However,

Theorem. Fix a monomial ordering on $R = \mathbb{F}[x_1, \dots, x_n]$ and a Gröbner basis $\{g_1, \dots, g_m\}$ of an ideal I. Then

(a) Every $f \in R$ is uniquely $f = f_I + r$ where $f_I \in I$, and r has no monomials divisible by any $\mathrm{in}(g_i)$

(b) The division algorithm computes f_I and r independently of the choices

(c) $\boxed{f \in I \iff r = 0}$

Pf (a) Existence: ok by division algorithm

Uniqueness: Sup $f = f_I + r = f_I' + r'$

Then $\underset{\substack{\uparrow \\ \text{monomial}}}{\mathrm{in}(r-r')} \in \mathrm{in}(I) = \langle \mathrm{in}(g_1), \dots, \mathrm{in}(g_m) \rangle$

(HW1 #5) So $\mathrm{in}(r-r')$ is a multiple of some $\mathrm{in}(g_i)$, a contradiction, unless $r - r' = 0$.

(b) Clear by (a).

(c) $\Leftarrow$: trivial

$\Rightarrow$: $f = f + 0$ is the unique expression. ∎

Lemma If $I = \langle f \mid f \in S \rangle$ then $I = \langle f \mid f \in T \rangle$ for a finite subset $T \subset S$.

Pf. Let $I = \langle h_1, \dots, h_n \rangle$ (by Hilbert) and write h_i in terms of finitely many terms of S. Those will do ∎

Prop $<$ monomial order

I ideal

(a) If $g_1, \dots, g_m \in I$ satisfy $\mathrm{in}(I) = \langle \mathrm{in}(g_i) \mid 1 \le i \le m \rangle$ then $I = \langle g_i \mid 1 \le i \le m \rangle$ (so $\{g_i\}$ = Gröbner basis)

(b) $\boxed{I \text{ has a Gröbner basis.}}$

Pf. (a) Let $f \in I$. Use division algorithm to write

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

Since $r \in I \longrightarrow \mathrm{in}(r) \in \mathrm{in}(I) = \langle \mathrm{in}(g_i) \rangle$

So some $\mathrm{in}(g_i) \mid \mathrm{in}(r)$ ($\Rightarrow\Leftarrow$)

or $r = 0$, and $f \in \langle g_i \rangle$.

(b) $\mathrm{in}(I) = \langle \mathrm{in}(f) \mid f \in I \rangle$

$\downarrow$ lemma

$\mathrm{in}(I) = \langle \mathrm{in}(f) \mid f \in J \rangle$ for $J \subset I$ finite.

Then J will do. ∎

How do you recognize a Gröbner basis?

To cancel the leading terms of f and g we do:

$$S(f,g) = \frac{M}{\mathrm{in}(f)} f - \frac{M}{\mathrm{in}(g)} g \qquad M = \text{(monic) lcm of } \mathrm{in}(f), \mathrm{in}(g)$$

Buchberger's Criterion

Given $<$, I, $G = \{g_1, \dots, g_m\}$ generating I:

G Gröbner basis $\iff \forall i,j$. $S(g_i, g_j)$ leaves remainder 0 upon division by g_1, then g_2, then…, then g_m

Pf. See Dummit-Foote or Eisenbud.