Lecture 52

(52.0) Recall - we started studying the polynomial ring

$$R = K[x_1, x_2, \ldots, x_n]$$

where K is a field. and $n \geq 1$.

- Notations : $\underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ "typical monomial"

$$\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$$

$f(x_1, \ldots, x_n)$ (or just f - to save time) $\in R$ has the form $f = \sum_{\underline{\alpha} \in \mathbb{Z}_{\geq 0}^n}^{\text{finite}} c(\underline{\alpha})\, \underline{x}^{\underline{\alpha}}$ ($c(\underline{\alpha})$: element of K)

- Monomial Order is a total ordering on the set of monomials

$$\left\{ \underline{x}^{\underline{\alpha}} \;\middle|\; \underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \right\} \text{ such that}$$

$$\underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\beta}} \Rightarrow \underline{x}^{\underline{\alpha}+\underline{\gamma}} \leq \underline{x}^{\underline{\beta}+\underline{\gamma}} \quad \forall\, \underline{\gamma} \in \mathbb{Z}_{\geq 0}^n$$

[Main example to keep in mind : lexicographic order (or dictionary order)]

- Leading term Once a choice of a monomial order has been made we define $LT\left(\sum_{\underline{\alpha} \in \mathbb{Z}_{\geq 0}^n}^{\text{finite}} c(\underline{\alpha})\, x^{\underline{\alpha}}\right) = c(\underline{\alpha}_0)\, \underline{x}^{\underline{\alpha}_0}$ where

$c(\underline{\alpha}_0) \neq 0$ and for $\underline{\alpha} \in \mathbb{Z}_{\geq 0}^n$, if $c(\underline{\alpha}) \neq 0$ then $\underline{\alpha}_0 \geq \underline{\alpha}$

- For an ideal $I \subsetneq K[x_1, \ldots, x_n]$ we defined

$$LT(I) = \underline{\text{ideal generated by the set}}$$

$$\{ LT(f) \mid f \in I \} \subset K[x_1, \ldots, x_n]$$

ideal

We noticed that the following statement is FALSE :

$$I = (f_1, \ldots, f_r) \Rightarrow LT(I) = (LT(f_1), \ldots, LT(f_r))$$

(52.1) Definition. – A finite set of generators of I, say $\{g_1, \ldots, g_m\}$ is called a Gröbner basis (of I) if

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

Remarks. – (1) This definition (i.e. a Gröbner basis) depends very crucially on the monomial order chosen.

(2) The existence of a Gröbner basis will be proved today, using Hilbert Basis Theorem., and an analogue of division "algorithm" for multivariable polynomials – that uses leading terms. (and hence, in turn, depends on $\leq$ = fixed monomial order.

(it is only in quotes because it is not very efficient.)

(52.2) Multivariable polynomial division.

Fixed data: $g_1, \ldots, g_m \in K[x_1, \ldots, x_n]$

Input: $f \in K[x_1, \ldots, x_n]$

Output: $q_1, \ldots, q_m \in K[x_1, \ldots, x_n]$

$r \in K[x_1, \ldots, x_n]$

such that $f = q_1 g_1 + \ldots + q_m g_m + r$ such that

(1) No term in r is divisible by $LT(f)$.

(2) $LT(q_i g_i) \leq LT(f)$ for every $i = 1, \ldots, m$.

Procedure: Start with $q_1, \ldots, q_m, r = 0$.

While $f \neq 0$:

- if $LT(f)$ is divisible by $LT(g_i)$ for some i (test in order $i = 1, \ldots, m$) - say $LT(f) = a_i LT(g_i)$

then

$$q_i \xrightarrow{\text{change to}} q_i + a_i$$

$$f \longmapsto f - a_i g_i$$

else

$$r \longmapsto r + LT(f)$$

$$f \longmapsto f - LT(f)$$

(52.3) Example. – $\boxed{m=1}$ $g = xy^4$

$f = x^3y^3 + 3x^2y^4$

Monomial order = lexicographic with $x > y$.

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

(52.4) Prop: (1) If $g_1, \dots, g_m \in I \subsetneq R = K[x_1, \dots, x_n]$ ideal (say, non-zero)

s.t. $LT(I) = (LT(g_1), \dots, LT(g_m))$

then $\{g_1, \dots, g_m\}$ is a Gröbner basis of I.

