

Since a field is clearly Noetherian, Hilbert's Basis Theorem and induction immediately give:

**Corollary 22.** Every ideal in the polynomial ring  $F[x_1, x_2, \dots, x_n]$  with coefficients from a field  $F$  is finitely generated.

If  $I$  is an ideal in  $F[x_1, \dots, x_n]$  generated by a (possibly infinite) set  $\mathcal{S}$  of polynomials, Corollary 22 shows that  $I$  is finitely generated, and in fact  $I$  is generated by a finite number of the polynomials from the set  $\mathcal{S}$  (cf. Exercise 1).

As the proof of Hilbert's Basis Theorem shows, the collection of leading coefficients of the polynomials in an ideal  $I$  in  $R[x]$  forms an extremely useful ideal in  $R$  that can be used to understand  $I$ . This suggests studying “leading terms” in  $F[x_1, x_2, \dots, x_n]$  more generally (and somewhat more intrinsically). To do this we need to specify a total ordering on the monomials, since without some sort of ordering we cannot in general tell which is the “leading” term of a polynomial. We implicitly chose such an ordering in the inductive proof of Corollary 22—we first viewed a polynomial  $f$  as a polynomial in  $x_1$  with coefficients in  $R = F[x_2, \dots, x_n]$ , say, then viewed its “leading coefficient” in  $F[x_2, \dots, x_n]$  as a polynomial in  $x_2$  with coefficients in  $F[x_3, \dots, x_n]$ , etc. This is an example of a *lexicographic* monomial ordering on the polynomial ring  $F[x_1, \dots, x_n]$  which is defined by first declaring an ordering of the variables, for example  $x_1 > x_2 > \dots > x_n$  and then declaring that the monomial term  $Ax_1^{a_1}x_2^{a_2} \cdots x_n^{a_n}$  with exponents  $(a_1, a_2, \dots, a_n)$  has higher order than the monomial term  $Bx_1^{b_1}x_2^{b_2} \cdots x_n^{b_n}$  with exponents  $(b_1, b_2, \dots, b_n)$  if the first component where the  $n$ -tuples differ has  $a_i > b_i$ . This is analogous to the ordering used in a dictionary (hence the name), where the letter “a” comes before “b” which in turn comes before “c”, etc., and then “aardvark” comes before “abacus” (although the ‘word’  $a^2 = aa$  comes before  $a$  in the lexicographical order). Note that the ordering is only defined up to multiplication by units (elements of  $F^\times$ ) and that multiplying two monomials by the same nonzero monomial does not change their ordering. This can be formalized in general.

**Definition.** A *monomial ordering* is a well ordering “ $\geq$ ” on the set of monomials that satisfies  $mm_1 \geq mm_2$  whenever  $m_1 \geq m_2$  for monomials  $m, m_1, m_2$ . Equivalently, a monomial ordering may be specified by defining a well ordering on the  $n$ -tuples  $\alpha = (a_1, \dots, a_n) \in \mathbb{Z}^n$  of multidegrees of monomials  $Ax_1^{a_1} \cdots x_n^{a_n}$  that satisfies  $\alpha + \gamma \geq \beta + \gamma$  if  $\alpha \geq \beta$ .

It is easy to show for any monomial ordering that  $m \geq 1$  for every monomial  $m$  (cf. Exercise 2). It is not difficult to show, using Hilbert's Basis Theorem, that any total ordering on monomials which for every monomial  $m$  satisfies  $m \geq 1$  and  $mm_1 \geq mm_2$  whenever  $m_1 \geq m_2$ , is necessarily a well ordering (hence a monomial ordering)—this equivalent set of axioms for a monomial ordering may be easier to verify. For simplicity we shall limit the examples to the particularly easy and intuitive lexicographic ordering, but it is important to note that there are useful computational advantages to using other monomial orderings in practice. Some additional commonly used monomial orderings are introduced in the exercises.

As mentioned, once we have a monomial ordering we can define the leading term of a polynomial:

**Definition.** Fix a monomial ordering on the polynomial ring  $F[x_1, x_2, \dots, x_n]$ .

- (1) The *leading term* of a nonzero polynomial  $f$  in  $F[x_1, x_2, \dots, x_n]$ , denoted  $LT(f)$ , is the monomial term of maximal order in  $f$  and the leading term of  $f = 0$  is 0. Define the *multidegree* of  $f$ , denoted  $\partial(f)$ , to be the multidegree of the leading term of  $f$ .
- (2) If  $I$  is an ideal in  $F[x_1, x_2, \dots, x_n]$ , the *ideal of leading terms*, denoted  $LT(I)$ , is the ideal generated by the leading terms of all the elements in the ideal, i.e.,  $LT(I) = (LT(f) \mid f \in I)$ .

The leading term and the multidegree of a polynomial clearly depend on the choice of the ordering. For example  $LT(2xy + y^3) = 2xy$  with multidegree  $(1, 1)$  if  $x > y$ , but  $LT(2xy + y^3) = y^3$  with multidegree  $(0, 3)$  if  $y > x$ . In particular, the leading term of a polynomial need not be the term of largest total degree. Similarly, the ideal of leading terms  $LT(I)$  of an ideal  $I$  in general depends on the ordering used. Note also that the multidegree of a polynomial satisfies  $\partial(fg) = \partial f + \partial g$  when  $f$  and  $g$  are nonzero, and that in this case  $LT(fg) = LT(f) + LT(g)$  (cf. Exercise 2).

The ideal  $LT(I)$  is by definition generated by monomials. Such ideals are called *monomial ideals* and are typically much easier to work with than generic ideals. For example, a polynomial is contained in a monomial ideal if and only if each of its monomial terms is a multiple of one of the generators for the ideal (cf. Exercise 10).

