~~**Warning** Reductions aren't always unique!~~

~~Ex Use lex. order on $S(X,Y)$~~

~~$f = X^2Y^2, \qquad G = \{XY^2, X^2Y+1\}$~~

~~$r = f^{(1)} = X^2Y^2 - X\cdot XY^2 = 0$~~

~~or $r = f^{(1)} = X^2Y^2 - Y\cdot(X^2Y+1) = -Y$~~

Def A Gröbner basis of an ideal I w.r.t. $\leq$ is a subset $G \subseteq I$ such that

$$\mathrm{lm}(I) = \{M : N \mid M \text{ for some } N \in \mathrm{lm}(G)\}.$$

Rmk "$\supseteq$" holds for any subset $G \subseteq I$.

Ex I is a Gröbner basis of I.

Ex $\{f\}$ is a Gröbner basis of (f) for any polynomial f.

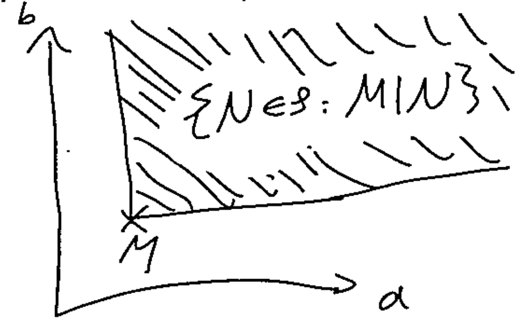
Rmk Let $A \subseteq S$. A monomial M is divisible by an element of A if and only if it is contained in the ideal (A) generated by the elements of A.

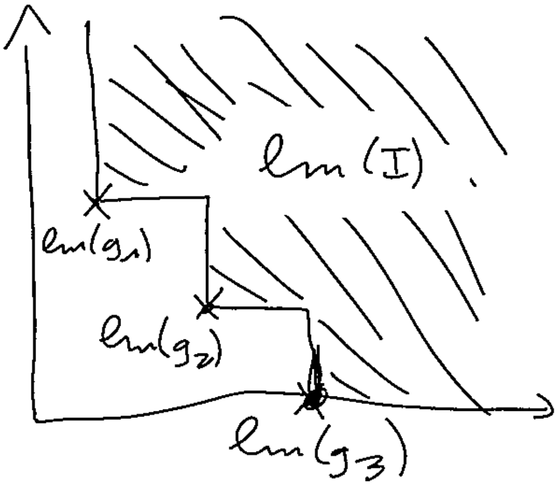
Cor 8.1 Any ideal $I \subseteq K[x_1, \dots, x_n]$ has a finite Gröbner basis.

Pf By Hilbert's Basis Theorem, the ideal $(\mathrm{lm}(I))$ is generated by finitely many elements $\mathrm{lm}(g_1), \dots, \mathrm{lm}(g_r)$ $(0 \neq g_1, \dots, g_r \in I)$. Take $G = \{g_1, \dots, g_r\}$. $\square$

Picture ($n=2$)

$M = x^a y^b$





Thm 8.2 The monomials $M \notin \operatorname{lm}(I)$ form a basis of the K-vector space $K[x_1, \dots, x_n]/I$.

Pf generators:

consider any $f \in K[x_1, \dots, x_n]$.

Let r be any reduction w.r.t. I.

$\Rightarrow r$ is a linear combination of monomials $M \notin \operatorname{lm}(I)$.

linearly independent:

The leading monomial of any nonzero linear combination f of monomials $M \notin \operatorname{lm}(I)$ is $\operatorname{lm}(f) \notin \operatorname{lm}(I)$.

$\Rightarrow f \notin I$. $\square$

Cor 8.3 $\dim_K (K[x_1, \dots, x_n]/I) = \#(S \setminus \operatorname{lm}(I))$.

Rmk Recall that $\# V(I) \le \dim_K(\dots)$!

~~Thm 8.5 Reduction w.r.t. a Gröbner basis is always unique.~~

~~Pf Let $r_1 \ne r_2$ be reductions of f w.r.t. G.~~

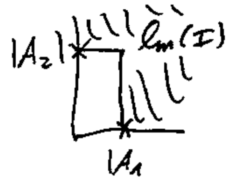
~~$\Rightarrow r_1 \equiv r_2 \bmod I$. $\Rightarrow r_1 - r_2 \in I$~~

~~$\Rightarrow \operatorname{lm}(r_1 - r_2) \in \operatorname{lm}(I)$.~~

~~$\Rightarrow r_1$ or r_2 isn't reduced w.r.t. G!~~ $\square$

Cor 8.4 (Combinatorial Nullstellensatz)

Let $A_1, \dots, A_n \subseteq K$ be finite sets,



$V = A_1 \times \dots \times A_n \subset K^n$.

Then, $X_1^{e_1} \cdots X_n^{e_n}$ is a standard monomial for $I = \mathcal{J}(V)$ if and only if

$0 \le e_1 < |A_1|, \dots, 0 \le e_n < |A_n|$. (I)

Pf $f_i = \prod_{a \in A_i} (X_i - a)$ lies in I and has leading monomial $X_i^{|A_i|}$.

$\Rightarrow$ Every standard monomial satisfies (I).

There are $|V|$ standard mon., but only $|A_1| \cdots |A_n| = |V|$ mon. satisfy (I).

$\Rightarrow$ All of them are standard. $\square$

Thm 8.5 Reductions w.r.t. Gröbner bases are always unique.

