two polynomials in $F[x_1, \ldots, x_n]$ and M is the monic least common multiple of the monomial terms $LT(f_1)$ and $LT(f_2)$ then we can cancel the leading terms by taking the difference

$$S(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2. \tag{9.1}$$

The next lemma shows that these elementary linear combinations account for all cancellation in leading terms of polynomials of the same multidegree.

Lemma 25. Suppose $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ are polynomials with the same multidegree α and that the linear combination $h = a_1 f_1 + \cdots + a_m f_m$ with constants $a_i \in F$ has strictly smaller multidegree. Then

$$h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i), \quad \text{for some constants } b_i \in F.$$

Proof: Write $f_i = c_i f_i'$ where $c_i \in F$ and f_i' is a monic polynomial of multidegree α. We have

$$h = \sum a_i c_i f_i' = a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \cdots$$
$$+ (a_1 c_1 + \cdots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') + (a_1 c_1 + \cdots + a_m c_m) f_m'.$$

Note that $f_{i-1}' - f_i' = S(f_{i-1}, f_i)$. Then since h and each $f_{i-1}' - f_i'$ has multidegree strictly smaller than α, we have $a_1 c_1 + \cdots + a_m c_m = 0$, so the last term on the right hand side is 0 and the lemma follows.

The next proposition shows that a set of generators $g_1, \ldots, g_m$ is a Gröbner basis if there are no new leading terms among the differences $S(g_i, g_j)$ not already accounted for by the g_i. This result provides the principal ingredient in an algorithm to construct a Gröbner basis.

For a fixed monomial ordering on $R = F[x_1, \ldots, x_n]$ and ordered set of polynomials $G = \{g_1, \ldots, g_m\}$ in R, write $f \equiv r \bmod G$ if r is the remainder obtained by general polynomial division of $f \in R$ by $g_1, \ldots, g_m$ (in that order).

Proposition 26. *(Buchberger's Criterion)* Let $R = F[x_1, \ldots, x_n]$ and fix a monomial ordering on R. If $I = (g_1, \ldots, g_m)$ is a nonzero ideal in R, then $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if and only if $S(g_i, g_j) \equiv 0 \bmod G$ for $1 \leq i < j \leq m$.

Proof: If $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I, then $S(g_i, g_j) \equiv 0 \bmod G$ by Theorem 23 since each $S(g_i, g_j)$ is an element of I.

Suppose now that $S(g_i, g_j) \equiv 0 \bmod G$ for $1 \leq i < j \leq m$ and take any element $f \in I$. To see that G is a Gröbner basis we need to see that $(LT(g_1), \ldots, LT(g_m))$ contains $LT(f)$. Since $f \in I$, we can write $f = \sum_{i=1}^{m} h_i g_i$ for some polynomials $h_1, \ldots, h_m$. Such a representation is not unique. Among all such representations choose one for which the largest multidegree of any summand (i.e., $\max_{i=1,\ldots,m} \partial(h_i g_i)$) is minimal, say α. It is clear that the multidegree of f is no worse than the largest multidegree of all the summands $h_i g_i$, so $\partial(f) \leq \alpha$. Write

$$\begin{aligned} f = \sum_{i=1}^{m} h_i g_i &= \sum_{\partial(h_i g_i)=\alpha} h_i g_i + \sum_{\partial(h_i g_i)<\alpha} h_i g_i \\ &= \sum_{\partial(h_i g_i)=\alpha} LT(h_i) g_i + \sum_{\partial(h_i g_i)=\alpha} (h_i - LT(h_i)) g_i + \sum_{\partial(h_i g_i)<\alpha} h_i g_i. \end{aligned} \tag{9.2}$$

Suppose that $\partial(f) < \alpha$. Then since the multidegree of the second two sums is also strictly smaller than α it follows that the multidegree of the first sum is strictly smaller than α. If $a_i \in F$ denotes the constant coefficient of the monomial term $LT(h_i)$ then $LT(h_i) = a_i h_i'$ where h_i' is a monomial. We can apply Lemma 25 to $\sum a_i(h_i' g_i)$ to write the first sum above as $\sum b_i S(h_{i-1}' g_{i-1}, h_i' g_i)$ with $\partial(h_{i-1}' g_{i-1}) = \partial(h_i' g_i) = \alpha$. Let $\beta_{i-1,i}$ be the multidegree of the monic least common multiple of $LT(g_{i-1})$ and $LT(g_i)$. Then an easy computation shows that $S(h_{i-1}' g_{i-1}, h_i' g_i)$ is just $S(g_{i-1}, g_i)$ multiplied by the monomial of multidegree $\alpha - \beta_{i-1,i}$. The polynomial $S(g_{i-1}, g_i)$ has multidegree less than $\beta_{i-1,i}$ and, by assumption, $S(g_{i-1}, g_i) \equiv 0 \bmod G$. This means that after general polynomial division of $S(g_{i-1}, g_i)$ by $g_1, \ldots, g_m$, each $S(g_{i-1}, g_i)$ can be written as a sum $\sum q_j g_j$ with $\partial(q_j g_j) < \beta_{i-1,i}$. It follows that each $S(h_{i-1}' g_{i-1}, h_i' g_i)$ is a sum $\sum q_j' g_j$ with $\partial(q_j' g_j) < \alpha$. But then all the sums on the right hand side of equation (2) can be written as a sum of terms of the form $p_i g_i$ with polynomials p_i satisfying $\partial(p_i g_i) < \alpha$. This contradicts the minimality of α and shows that in fact $\partial(f) = \alpha$, i.e., the leading term of f has multidegree α.

