Lecture 3

Last time ideal, varieties.

- (Hilbert Basis Theorem) Every ideal I in $k[x_1, \ldots, x_n]$ has a *finite* generating set. In other words, given an ideal I, there exists a finite collection of polynomials $\{f_1, \ldots, f_s\} \subset k[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle$.

For polynomials in one variable, this is a standard consequence of the one-variable polynomial division algorithm.

- (Division Algorithm in $k[x]$) Given two polynomials $f, g \in k[x]$, we can divide f by g, producing a unique quotient q and remainder r such that

$$f = qg + r,$$

and either $r = 0$, or r has degree strictly smaller than the degree of g.

(2.1) Definition. A *monomial order* on $k[x_1, \ldots, x_n]$ is any relation $>$ on the set of monomials x^α in $k[x_1, \ldots, x_n]$ (or equivalently on the exponent vectors $\alpha \in \mathbb{Z}^n_{\geq 0}$) satisfying:

a. $>$ is a *total (linear) ordering* relation.

b. $>$ is *compatible with multiplication* in $k[x_1, \ldots, x_n]$, in the sense that if $x^\alpha > x^\beta$ and x^γ is any monomial, then $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^{\beta+\gamma} = x^\beta x^\gamma$.

c. $>$ is a *well-ordering*. That is, every non-empty collection of monomials has a smallest element under $>$.

(2.2) Definition (Lexicographic Order). Let x^α and x^β be monomials in $k[x_1, \ldots, x_n]$. We say $x^\alpha >_{lex} x^\beta$ if in the difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive.

Lexicographic order is analogous to the ordering of words used in dictionaries.

(2.3) Definition (Graded Reverse Lexicographic Order). Let x^α and x^β be monomials in $k[x_1, \ldots, x_n]$. We say $x^\alpha >_{grevlex} x^\beta$ if $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$, or if $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$, and in the difference $\alpha - \beta \in \mathbb{Z}^n$, the right-most nonzero entry is negative.

For instance in $k[x, y, z]$, with $x > y > z$, we have

$$x^3y^2z >_{lex} x^2y^6z^{12} \tag{2.4}$$

since when we compute the difference of the exponent vectors:

$$(3, 2, 1) - (2, 6, 12) = (1, -4, -11),$$

the left-most nonzero entry is positive. Similarly,

$$x^3y^6 >_{lex} x^3y^4z$$

since in $(3, 6, 0) - (3, 4, 1) = (0, 2, -1)$, the leftmost nonzero entry is positive. Comparing the *lex* and *grevlex* orders shows that the results can be quite different. For instance, it is true that

$$x^2y^6z^{12} >_{grevlex} x^3y^2z.$$

Compare this with (2.4), which contains the same monomials. Indeed, *lex* and *grevlex* are different orderings even on the monomials of the same total degree in three or more variables, as we can see by considering pairs of monomials such as $x^2y^2z^2$ and xy^4z. Since $(2, 2, 2) - (1, 4, 1) = (1, -2, 1)$,

$$x^2y^2z^2 >_{lex} xy^4z.$$

On the other hand by the Definition (2.3),

$$xy^4z >_{grevlex} x^2y^2z^2.$$

order $>$ on $k[x_1, \ldots, x_n]$, we consider the terms in $f = \sum_\alpha c_\alpha x^\alpha$. Then the *leading term* of f (with respect to $>$) is the product $c_\alpha x^\alpha$ where x^α is the *largest* monomial appearing in f in the ordering $>$. We will use the notation $\mathrm{LT}_>(f)$ for the leading term, or just $\mathrm{LT}(f)$ if there is no chance of confusion about which monomial order is being used.

- (Division Algorithm in $k[x_1, \ldots, x_n]$) Fix any monomial order $>$ in $k[x_1, \ldots, x_n]$, and let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then every $f \in k[x_1, \ldots, x_n]$ can be written as:

$$f = a_1 f_1 + \cdots + a_s f_s + r, \tag{2.5}$$

where $a_i, r \in k[x_1, \ldots, x_n]$, and either $r = 0$, or r is a linear combination of monomials, none of which is divisible by any of $\mathrm{LT}_>(f_1), \ldots, \mathrm{LT}_>(f_s)$. We will call r a *remainder* of f on division by F.

Exercise 1. Recall from (1.4) that $p = x^2 + \frac{1}{2}y^2 z - z - 1$ *is* an element of the ideal $I = \langle x^2 + z^2 - 1, x^2 + y^2 + (z-1)^2 - 4\rangle$. Show, however, that the remainder on division of p by this generating set F is not zero. For instance, using $>_{lex}$, we get a remainder

$$\overline{p}^F = \frac{1}{2}y^2 z - z - z^2.$$

(3.1) Definition. Fix a monomial order $>$ on $k[x_1, \ldots, x_n]$, and let $I \subset k[x_1, \ldots, x_n]$ be an ideal. A *Gröbner basis* for I (with respect to $>$) is a finite collection of polynomials $G = \{g_1, \ldots, g_t\} \subset I$ with the property that for every nonzero $f \in I$, $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$ for some i.

- (Uniqueness of Remainders) Fix a monomial order $>$ and let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Division of $f \in k[x_1, \ldots, x_n]$ by a Gröbner basis for I produces an expression $f = g + r$ where $g \in I$ and no term in r is divisible by any element of $\textsc{lt}(I)$. If $f = g' + r'$ is any other such expression, then $r = r'$.

- (Elimination Ideals) If I is an ideal in $k[x_1, \ldots, x_n]$, then the *ℓth elimination ideal* is

$$I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n].$$

  Intuitively, if $I = \langle f_1, \ldots, f_s \rangle$, then the elements of I_ℓ are the linear combinations of the $f_1, \ldots, f_s$, with polynomial coefficients, that eliminate $x_1, \ldots, x_\ell$ from the equations $f_1 = \cdots = f_s = 0$.

- (The Elimination Theorem) If G is a Gröbner basis for I with respect to the *lex* order ($x_1 > x_2 > \cdots > x_n$) (or any order where monomials involving at least one of $x_1, \ldots, x_\ell$ are greater than all monomials involving only the remaining variables), then

$$G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$$

  is a Gröbner basis of the ℓth elimination ideal I_ℓ.
- (Partial Solutions) A point $(a_{\ell+1}, \ldots, a_n) \in \mathbf{V}(I_\ell) \subset k^{n-\ell}$ is called a *partial solution*. Any solution $(a_1, \ldots, a_n) \in \mathbf{V}(I) \subset k^n$ truncates to a partial solution, but the converse may fail—not all partial solutions extend to solutions. This is where the Extension Theorem comes in. To prepare for the statement, note that each f in $I_{\ell-1}$ can be written as a polynomial in x_ℓ, whose coefficients are polynomials in $x_{\ell+1}, \ldots, x_n$:

$$f = c_q(x_{\ell+1}, \ldots, x_n)x_\ell^q + \cdots + c_0(x_{\ell+1}, \ldots, x_n).$$

  We call c_q the leading coefficient polynomial of f if x_ℓ^q is the highest power of x_ℓ appearing in f.
- (The Extension Theorem) If k is algebraically closed (e.g., $k = \mathbb{C}$), then a partial solution $(a_{\ell+1}, \ldots, a_n)$ in $\mathbf{V}(I_\ell)$ extends to $(a_\ell, a_{\ell+1}, \ldots, a_n)$ in $\mathbf{V}(I_{\ell-1})$ provided that the leading coefficient polynomials of the elements of a *lex* Gröbner basis for $I_{\ell-1}$ do not all vanish at $(a_{\ell+1}, \ldots, a_n)$.