Nov 1 Recap

Univariate Division

\[ f = \text{LT}(f) + \text{Tail}(f) \]

\[ g = \text{LT}(g) + \text{Tail}(g) \]

\[ \frac{f}{g} \rightarrow r \quad r = f - \frac{\text{LT}(f)}{\text{LT}(g)} \cdot g \]

\[ \text{dividend} \quad \text{quotient} \quad \text{divisor} \]

\[ f \div g \rightarrow r \quad \text{1-step remainder} \quad \text{\#final remainder} \]
Multivariate polynomials

→ need term ordering.

Lex, deglex, degrevlex

Example:

\[ f = y^2x + 4yx - 3x^2 \]

\[ g = 2y + x + 1 \]

Deglex \( y > x \)

\[ \gamma = f - \frac{c \cdot x}{\text{LT}(g)} \cdot g \]

\[ = f - \frac{y^2x}{2y} \cdot g \]

\[ = -\frac{1}{2}y^2x^2 + \frac{7}{2}yx - 3x^2 \]

\( c \cdot x = 1^{st} \text{ monomial in } f \text{ that can be cancelled by } \text{LT}(g) \).
Poly reduction via division

Given: $f, F = \{ f_i, \ldots, f_k \}$.

1. Take $\text{LT}(f)$.
2. Divisible by $\text{LT}(f_i)$? If so,
   
   $\gamma = f - \frac{\text{LT}(f)}{\text{LT}(f_i)} \cdot f_i$

3. Continue. $\gamma = \text{new}(f)$.

Is $\text{LT}(\gamma)$ divisible by $\text{LT}(f_i)$?

If not, is $\text{LT}(\gamma) \div \text{LT}(f_2)$?

If not, is $\text{LT}(\gamma) \div \text{LT}(f_3)$?

If not, is $\text{LT}(\gamma) \div \text{LT}(f_i) \forall i$? Then $\text{LT}(\gamma) = \text{remainder}$. 

If $\text{LT}(\gamma)$ not divisible by $\text{LT}(f_i) \forall i$, then $\text{LT}(\gamma) = \text{remainder}$. 

Ex. Let \( x > y \) \( \in \mathbb{Q} \setminus \{x, y\} \)

\[ f = xy^2 + 1 \quad \text{and} \quad I = \langle f_1, f_2 \rangle \]

\[ f_1 = xy + 1, \quad f_2 = y + 1 \]

\[ \frac{\text{LT}(f_1)}{\text{LT}(f)} \quad \checkmark \]

\[ x = f - \frac{\text{LT}(f)}{\text{LT}(f_1)} \cdot f_1 \]

\[ = (xy^2 + 1) - \left[ \frac{xy^2}{xy} \right] (xy + 1) \]

\[ = xy^2 + 1 - (y)(xy + 1) \]

\[ = xy^2 + 1 - xy^2 - y \]

\[ = -y + 1 = x \]
\[ x = -y + 1, \quad f_1 = ay^2 + 1, \quad f_2 = y + 1 \]

\[ \Rightarrow \text{ new}(f) = r = -y + 1 \]

Is \( LT(f) \div LT(f_1) \)?

\(-y \div xy^2 \)? No.

Pick \( f_2 \) now.

Is \( LT(f) \div LT(f_2) \)?

\(-y \div y \)? \( \checkmark \)

\[ x = f - \frac{LT(f)}{LT(f_2)} \cdot f_2 \]

\[ = (y+1) - c(-1)(y+1) \]

\[ = -y + 1 + y + 1 = 2 = x \]
Step 3. $x = 2 = \text{new}(f)$

Is $\text{LT}(f) \div \text{LT}(f_1)$? $\times$

Is $\text{LT}(f) \div \text{LT}(f_2)$? $\times$

Move 2 into the remainder.

$x = 2$. \text{new}_f = f - 2

$= 2 - 2 = 0$

No more terms to cancel.

So, $f \rightarrow f_1 + f_2 + 2$
Motivate Groebner basis by means of ideal membership testing:

\[ J = \langle f_1, \ldots, f \rangle \] & another poly \( f \). Given.

Assume \( f \in I \).

\[ f = u_1 f_1 + u_2 f_2 + \cdots + u_s f_s + \sum_j \]

1. 1-step reduction.

\[ f \xrightarrow{f_i} y_1 = f - u_i f_i \]

\( f_i \in J, f \notin J, u_i f_i \notin J \) so \( y_1 \notin J \).

\( y_1 \) should have a \( \text{LT}(y_1) \)

\[ \text{LT}(f_i) \) (some \( f_i \)) should divide \( \text{LT}(y_1) \)

\[ y_2 = y_1 - \frac{\text{LT}(y_1)}{\text{LT}(f_i)} f_i \]

\[ y_2 \in J \checkmark \]

\( \text{LT}(y_2) \) should also be cancelled!

\[ \ldots \ldots \text{ultimately, all terms should cancel} \ldots \]
Example. \( f = x \). \( f_1 = x^2 \), \( f_2 = x^2 - x \)

\[ f = f_1 - f_2 \] \( I = \langle f_1, f_2 \rangle \)

So \( f \in I \).

But. \( \text{LT}(f_1) \neq \text{LT}(f) \) \( x^2 + x \)

\( \text{LT}(f_2) \neq \text{LT}(f) \) \( x^2 + x \).

\( \rightarrow \) Division, by itself, cannot decide ideal membership. Why?

\( \rightarrow \) Because, I does not have "all the requisite leading terms".
So how to obtain these missing leading terms in the ideal?

Think Gaussian elimination.

\[ f_1: \ 2x + 3y = 4 \]
\[ f_2: \ 3x + 2y = 1 \]

\[ 3f_1: \ 6x + 9y = 12 \]
\[ -2f_2: \ 6x + 4y = -2 \]

new leading term.

\[ y = [3] f_1 - [2] f_2 \]

\[ = 5y - 10 \]

new leading term.

\[ I = \langle f_1, f_2 \rangle = \langle f_1, f_2, 0 \rangle \]
given \( f \) and \( I = \langle f_1, f_2, f_3 \rangle \).

Is \( f \) in \( I \)?

Compute \( G = \gcd(I) \)

\[ = \{ g_1, \ldots, g_t \} \]

\[ f \underset{g_1, g_2, \ldots, g_t}{\rightarrow} 0? \]

Ideal membership test!