(2) Gröbner basis exist. (I has a Gröbner basis).

Proof. – (1) To prove: $I = (g_1, \dots, g_m)$

Let $f \in I$, by (52.2) we can write

$$f = \sum_{i=1}^{m} q_i g_i + r \quad \text{s.t. (1) \& (2) of (52.2) hold true.}$$

As $f \in I$, we get $r \in I$. Hence $\underline{LT(r) \in LT(I)}$

$\Rightarrow$ $LT(g_i)$ divides $LT(r)$ for some i

we get a contradiction to (2) of (52.2), unless $r = 0$.

(why? – see next page.)

(why? from previous page : -

(*) Since $LT(I) = (LT(g_1), \ldots, LT(g_m))$, and each $LT(g_i)$ is a monomial we have the following :

$p \in LT(I) \iff p = h_1 LT(g_1) + \ldots + h_m LT(g_m)$ for some $h_1, \ldots, h_m \in R$

$\iff$ each monomial appearing in p must be divisible by some $LT(g_i)$ - end of why.)

Now that we know $r = 0$, we have $f = \sum_{i=1}^{m} q_i g_i$.

Hence $I = (g_1, \ldots, g_m)$ as claimed.

(2) As $LT(I)$ is an ideal of R - and smallest one containing the (infinite) set $\{LT(f) \mid f \in I\}$ - every $p \in LT(I)$ can be written as a finite linear combination

$p = h_1 LT(f_1) + \ldots + h_r LT(f_r)$,

where $f_1, \ldots, f_r \in I$ and $h_1, \ldots, h_r \in R$. (This is the defn. of ideal gen. by a set.)

Now $LT(I) = (p_1, \ldots, p_N)$ for some $p_1, \ldots, p_N \in LT(I)$ by Hilbert Basis Theorem. By what we just observed

$p_j = h_{j,1} LT(f_{j,1}) + \ldots + h_{j,r_j} \cdot LT(f_{j,r_j})$

Hence we have finitely many elements

$$f_{1,1}, \dots, f_{1,r_1}; f_{2,1}, \dots, f_{2,r_2}; \dots; f_{N,1}, \dots, f_{N,r_N} \in I$$

(rename them to $g_1, \dots, g_m \in I$)

so that $LT(I) = (LT(g_1), \dots, LT(g_m))$ and by (1)

$\{g_1, \dots, g_m\}$ is a Gröbner basis. □

(52.5) Theorem (Membership test). – Again let $I \subset R$ be an ideal and $\{g_1, \dots, g_m\}$ a Gröbner basis of I. Then, for any $f \in R$, there exist unique elements $f_I \in I$ and $r \in R$ such that

(i) $f = f_I + r$

(ii) No monomial appearing in r is divisible by any of the $LT(g_i)$'s.

Proof – we can certainly write $f = \boxed{\sum_{i=1}^{m} q_i g_i}_{f_I \in I} + r$ (see (52.2))

satisfying these conditions. We only need to prove the uniqueness:

$$f = f_I + r = \tilde{f}_I + \tilde{r} \Rightarrow r - \tilde{r} = \tilde{f}_I - f_I \in I$$

$\Rightarrow LT(r-\tilde{r}) \in LT(I) = (LT(g_1), \dots, LT(g_m))$ (by defn of Gröbner basis)

$\Rightarrow r - \tilde{r} = 0 \Rightarrow r = \tilde{r}$ and hence $\tilde{f}_I = f_I$. □

(see (*) on page 4 above)

Cor : $f \in I \iff r = 0$

Proof. – Obvious !

Meaning : if we are given an ideal I, as being generated by $f_1, \ldots, f_\ell$; and asked to check whether $f \in I$ or not, then

1. Replace $f_1, \ldots, f_\ell$ by a Gröbner basis, say $g_1, \ldots, g_m$
2. Use the algorithm on page 3 – §52.2 to compute the remainder r.

$r = 0 \rightsquigarrow f \in I$

$r \neq 0 \rightsquigarrow f \notin I$ ← [This part will not be true if $g_1, \ldots, g_m$ were not a Gröbner basis – its raison d'être.]