Lecture LVII: Towards Gröbner bases II

§ 57.1 Setup and Notation:

Recall: Last time we started studying the polynomial ring $R = K[x_1, \dots, x_n]$ with $n \geq 1$, K field

- **Notations:** $\underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ "Typical monomial" $\underline{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$

  $f(x_1, \dots, x_n) \in R$ (or just f, to simplify notation) has the form

$$f = \sum_{\substack{\underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \\ \text{finite}}} c_{(\underline{\alpha})} \, \underline{x}^{\underline{\alpha}}$$

  $c_{(\underline{\alpha})} \in K$

- **Monomial Order:** a total ordering on the set of monomials $\{ \underline{x}^{\underline{\alpha}} : \underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \}$ (or $\mathbb{Z}_{\geq 0}^n$) such that
  - $\underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\beta}} \Rightarrow \underline{x}^{\underline{\alpha}+\underline{\gamma}} \leq \underline{x}^{\underline{\beta}+\underline{\gamma}} \quad \forall \underline{\gamma} \in \mathbb{Z}_{\geq 0}^n$
  - $\leq$ is a well-ordering (so $1 < \underline{x}^{\underline{\alpha}} \ \forall \underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \setminus \{\underline{0}\}$)

- **Leading Terms:** Once a choice of monomial order has been made, we define

$$LT\left(\sum_{\substack{\underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \\ \text{finite}}} c_{(\underline{\alpha})} \underline{x}^{\underline{\alpha}} \right) = c_{(\underline{\alpha}_0)} \underline{x}^{\underline{\alpha}_0}$$

  where $\cdot\, c_{(\underline{\alpha}_0)} \neq 0$

  $\cdot\, c_{(\underline{\alpha})} \neq 0 \Rightarrow \underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\alpha}_0}$.

Convention: $LT(0) = 0$.

Lemma: $1 < \underline{x}^{\underline{\alpha}} \quad \forall \underline{\alpha} \in (\mathbb{Z}_{\geq 0})^n \setminus \{\underline{0}\}$.

Proof: It is enough to show $1 < x_i \ \forall i$

Indeed: if $\exists\, i$ s.t. $1 > x_i$. Then $x_i = 1 \cdot x_i > x_i^2$, so $x_i^2 > x_i^3$, and by induction on $k \geq 0$ $x_i^k > x_i^{k+1}$. This implies $\{ x_i^k : k \geq 0 \}$ has no smallest element.

Now, given $1 < x_i \ \forall i$, we have by induction on k: $1 < x_i^k \ \forall k \geq 1$

Thus, given $\underline{\alpha} \in \mathbb{Z}_{\geq 0}$ we have $\begin{cases} 1 < x_i^{\alpha_i} & \text{if } \alpha_i > 0 \\ 1 = x_i^{\alpha_i} & \text{if } \alpha_i = 0 \end{cases}$

Then writing $\underline{x}^{\underline{\alpha}} = x_{i_1}^{\alpha_{i_1}} \cdots x_{i_s}^{\alpha_{i_s}}$ where $\alpha_j = 0$ iff $j \notin \{i_1, \dots, i_s\}$, we get $1 < x_{i_1}^{\alpha_{i_1}} \Rightarrow 1 < x_{i_2}^{\alpha_{i_2}} < x_{i_1}^{\alpha_{i_1}} x_{i_2}^{\alpha_{i_2}} \Rightarrow 1 < x_{i_1}^{\alpha_{i_3}} < x_{i_1}^{\alpha_{i_1}} x_{i_2}^{\alpha_{i_2}} x_{i_3}^{\alpha_{i_3}}$, ...

Continuing in this way (induction on s) given $1 < \underline{x}^{\underline{\alpha}}$, as we wanted. □

Remark: Not is true! For multiplicative total orders: $1 \leq \underline{x}^{\underline{\alpha}} \ \forall \underline{\alpha} \iff <$ is a well-order.

§57.2 Main examples of monomial orderings:

① Dictionary order or lexicographic order: $\geq_{lex}$

We fix an arbitrary ordering of variables, and then decide which monomial is "bigger" according to the following rule (the same we used to look up words in a dictionary):

$$x_1^{\alpha_1}\cdots x_n^{\alpha_n} >_{lex} x_1^{\beta_1}\cdots x_n^{\beta_n} \quad \text{iff} \quad \exists\, k=1,\dots,n \text{ such that}$$
$$\alpha_1=\beta_1,\dots,\alpha_k=\beta_k \text{ and } \alpha_{k+1}>\beta_{k+1}$$

(Here we fix the order $x_1 > x_2 > \cdots > x_n$)

Example: $n=3$ $\quad x_1^{k_1}x_2^{k_2}x_3^{k_3} > x_1^{l_1}x_2^{l_2}x_3^{l_3}$ iff
$$\begin{cases} k_1 > l_1, \text{ or} \\ k_1 = l_1 \ \&\ k_2 > l_2 \\ k_1 = l_1 \ \&\ k_2 = l_2 \ \&\ k_3 > l_3 \end{cases}$$

For instance $x_1^2x_2^1x_3^1 > x_1^1x_2^4x_3^0$

Check: $>_{lex}$ is a term order (use $1 \leq x^{\alpha}$ $\forall \alpha \neq 0$)

Note: They are $n!$ possible $>_{lex}$, determined by the ordering of the variables.

② Graded lex order: $\geq_{grlex}$

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $x^{\alpha} >_{grlex} x^{\beta}$ if

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i \quad \text{or} \quad |\alpha| = |\beta| \text{ and } x^{\alpha} >_{lex} x^{\beta}$$

In short: (1) First, we order monomials by total degree

(2) Then, if the total degree is the same, we break the tie with $>_{lex}$.