It was important in the proof of Hilbert's Basis Theorem to have *all* of the leading terms of the ideal  $I$ . If  $I = (f_1, \dots, f_m)$ , then  $LT(I)$  contains the leading terms  $LT(f_1), \dots, LT(f_m)$  of the generators for  $I$  by definition. Since  $LT(I)$  is an ideal, it contains the ideal generated by these leading terms:

$$(LT(f_1), \dots, LT(f_m)) \subseteq LT(I).$$

The first of the following examples shows that the ideal  $LT(I)$  of leading terms can in general be strictly larger than the ideal generated just by the leading terms of some generators for  $I$ .

## Examples

- (1) Choose the lexicographic ordering  $x > y$  on  $F[x, y]$ . The leading terms of the polynomials  $f_1 = x^3y - xy^2 + 1$  and  $f_2 = x^2y^2 - y^3 - 1$  are  $LT(f_1) = x^3y$  (so the multidegree of  $f_1$  is  $\partial(f_1) = (3, 1)$ ) and  $LT(f_2) = x^2y^2$  (so  $\partial(f_2) = (2, 2)$ ). If  $I = (f_1, f_2)$  is the ideal generated by  $f_1$  and  $f_2$  then the leading term ideal  $LT(I)$  contains  $LT(f_1) = x^3y$  and  $LT(f_2) = x^2y^2$ , so  $(x^3y, x^2y^2) \subseteq LT(I)$ . Since

$$yf_1 - xf_2 = y(x^3y - xy^2 + 1) - x(x^2y^2 - y^3 - 1) = x + y$$

we see that  $g = x + y$  is an element of  $I$  and so the ideal  $LT(I)$  also contains the leading term  $LT(g) = x$ . This shows that  $LT(I)$  is strictly larger than  $(LT(f_1), LT(f_2))$ , since every element in  $(LT(f_1), LT(f_2)) = (x^3y, x^2y^2)$  has total degree at least 4. We shall see later that in this case  $LT(I) = (x, y^4)$ .

- (2) With respect to the lexicographic ordering  $y > x$ , the leading terms of  $f_1$  and  $f_2$  in the previous example are  $LT(f_1) = -xy^2$  (which one could write as  $-y^2x$  to emphasize the chosen ordering) and  $LT(f_2) = -y^3$ . We shall see later that in this ordering  $LT(I) = (x^4, y)$ , which is a different ideal than the ideal  $LT(I)$  obtained in the previous example using the ordering  $x > y$ , and is again strictly larger than  $(LT(f_1), LT(f_2))$ .
- (3) Choose any ordering on  $F[x, y]$  and let  $f = f(x, y)$  be any nonzero polynomial. The leading term of every element of the principal ideal  $I = (f)$  is then a multiple of the leading term of  $f$ , so in this case  $LT(I) = (LT(f))$ .

In the case of one variable, leading terms are used in the Division Algorithm to reduce one polynomial  $g$  modulo another polynomial  $f$  to get a unique remainder  $r$ , and this remainder is 0 if and only if  $g$  is contained in the ideal  $(f)$ . Since  $F[x_1, x_2, \dots, x_n]$  is not a Euclidean Domain if  $n \geq 2$  (since it is not a P.I.D.), the situation is more complicated for polynomials in more than one variable. In the first example above, neither  $f_1$  nor  $f_2$  divides  $g$  in  $F[x, y]$  (by degree considerations, for example), so attempting to first divide  $g$  by one of  $f_1$  or  $f_2$  and then by the other to try to reduce  $g$  modulo the ideal  $I$  would produce a (nonzero) “remainder” of  $g$  itself. In particular, this would suggest that  $g = yf_1 - xf_2$  is not an element of the ideal  $I$  even though it is. The reason the polynomial  $g$  of degree 1 can be a linear combination of the two polynomials  $f_1$  and  $f_2$  of degree 4 is that the leading terms in  $yf_1$  and  $xf_2$  cancel in the difference, and this is reflected in the fact that  $LT(f_1)$  and  $LT(f_2)$  are not sufficient to generate  $LT(I)$ . A set of generators for an ideal  $I$  in  $F[x_1, \dots, x_n]$  whose leading terms generate the leading terms of *all* the elements in  $I$  is given a special name.

**Definition.** A *Gröbner basis* for an ideal  $I$  in the polynomial ring  $F[x_1, \dots, x_n]$  is a finite set of generators  $\{g_1, \dots, g_m\}$  for  $I$  whose leading terms generate the ideal of all leading terms in  $I$ , i.e.,

$$I = (g_1, \dots, g_m) \quad \text{and} \quad LT(I) = (LT(g_1), \dots, LT(g_m)).$$

*Remark:* Note that a Gröbner “basis” is in fact a set of *generators* for  $I$  (that depends on the choice of ordering), i.e., every element in  $I$  is a linear combination of the generators, and not a basis in the sense of vector spaces (where the linear combination would be *unique*, cf. Sections 10.3 and 11.1). Although potentially misleading, the terminology “Gröbner basis” has been so widely adopted that it would be hazardous to introduce a different nomenclature.

One of the most important properties of a Gröbner basis (proved in Theorem 23 following) is that every polynomial  $g$  can be written *uniquely* as the sum of an element in  $I$  and a remainder  $r$  obtained by a general polynomial division. In particular, we shall see that  $g$  is an element of  $I$  if and only if this remainder  $r$  is 0. While there is a similar decomposition in general, we shall see that if we do not use a Gröbner basis the uniqueness is lost (and we cannot detect membership in  $I$  by checking whether the remainder is 0) because there are leading terms not accounted for by the leading terms of the generators.