Lecture 53

(53.0) **Recollections.** — $R = K[x_1, \dots, x_n]$ $\left(\begin{matrix} K : \text{field} \\ n \geq 1 \end{matrix}\right)$

- $\underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ $\underline{\alpha} \in \mathbb{N}^n$ $(\mathbb{N} = \mathbb{Z}_{\geq 0})$.
  monomials

- $f = \sum_{\alpha \in \mathbb{N}^n}^{\text{finite}} c(\underline{\alpha}) \, \underline{x}^{\underline{\alpha}}$ typical poly. in R.

- $\leq$ = a monomial order (i.e. total order on $\{\underline{x}^{\underline{\alpha}} \mid \underline{\alpha} \in \mathbb{N}^n\}$
  s.t. $x^\alpha \leq x^\beta \Rightarrow x^{\alpha+\gamma} \leq x^{\beta+\gamma}$). Say, lexicographic order

- Multivariable division algorithm
  Fixed data $G = \{g_1, \dots, g_m\} \subset R$ a subset
  Input : $f \in R$.

  Procedure set $q_1, \dots, q_m, r = 0$

  while $f \neq 0$:

  $$\boxed{\begin{array}{ll} \underline{\text{if}} \ LT(f) = a_i \, LT(g_i) \text{ for some } i \in \{1, \dots, m\} & \\ \underline{\text{then}} & f \longmapsto f - a_i g_i \\ & q_i \longmapsto q_i + a_i \\ \underline{\text{else}} & f \longmapsto f - LT(f) \\ & r \longmapsto r + LT(f) \end{array}}$$

  return : r — remainder

  recall : $f = \sum c(\alpha) x^\alpha$
  $\Rightarrow LT(f) = c(\alpha_0) \, x^{\alpha_0}$
  where $c(\alpha_0) \neq 0$
  and $c(\alpha) \neq 0 \Rightarrow \alpha \leq \alpha_0$

- $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of I if, and only if

$$\underset{\sim\sim\sim}{LT(I)} = \left(LT(g_1), \ldots, LT(g_m)\right)$$

ideal generated by the set $\{LT(f) \mid f \in I\}$

(53.1) Facts about Gröbner basis – proved in last lecture

1. Every ideal has a Gröbner basis.
2. If $\{g_1, \ldots, g_m\}$ is a Gröbner basis of I, then

$$f \in I \iff \text{the } r \text{ from our division algorithm is } 0.$$

(53.2) Buchberger's Theorem. – How to tell if a finite set of generators of I is a Gröbner basis or not?

<u>Notations</u> :

- given $G = \{g_1, \ldots, g_m\} \subset R$, we will write $\boxed{f \equiv 0 \mod G}$ if our multivariate division algorithm outputs $r = 0$.

- given $f_1, f_2 \in R$, let M be the monic least common multiple of $LT(f_1)$ and $LT(f_2)$.

$$\left(LT(f_1) = c_1 \cdot X^{\alpha} \;;\; LT(f_2) = c_2 \cdot X^{\beta} \implies M = 1 \cdot X_1^{\max(\alpha_1, \beta_1)} \cdots X_n^{\max(\alpha_n, \beta_n)} \right)$$

$$\boxed{S(f_1, f_2) := \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2}$$

Theorem (Buchberger). – Let $I = (g_1, \dots, g_m) \subset R$ be an ideal. Then $\{g_1, \dots, g_m\}$ is a Gröbner basis

$$\Longleftrightarrow \quad S(g_i, g_j) \equiv 0 \pmod{G}.$$

(53.3) Example. $R = K[x, y]$

$\leq$ = lexicographic avec $x > y$.

Let $I = (f_1, f_2)$ where
$$f_1 = x^3y - xy^2 + 1$$
$$f_2 = x^2y^2 - y^3 - 1$$

$G_0 = \{f_1, f_2\}$

$$S(f_1, f_2) = y f_1 - x f_2 = x + y$$
$$\equiv \underset{\neq 0}{x + y} \mod G = \{f_1, f_2\}$$

$\Rightarrow \{f_1, f_2\}$ is not a Gröbner basis.

(53.4) Example continued. – Take $G_1 = \{f_1, f_2, f_3 = x + y\}$.

$$S(f_2, f_3) = f_2 - xy^2(x+y) = -xy^3 - y^3 - 1$$
$$\equiv \underset{\neq 0}{y^4 - y^3 - 1} \mod G_1$$

$\Rightarrow$ G_1 is not a Gröbner basis.

(53.5) Example contd. contd. Take $G_2 = \{f_1, f_2, f_3, \underset{y^4-y^3-1}{\underset{\|}{f_4}}\}$

e.g. $S(f_3, f_4) = y^4(\cancel{x}+y) - x(\cancel{y^4}-y^3-1)$

$= y^5 + xy^3 + x \equiv 0 \pmod{G_2}$.

<u>Exercise</u> - for your laptop - G_2 is a Gröbner basis.

$\{x^3y - xy^2+1,\ x^2y^2 - y^3 - 1,\ x+y,\ y^4-y^3-1\} = G_2$

$\{\underbrace{\boxed{x^3y,\ x^2y^2}}_{\text{already in } (x,\,y^4)},\ x,\ y^4\} = LT(G_2)$

$\rightsquigarrow$ better generators for I : $(x+y,\ y^4-y^3-1)$

"minimal Gröbner basis"

(53.6) Buchberger algorithm.

Input : $f_1, \dots, f_s \in R = K[x_1, \dots, x_n]$

Output : $G = \{g_1, \dots, g_m\} \supseteq F = \{f_1, \dots, f_s\}$

a Gröbner basis of $I = (f_1, \dots, f_s)$

initialize $G \mapsto F$.

$G_{temp} = \phi$

~~撃~~ while $G \neq G_{temp}$:

- set $G_{temp} = G$
- For every $p \neq q$ in G_{temp}

  $r := S(p,q) \mod G_{temp}$

  if $r \neq 0$, $G \longmapsto G \cup \{r\}$

return G. (to go from G to $G^{minimal}$ is easy.)

(53.7) Another lesson from our example - eliminating variables.

If G is a Gröbner basis for a non-zero ideal $I \subset K[x_1, \dots, x_n]$ w.r.t. lexicographic order $\leq$ where $x_1 > x_2 > \dots > x_n$

then $G \cap K[x_i, x_{i+1}, \dots, x_n]$ generates $I \cap K[x_i, x_{i+1}, \dots, x_n]$

e.g. $I = (2x^2 + 2xy + y^2 - 2x - 2y,\ x^2 + y^2 - 1) \subset \mathbb{R}[x,y]$

Problem : solve for $(x, y) \in \mathbb{R}^2$ s.t.

$$2x^2 + 2xy + y^2 - 2x - 2y = 0$$

$$x^2 + y^2 = 1$$

Gröbner basis (computed using a computer)

$$g_1 = 2x + y^2 + 5y^3 - 2$$

$$g_2 = 5y^4 - 4y^3$$

$$g_2 = 0 \Rightarrow y = 0 \text{ or } y = \frac{4}{5}$$

$$g_1 \Big|_{y=0} : \quad 2x - 2 = 0 \Rightarrow x = 1$$

$$g_1 \Big|_{y=\frac{4}{5}} = 0 \rightsquigarrow \frac{-3}{5}$$