Pf Let $r_1 \neq r_2$ be reductions of f w.r.t. G.

$\Rightarrow r_1 \equiv r_2 \mod I$. $\Rightarrow r_1 - r_2 \in I$

$\Rightarrow \mathrm{lm}(r_1 - r_2) \in \mathrm{lm}(I)$

$\Rightarrow r_1$ and r_2 can't both be reduced w.r.t. G. ↯ $\square$

Cor 8.6 Let G be a Gröbner basis of I. Then, $f \in I$ if and only if its reduction w.r.t. G is 0.

Pf Any reduction $r \equiv f \bmod I$ is a linear combination of monomials $M \notin lm(I)$. Then, $r \in I$ if and only if $r = 0$. $\square$

Cor 8.7 Any Gröbner basis G of I generates I.

Pf

If $f \in I$, then $0 \underset{\substack{\uparrow \\ f \in I}}{=} r \equiv f \bmod (G)$, so $f \in (G)$. $\square$

Thm 8.8 (Buchberger's Criterion)

A set G is a Gröbner basis for $I := (G)$ if and only if for all $0 \neq f, g \in G$, some/every reduction of

$$S(f,g) = \frac{M}{lt(f)} \cdot f - \frac{M}{lt(g)} \cdot g \text{ w.r.t. to } G$$

is 0, where $M = lcm(lm(f), lm(g))$.

Note: $lt\left(\frac{M}{lt(f)} \cdot f\right) = M = lt\left(\frac{M}{lt(g)} \cdot g\right)$, so the leading terms cancel.

Pf "$\Rightarrow$" Apply Cor 8.~~6~~6 to $S(f,g) \in I$.

"$\Leftarrow$" Let $0 \neq f \in I$. Write

$$f = \lambda_1 g_1 H_1 + \dots + \lambda_r g_r H_r \qquad (I)$$

with $0 \neq g_i \in G$ and monomials $H_i \in S$ with minimal $M := \max_{1 \leq i \leq r} (\mathrm{lm}(g_i H_i))$. $\lambda_i \in K^\times$

Clearly $\mathrm{lm}(f) \leq M$.

If $\mathrm{lm}(f) = M$, then $\mathrm{lm}(f) = \mathrm{lm}(g_i H_i)$
$= \mathrm{lm}(g_i) \cdot H_i$,

so $\mathrm{lm}(f)$ is divisible by the leading mon. of an element of G.

Assume $\mathrm{lm}(f) < M$.

$\Rightarrow$ the monomial M has to cancel in the RHS of (I).

w.l.o.g. $\mathrm{lm}(g_i H_i) = M$ for $i = 1, \dots, t$
$\mathrm{lm}(g_i H_i) < M$ for $i = t+1, \dots, r$

$$\Rightarrow \sum_{i=1}^{t} \lambda_i \, \mathrm{lc}(g_i) = 0. \quad (\text{in part., } t \geq 2)$$

By assumption, we can write

$$\frac{M}{\mathrm{lcm}(\mathrm{lm}(g_i), \mathrm{lm}(g_1))} \cdot S(g_i, g_1) = \frac{M}{\mathrm{lt}(g_i)} \cdot g_i - \frac{M}{\mathrm{lt}(g_1)} \cdot g_1$$

$$= \sum_j p_j^{(i)} \cdot q_j^{(i)}$$

with $0 \neq p_j^{(i)} \in G$ and $q_j^{(i)} \in K[x_1, \dots, x_n]$,

and $\mathrm{lm}(p_j^{(i)} \cdot q_j^{(i)}) \leq \mathrm{lm}\left(\frac{M}{\mathrm{lt}(g_i)} g_i - \frac{M}{\mathrm{lt}(g_1)} \cdot g_1\right)$

$< M$.

$$\Rightarrow g_i H_i = \frac{\mathrm{lt}(g_i) H_i}{M} \cdot \sum p_j^{(i)} q_j^{(i)}$$

$$+ \frac{\mathrm{lt}(g_i) H_i H_1}{\mathrm{lt}(g_1) H_1} \cdot g_1 \qquad \text{for } i = 1, \dots, t$$

$$= \mathrm{lc}(g_i H_i) \cdot \sum p_j^{(i)} q_j^{(i)} + \frac{\mathrm{lc}(g_i) H_1}{\mathrm{lc}(g_1)} \cdot g_1$$

$\Rightarrow \lambda_1 g_1 H_1 + \dots + \lambda_t g_t H_t$

$$= \sum_{i=1}^{t} \underbrace{\lambda_i \mathrm{lc}(g_i H_i)}_{\in K} \cdot \underbrace{\sum \overbrace{p_j^{(i)}}^{\in G} q_j^{(i)}}_{\mathrm{lm}(\cdot) < M} + \underbrace{\sum_{i=1}^{t} \frac{\lambda_i \mathrm{lc}(g_i)}{\mathrm{lc}(g_1)}}_{0} \cdot g_1 H_1$$

$\Rightarrow$ We can rewrite f as a sum as in (I)

with smaller $M = \max_{1 \leq i \leq r} (\mathrm{lm}(g_i H_i))$. $\lightning$

$\square$

<u>Similar to:</u>

$\{(a_1, \dots, a_n) \mid a_1 + \dots + a_n = 0\}$ is spanned by

$e_i - e_j$ for $1 \leq i, j \leq n$.