Examples: $n=3$ $\quad x_1 >_{lex} x_2 >_{lex} x_3$

- $x_1x_2^2x_3^3 >_{grlex} x_1^3x_2^2$ but $x_1^3x_2^2 >_{lex} x_1x_2^2x_3^3$
- $x_1x_2^2x_3^4 >_{grlex} x_1x_2x_3^5$: both have degree 7 & $x_1x_2^2x_3^4 >_{lex} x_1x_2x_3^5$
- $x_1 >_{grlex} x_2 >_{grlex} x_3$

Check: $>_{grlex}$ is a term order (use $1 \leq x^{\alpha}$ $\forall \alpha \neq 0$)

Note: They are $n!$ possible $>_{grlex}$, since there are $n!$ possible $>_{lex}$.

(3) Graded Reverse Lex order: $\geq_{grevlex}$

Let $\underline{\alpha}, \underline{\beta} \in \mathbb{Z}^n_{\geq 0}$. We say $\underline{x}^{\underline{\alpha}} >_{grevlex} \underline{x}^{\underline{\beta}}$ if

$|\underline{\alpha}| > |\underline{\beta}|$ or ($|\underline{\alpha}| = |\underline{\beta}|$ and the rightmost nonzero entry of $\underline{\alpha} - \underline{\beta} \in \mathbb{Z}^n$ is negative)

In short: (1) First, we order first by total degree.

(2) We break ties by "reverse lexicographic".

The condition (1) ensures the well-order.

Examples: $n=3$

- $x_1^4 x_2^7 x_3 >_{grevlex} x_1^4 x_2^2 x_3^3$ $\quad |\underline{\alpha}| = 12 > |\underline{\beta}| = 9$
- $x_1 x_2^5 x_3^2 >_{grevlex} x_1^4 x_2^1 x_3^3$ $\quad |\underline{\alpha}| = |\underline{\beta}| = 8$ & $(1,5,2) - (4,1,3) = (-3,4,-1)$ ↑

Observation: $x_1 >_{grevlex} x_2 >_{grevlex} \cdots >_{grevlex} x_n$.

Check: $>_{grevlex}$ is a term order (use $1 \leq x^{\underline{\alpha}}$ $\forall \underline{\alpha} \neq \underline{0}$)

§57.3 Leading terms:

Definition: Given $I \subseteq K[x_1, \ldots, x_n]$ an ideal, we define the leading ideal of I as

$$LT(I) = \text{ideal in } K[x_1, \ldots, x_n] \text{ generated by } \{LT(f) : f \in I\}$$

Remark: Since $K[x_1, \ldots, x_n]$ is Noetherian, we know $LT(I)$ is finitely generated. In addition, we can pick a finite set among the (infinitely many) generators of $\{LT(f) : f \in I\}$ by Lemma §52.1.

§57.4 Definition of Gröbner bases:

Definition: A finite set of generators of I say $\{g_1, \ldots, g_m\}$ is called a Gröbner basis of I with respect to a monomial order $<$ on $K[x_1, \ldots, x_n]$ if

$$LT(I) = (LT(g_1), \ldots, LT(g_m))$$

Remark: It is clear that we can find $\{g_1, \ldots, g_m\} \subseteq I$ with

$$LT(I) = (LT(g_1), \ldots, LT(g_m))$$

Why can we ensure $\{g_1, \ldots, g_m\}$ generated I? We will indeed show that this

is true. More precise, we will prove:

Proposition 1: Assume $I \subseteq R = K[x_1, \dots, x_n]$ is a non-zero ideal and $\{g_1, \dots, g_m\} \subseteq I$ satisfy $LT(I) = (LT(g_1), \dots, LT(g_m))$. Then, $\{g_1, \dots, g_m\}$ is a Gröbner basis of I.

We will prove this statement by developing a division algorithm.

Remarks: (1) The definition of a G.B. depends very crucially on the monomial order chosen.

(2) The existence of a G.B. is a priori not obvious. We will prove it by combining Hilbert's Basis Theorem together with an analog of the division algorithm for multivariate polynomials that uses leading terms instead of degree (hence, it will depend on the fixed monomial order). The algorithm is not very efficient and some choices of $<$ are better than others.

(3) We will not need to compute $LT(I)$ to show a list of polynomials is a G.B. for I.

⚠ **Catch:** We noticed that the following statement is FALSE:

$$I = (f_1, \dots, f_r) \implies LT(I) = (LT(f_1), \dots, LT(f_r))$$

Gröbner bases will be a set of generators of I making this statement True. It will allow to incorporate concrete algorithms to detect membership of a polynomial in I, among other things.

Example: Say $n = 2$ and let us just write x & y for our variables. So $R = K[x, y]$. Let us also choose lexicographic order, with $x > y$.

$$f(x,y) = x^3y - xy^2 + 1 \implies LT(f) = x^3y$$

$$g(x,y) = x^2y^2 - y^3 - 1 \implies LT(g) = x^2y^2$$

Set $I = (f, g) \subseteq K[x, y]$. We have $LT(I) \neq (LT(f), LT(g))$ because

$$x + y = yf - xg \in I \quad \text{but} \quad LT(x+y) = x \notin (x^3y, x^2y^2).$$

Q: Is $\{f, g, x+y\}$ a Gröbner basis of I?

A It's hard to decide this with our current knowledge since we don't know what $LT(I)$ is (i.e. we don't have a finite set of generators or a way to test membership). We will develop an algorithm for computing Gröbner bases that will decide if a

set of polynomials in I is a G.B for I without knowing $LT(I)$. The method will be similar than the one in the example. A posteriori, we can use a G.B. to

(1) compute $LT(I)$

(2) decide membership of a polynomial f in the ideal I

Both things will depend on a "multivariate" division algorithm, which we will see next time.