We first use the leading terms of polynomials defined by a monomial ordering on $F[x_1, \ldots, x_n]$ to extend the one variable Division Algorithm to a noncanonical polynomial division in several variables. Recall that for polynomials in one variable, the usual Division Algorithm determines the quotient $q(x)$ and remainder $r(x)$ in the equation $f(x) = q(x)g(x) + r(x)$ by successively testing whether the leading term of the dividend $f(x)$ is divisible by the leading term of $g(x)$: if $LT(f) = a(x)LT(g)$, the monomial term $a(x)$ is added to the quotient and the process is iterated with $f(x)$ replaced by the dividend $f(x) - a(x)g(x)$, which is of smaller degree since the leading terms cancel (by the choice of $a(x)$). The process terminates when the leading term of the divisor $g(x)$ no longer divides the leading term of the dividend, leaving the remainder $r(x)$. We can extend this to division by a finite number of polynomials in several variables simply by allowing successive divisions, resulting in a remainder and several quotients, as follows.

General Polynomial Division

Fix a monomial ordering on $F[x_1, \ldots, x_n]$, and suppose $g_1, \ldots, g_m$ is a set of nonzero polynomials in $F[x_1, \ldots, x_n]$. If f is any polynomial in $F[x_1, \ldots, x_n]$, start with a set of quotients $q_1, \ldots, q_m$ and a remainder r initially all equal to 0 and successively test whether the leading term of the dividend f is divisible by the leading terms of the divisors $g_1, \ldots, g_m$, in that order. Then

i. If $LT(f)$ is divisible by $LT(g_i)$, say, $LT(f) = a_i LT(g_i)$, add a_i to the quotient q_i, replace f by the dividend $f - a_i g_i$ (a polynomial with lower order leading term), and reiterate the entire process.

ii. If the leading term of the dividend f is not divisible by any of the leading terms $LT(g_1), \ldots, LT(g_m)$, add the leading term of f to the remainder r, replace f by the dividend $f - LT(f)$ (i.e., remove the leading term of f), and reiterate the entire process.

The process terminates (cf. Exercise 3) when the dividend is 0 and results in a set of quotients $q_1, \ldots, q_m$ and a remainder r with

$$f = q_1 g_1 + \cdots + q_m g_m + r.$$

Each $q_i g_i$ has multidegree less than or equal to the multidegree of f and the remainder r has the property that no nonzero term in r is divisible by any of the leading terms $LT(g_1), \ldots, LT(g_m)$ (since only terms with this property are added to r in (ii)).

Examples

Fix the lexicographic ordering $x > y$ on $F[x, y]$.

(1) Suppose $f = x^3y^3 + 3x^2y^4$ and $g = xy^4$. The leading term of f is x^3y^3, which is not divisible by (the leading term of) g, so x^3y^3 is added to the remainder r (so now $r = x^3y^3$) and f is replaced by $f - LT(f) = 3x^2y^4$ and we start over. Since $3x^2y^4$ is divisible by $LT(g) = xy^4$, with quotient $a = 3x$, we add $3x$ to the quotient q (so $q = 3x$), and replace $3x^2y^4$ by $3x^2y^4 - aLT(g) = 0$, at which point the process terminates. The result is the quotient $q = 3x$ and remainder $r = x^3y^3$ and

$$x^3y^3 + 3x^2y^4 = f = qg + r = (3x)(xy^4) + x^3y^3.$$

Note that if we had terminated at the first step because the leading term of f is not divisible by the leading term of g (which terminates the Division Algorithm for polynomials in one variable), then we would have been left with a 'remainder' of f itself, even though 'more' of f is divisible by g. This is the reason for step 2 in the division process (which is not necessary for polynomials in one variable).

(2) Let $f = x^2+x-y^2+y$, and suppose $g_1 = xy+1$ and $g_2 = x+y$. In the first iteration, the leading term x^2 of f is not divisible by the leading term of g_1, but is divisible by the leading term of g_2, so the quotient q_2 is x and the dividend f is replaced by the dividend $f - xg_2 = -xy + x - y^2 + y$. In the second iteration, the leading term of $-xy + x - y^2 + y$ is divisible by $LT(g_1)$, with quotient -1, so $q_1 = -1$ and the dividend is replaced by $(-xy + x - y^2 + y) - (-1)g_1 = x - y^2 + y + 1$. In the third iteration, the leading term of $x - y^2 + y + 1$ is not divisible by the leading term of g_1, but is divisible by the leading term of g_2, with quotient 1, so 1 is added to q_2 (which is now $q_2 = x+1$) and the dividend becomes $(x-y^2+y+1)-(1)(g_2) = -y^2+1$. The leading term is now $-y^2$, which is not divisible by either $LT(g_1) = xy$ or $LT(g_2) = x$, so $-y^2$ is added to the remainder r (which is now $-y^2$) and the dividend becomes simply 1. Finally, 1 is not divisible by either $LT(g_1)$ or $LT(g_2)$, so is added to the remainder (so r is now $-y^2 + 1$), and the process terminates. The result is

$$q_1 = -1, \qquad q_2 = x + 1, \qquad r = -y^2 + 1 \quad \text{and}$$

$$\begin{aligned} f &= x^2 + x - y^2 + y = (-1)(xy + 1) + (x + 1)(x + y) + (-y^2 + 1) \\ &= q_1 g_1 + q_2 g_2 + r. \end{aligned}$$

(3) Let $f = x^2 + x - y^2 + y$ as in the previous example and interchange the divisors g_1 and g_2: $g_1 = x + y$ and $g_2 = xy + 1$. In this case an easy computation gives

$$q_1 = x - y + 1, \qquad q_2 = 0, \qquad r = 0 \quad \text{and}$$

$$f = x^2 + x - y^2 + y = (x - y + 1)(x + y) = q_1 g_1 + q_2 g_2 + r,$$

showing that the quotients q_i and the remainder r are in general not unique and depend on the order of the divisors $g_1, \dots, g_m$.

