Math 3032 (18 March 2021)

$x_1 = x \quad x_2 = y$

HW 7 due today.

optional HW due Tuesday.

HW 8 due next week.

Today: Continue from last time on construction of Gröbner bases.

Goal: Start with some explicit but complicated description of an ideal $I \subseteq \mathbb{F}[x_1, \dots, x_n] =: \mathbb{F}[\vec{x}]$ (basis)

Want "simpler" description. The following operations take bases to bases (for the same ideal)

- reorder
- remove 0
- append any elt of I
- rescale basis elts by nonzero ("scalars" = elts of $\mathbb{F}^\times$ = constant polynomials)
- if $f(\vec{x}), g(\vec{x}) \in$ basis, replace $f(\vec{x}) \rightsquigarrow f(\vec{x}) - c(\vec{x})\, g(\vec{x})$ (arbitrary in $\mathbb{F}[\vec{x}]$)

E.g. starting basis:

$x^2y^3 \simeq x^2y^3 + x^2 + 2$ $\quad = f(x,y)$

$- xy(xy^2 + y^3 + 3)$

$- xy^4 + x^2 - 3xy + 2$

$+ y^2(xy^2 + y^3 + 3)$

$x^2 - 3xy + y^5 + 3y^2 + 2$

Agree: $x \gg y \gg 1$ "simpler" means smaller largest term.

$xy^2 + y^3 + 3 \simeq xy^2$

$\quad = g(x,y)$

N.B: these replacements are a mix of long div and row echelon reduction.

If we get stuck, append a third basis vector

$y^2(x^2 - 3xy + y^5 + 3y^2 + 2) - x(xy^2 + y^3 + 3)$

$= -3xy^3 - xy^3 - 3x + y^7 + 3y^4 + 2y^2$

E.g. current basis:

$x^2 - 3xy + y^5 + 3y^2 + 2$ | $xy^2 + y^3 + 3$ | $-4xy^3 - 3x + y^7 + 3y^4 + 2y^2$ | ...

$h(x,y)$ | g | $S(x,y)$

Now start dividing into S by other basis vectors.

$$+4y^2(xy^2 + y^3 + 3)$$

$$-3x + y^7 + 4y^5 + 3y^4 + 12y^2$$

$\rightsquigarrow x + -\frac{1}{3}(\quad) = x + p(y)$

replace h:

$h(x,y) - (x - 3y)(x + p(y))$

= some poly just in y.

$a(y)$

replace g:

$g - y^2(x + p(y))$

some poly in y.

$b(y)$.

by dividing these into each other $\rightsquigarrow$ some $\gcd(a,b) = z(y)$.

We will end up computing polys $p(y)$, $q(y)$ s.t.

$$I = \langle x + p(y),\ q(y) \rangle.$$

Common zeros of $f(x,y)$ and $g(x,y)$ (i.e. common solns to $f(x,y)=g(x,y)=0$)

$\equiv$ common zeros of $x+p(y)$, $q(y)$.

either by
- factoring if you can
- Newton's alg. (calculus)

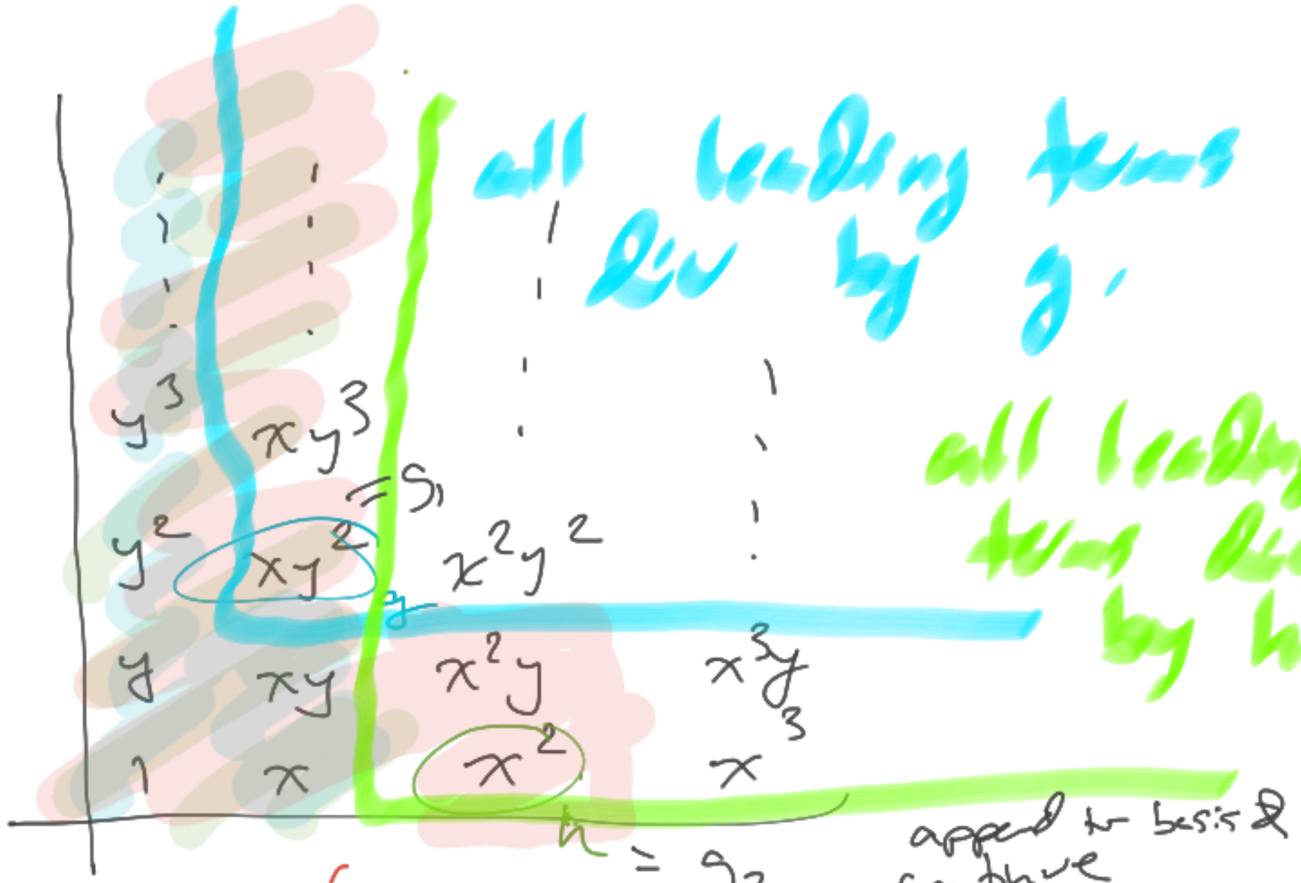
get a good sense of zeros of $q(y)$.

