Ex] $I = (y - x^2, z - x^3)$ is a GB in lex $y > z > x$

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3)$$

(yz ← lcm)

$$= -z^2 + yx^3$$

if we divide $S(y - x^2, z - x^3)$ by $\{y - x^2, z - x^3\}$ we get remainder zero.

Thm: (Buchberger's Algorithm)

Let $I = (f_1, \ldots, f_s) \neq 0$ be a poly. ideal

A Gröbner basis for I can be constructed in a finite number of steps by the following

Input: $F = (f_1, \ldots, f_s)$

Output: a GB $G = (g_1, \ldots, g_t)$ for I, $F \subseteq G$

$G := F$

Repeat:

$G' = G$

For each pair $\{p, q\}$ in G' DO

$r = \overline{S(p,q)}^{G'}$

If $r \neq 0$ Then $G = G \cup \{r\}$

until $G = G'$

Return G

Proof: $I = (G)$ at every step since F is a basis of I and $\overline{S(p,q)}^{G} \in I$

So $G \cup \{r\} \subseteq I$

Now note if $G = G'$ $\Rightarrow$ $r = \overline{S(p,q)}^{G} = 0$ $\forall$ pairs $p,q \in G$

$\Rightarrow$ G is a $G.B.$

Show alg. terminates:

$(LT(G')) \subseteq (LT(G))$ since $G' \subseteq G$ ← has r added

If $G' \neq G$ $(LT(G')) \subsetneq (LT(G))$ since

$LT(r) =$ rem of div by G'

is not div by any of $LT(G')$

$\therefore LT(r) \notin (LT(G'))$

The ideals $(LT(G')) \subseteq (LT(G))$

form an ascending chain as alg runs

$\therefore$ They must stabilize at some stage

by ACC

∎

Lemma: Let G be a GB of $I \subset K[x_1, \ldots, x_n]$

$p \in G$ s.t $LT(p) \in (LT(G \setminus \{p\}))$ Then

$G \setminus \{p\}$ is also a GB.

minimal GB: GB G where make $LC = 1$ and remove any redundant $p \in G$.

Def A reduced Gröbner basis G of I is

a GB s.t

- $LC(p) = 1 \quad \forall p \in G$
- $\forall p \in G$ no monomial of p lies in $(LT(G \setminus \{p\}))$

This is how M2 checks equality of ideals.

Theorem | Let $I \neq \{0\}$ be a poly ideal! For a fixed monomial order I has a unique reduced Gröbner basis.