The computation in Example 3 shows that the polynomial $f = x^2 + x - y^2 + y$ is an element of the ideal $I = (x + y, xy + 1)$ since the remainder obtained in this case was 0 (in fact f is just a multiple of the first generator). In Example 2, however, the same polynomial resulted in a nonzero remainder $-y^2 + 1$ when divided by $xy + 1$ and $x + y$, and it was not at all clear from that computation that f was an element of I.

The next theorem shows that if we use a Gröbner basis for the ideal I then these difficulties do not arise: we obtain a *unique* remainder, which in turn can be used to determine whether a polynomial f is an element of the ideal I.

Theorem 23. Fix a monomial ordering on $R = F[x_1, \dots, x_n]$ and suppose $\{g_1, \dots, g_m\}$ is a Gröbner basis for the nonzero ideal I in R. Then

(1) Every polynomial $f \in R$ can be written uniquely in the form

$$f = f_I + r$$

where $f_I \in I$ and no nonzero monomial term of the 'remainder' r is divisible by any of the leading terms $LT(g_1), \dots, LT(g_m)$.

(2) Both f_I and r can be computed by general polynomial division by $g_1, \ldots, g_m$ and are independent of the order in which these polynomials are used in the division.

(3) The remainder r provides a unique representative for the coset of f in the quotient ring $F[x_1, \ldots, x_n]/I$. In particular, $f \in I$ if and only if $r = 0$.

Proof: Letting $f_I = \sum_{i=1}^m q_i g_i \in I$ in the general polynomial division of f by $g_1, \ldots, g_m$ immediately gives a decomposition $f = f_I + r$ for any generators $g_1, \ldots, g_m$. Suppose now that $\{g_1, \ldots, g_m\}$ is a Gröbner basis, and $f = f_I + r = f_I' + r'$. Then $r - r' = f_I' - f_I \in I$, so its leading term $LT(r - r')$ is an element of $LT(I)$, which is the ideal $(LT(g_1), \ldots, LT(g_m))$ since $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I. Every element in this ideal is a sum of multiples of the monomial terms $LT(g_1), \ldots, LT(g_m)$, so is a sum of terms each of which is divisible by one of the $LT(g_i)$. But both r and r', hence also $r - r'$, are sums of monomial terms none of which is divisible by $LT(g_1), \ldots, LT(g_m)$, which is a contradiction unless $r - r' = 0$. It follows that $r = r'$ is unique, hence so is $f_I = f - r$, which proves (1).

We have already seen that f_I and r can be computed algorithmically by polynomial division, and the uniqueness in (1) implies that r is independent of the order in which the polynomials $g_1, \ldots, g_m$ are used in the division. Similarly $f_I = \sum_{i=1}^m q_i g_i$ is uniquely determined (even though the individual quotients q_i are not in general unique), which gives (2).

The first statement in (3) is immediate from the uniqueness in (1). If $r = 0$, then $f = f_I \in I$. Conversely, if $f \in I$, then $f = f + 0$ together with the uniqueness of r implies that $r = 0$, and the final statement of the theorem follows.

As previously mentioned, the importance of Theorem 23, and one of the principal uses of Gröbner bases, is the uniqueness of the representative r, which allows effective computation in the quotient ring $F[x_1, \ldots, x_n]/I$.

We next prove that a set of polynomials in an ideal whose leading terms generate all the leading terms of an ideal is in fact a set of generators for the ideal itself (and so is a Gröbner basis—in some works this is taken as the definition of a Gröbner basis), and this shows in particular that a Gröbner basis always exists.

Proposition 24. Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and let I be a nonzero ideal in R.

(1) If $g_1, \ldots, g_m$ are any elements of I such that $LT(I) = (LT(g_1), \ldots, LT(g_m))$, then $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I.

(2) The ideal I has a Gröbner basis.

Proof: Suppose $g_1, \ldots, g_m \in I$ with $LT(I) = (LT(g_1), \ldots, LT(g_m))$. We need to see that $g_1, \ldots, g_m$ generate the ideal I. If $f \in I$, use general polynomial division to write $f = \sum_{i=1}^m q_i g_i + r$ where no nonzero term in the remainder r is divisible by any $LT(g_i)$. Since $f \in I$, also $r \in I$, which means $LT(r)$ is in $LT(I)$. But then $LT(r)$ would be divisible by one of $LT(g_1), \ldots, LT(g_m)$, which is a contradiction unless $r = 0$. Hence $f = \sum_{i=1}^m q_i g_i$ and $g_1, \ldots, g_m$ generate I, so are a Gröbner basis for I, which proves (1).