each zero of $q(y)$ will give a unique zero of $x + p(y)$, namely

$$x = -p(y).$$

Mostly: just long div.

Only nontriv. part was when no two basis vectors (leading terms of div. by each other. In this case:



$\forall$ pair of basis vectors $g_i(\vec{x})$, $g_j(\vec{x})$, write down $S_{ij}(\vec{x})$

$$= m_i(\vec{x}) g_i(\vec{x}) + m_j(\vec{x}) g_j(\vec{x})$$

m_i = monomials minimal to create a cancellation.

divide into S by g's

Either:
- get to 0.
- get smaller than every g.

$\Leftarrow$ append to basis & continue the alg.

This motivates the following definition:

Depends on a choice of ordering $x_1 >> x_2 >> \dots >> x_n$

Defn: A **Gröbner** basis for $I \subseteq \mathbb{F}[\vec{x}]$ is a basis $g_1(\vec{x}), \dots, g_r(\vec{x})$ s.t. $\forall f(\vec{x}) \in I$, $\exists g_i(\vec{x}) \in$ basis s.t. leading term of g_i divides leading term of f.

Awesome because then it is algorithmic to write $\forall f \in I$

$$f(\vec{x}) = \sum_{i=1}^{r} c_i(\vec{x})\, g_i(\vec{x}) \qquad c_i(\vec{x}) \in \mathbb{F}[\vec{x}].$$

Algorithm: Pick g_i s.t. $\downarrow$. Run long div:

$$f(\vec{x}) = c_i(\vec{x})\, g_i(\vec{x}) + \underbrace{\text{remainder}}_{\in \text{ still in } I}.$$

So repeat. Pick g_j "dividing" remainder. Divide. Etc.

"leading term"

Algorithm for finding a Gröbner basis:

(0) Find any basis.

(1) Use long div as much as possible using $g_1(\vec{x}), \ldots, g_r(\vec{x})$.

(2) When that runs out of steam, inspect

$S_{ij}(\vec{x})$ (from slide 5).

Divide into them by g's. Either:

↳ (a) get something smaller than the g's.
append it and return to step 1.

or: ↳ (b) all $S_{ij}(\vec{x})$'s can be reduced to 0 by dividing by $g_k(\vec{x})$'s.

Thm: If (5), then the basis $g_1(\vec{x}) \ldots g_r(\vec{x})$ is Gröbner.

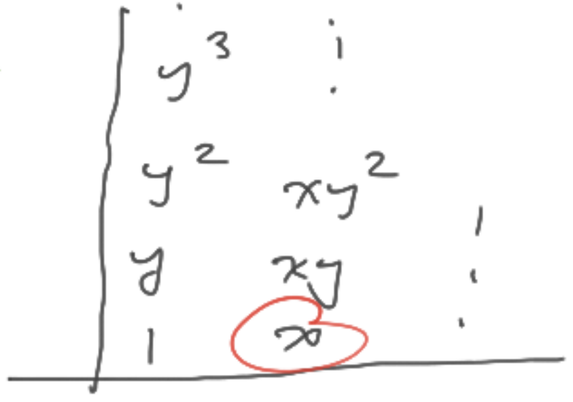
Proposition: In one-variable case, every $I = \langle p(x) \rangle$ for some p. Basis is Gröbner iff it contains this p.
multiple of
In particular, any singleton basis is Gröbner.