If we now take the terms in equation (2) of multidegree α we see that

$$LT(f) = \sum_{\partial(h_i g_i)=\alpha} LT(h_i) LT(g_i),$$

so indeed $LT(f) \in (LT(g_1), \ldots, LT(g_m))$. It follows that $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis.

Buchberger's Algorithm

Buchberger's Criterion can be used to provide an algorithm to find a Gröbner basis for an ideal I, as follows. If $I = (g_1, \ldots, g_m)$ and each $S(g_i, g_j)$ leaves a remainder of 0 when divided by $G = \{g_1, \ldots, g_m\}$ using general polynomial division then G

is a Gröbner basis. Otherwise $S(g_i, g_j)$ has a nonzero remainder r. Increase G by appending the polynomial $g_{m+1} = r$: $G' = \{g_1, \ldots, g_m, g_{m+1}\}$ and begin again (note that this is again a set of generators for I since $g_{m+1} \in I$). It is not hard to check that this procedure terminates after a finite number of steps in a generating set G that satisfies Buchberger's Criterion, hence is a Gröbner basis for I (cf. Exercise 16). Note that once an $S(g_i, g_j)$ yields a remainder of 0 after division by the polynomials in G it also yields a remainder of 0 when additional polynomials are appended to G.

If $\{g_1, \ldots, g_m\}$ is a Gröbner basis for the ideal I and $LT(g_j)$ is divisible by $LT(g_i)$ for some $j \neq i$, then $LT(g_j)$ is not needed as a generator for $LT(I)$. By Proposition 24 we may therefore delete g_j and still retain a Gröbner basis for I. We may also assume without loss that the leading term of each g_i is monic. A Gröbner basis $\{g_1, \ldots, g_m\}$ for I where each $LT(g_i)$ is monic and where $LT(g_j)$ is not divisible by $LT(g_i)$ for $i \neq j$ is called a *minimal Gröbner basis*. While a minimal Gröbner basis is not unique, the number of elements and their leading terms are unique (cf. Exercise 15).

Examples

(1) Choose the lexicographic ordering $x > y$ on $F[x, y]$ and consider the ideal I generated by $f_1 = x^3y - xy^2 + 1$ and $f_2 = x^2y^2 - y^3 - 1$ as in Example 1 at the beginning of this section. To test whether $G = \{f_1, f_2\}$ is a Gröbner basis we compute $S(f_1, f_2) = yf_1 - xf_2 = x + y$, which is its own remainder when divided by $\{f_1, f_2\}$, so G is not a Gröbner basis for I. Set $f_3 = x + y$, and increase the generating set: $G' = \{f_1, f_2, f_3\}$. Now $S(f_1, f_2) \equiv 0 \bmod G'$, and a brief computation yields

$$S(f_1, f_3) = f_1 - x^2yf_3 = -x^2y^2 - xy^2 + 1 \equiv 0 \bmod G'$$

$$S(f_2, f_3) = f_2 - xy^2f_3 = -xy^3 - y^3 - 1 \equiv y^4 - y^3 - 1 \bmod G'.$$

Let $f_4 = y^4 - y^3 - 1$ and increase the generating set to $G'' = \{f_1, f_2, f_3, f_4\}$. The previous 0 remainder is still 0, and now $S(f_2, f_3) \equiv 0 \bmod G''$ by the choice of f_4. Some additional computation yields

$$S(f_1, f_4) \equiv S(f_2, f_4) \equiv S(f_3, f_4) \equiv 0 \bmod G''$$

and so $\{x^3y - xy^2 + 1, x^2y^2 - y^3 - 1, x + y, y^4 - y^3 - 1\}$ is a Gröbner basis for I. In particular, $LT(I)$ is generated by the leading terms of these four polynomials, so $LT(I) = (x^3y, x^2y^2, x, y^4) = (x, y^4)$, as previously mentioned. Then $x + y$ and $y^4 - y^3 - 1$ in I have leading terms generating $LT(I)$, so by Proposition 24, $\{x + y, y^4 - y^3 - 1\}$ gives a minimal Gröbner basis for I:

$$I = (x + y, y^4 - y^3 - 1).$$

This description of I is much simpler than $I = (x^3y - xy^2 + 1, x^2y^2 - y^3 - 1)$.

(2) Choose the lexicographic ordering $y > x$ on $F[x, y]$ and consider the ideal I in the previous example. In this case, $S(f_1, f_2)$ produces a remainder of $f_3 = -x - y$; then $S(f_1, f_3)$ produces a remainder of $f_4 = -x^4 - x^3 + 1$, and then all remainders are 0 with respect to the Gröbner basis $\{x^3y - xy^2 + 1, x^2y^2 - y^3 - 1, -x - y, -x^4 - x^3 + 1\}$. Here $LT(I) = (-xy^2, -y^3, -y, -x^4) = (y, x^4)$, as previously mentioned, and $\{x + y, x^4 + x^3 - 1\}$ gives a minimal Gröbner basis for I with respect to this ordering:

$$I = (x + y, x^4 + x^3 - 1),$$

a different simpler description of I.