Proposition: In two-variable case, $\forall p(y), q(y) \in \mathbb{F}[y]$ any basis of form $\langle x + p(y), q(y) \rangle$ is Gröbner.

(There are plenty of Gröbner bases not of this form.)

Any poly at all (including those in I) that contains an x will be (eading by $x + p(y)$.

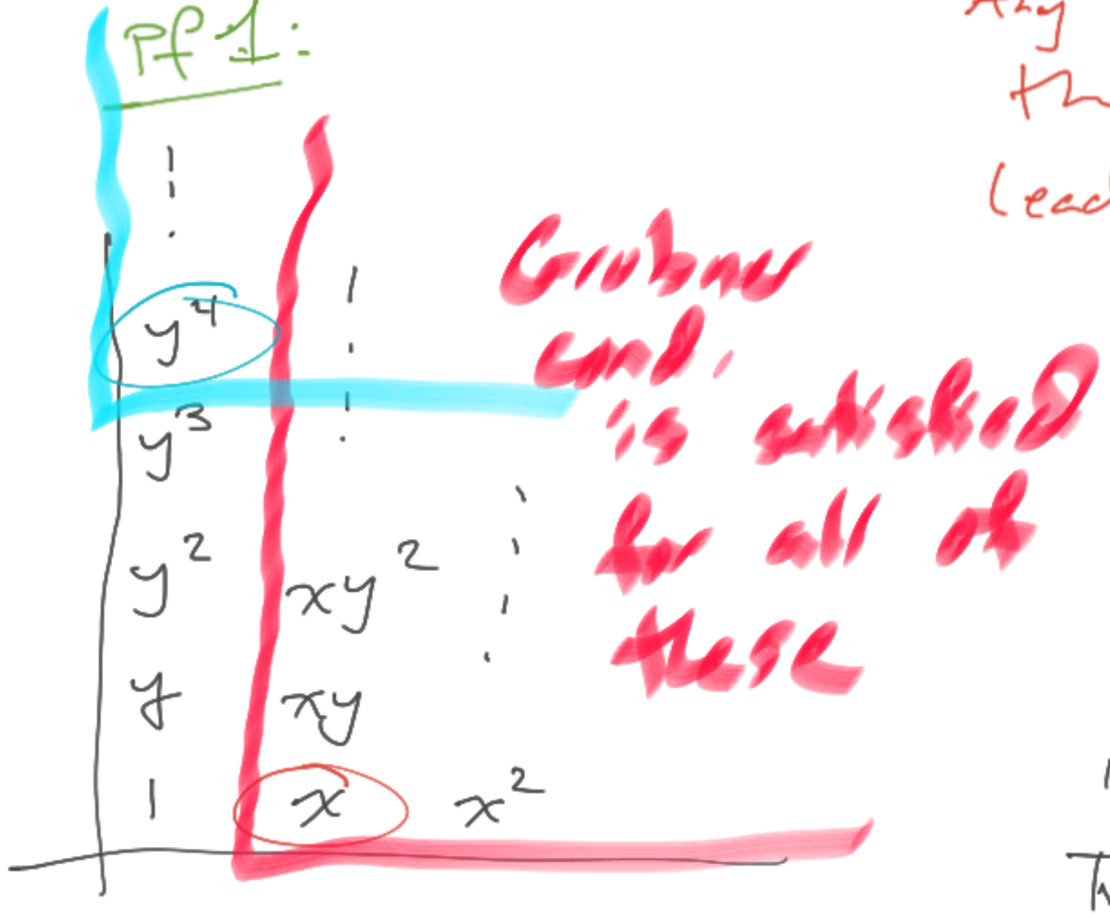
Pf:



Proposition: In two-variable case, $\forall\, p(y), z(y) \in \mathbb{F}[y]$ any basis of form $\langle x + p(y), z(y) \rangle$ is Gröbner.

(There are plenty of Gröbner bases not of this form.)

Pf 1:



Any poly at all (including those in I) that contains an x will be leading el. by $x + p(y)$.

Only issue are elts of $I \cap \mathbb{F}[y]$.

eg. $\deg z = 4$

If $f(y) \in I$

$$\| $$

$$a(x,y)(x + p(y)) + b(x,y)\, z(y).$$

If $a \neq 0$ then this contains x so $a \equiv 0$.

Then $b \in \mathbb{F}[y]$. So $\deg f \geq \deg z$. ∎

Pf 2: In special case where $g(y)$ has $\deg(g)$ distinct zeros,

We saw already that every zero of $g(y)$ was a zero of $x + p(y)$. Hence a common zero of all $f(x,y) \in I$.

So every $f \in I$ has at least $\deg(g)$ zeros.

So $\deg(f) \geq \deg(g)$.

Let S is a set.

Defn: A preorder on S is a binary relation "$\leq$"

s.t.

[reflexivity] $a \leq a \quad \forall a \in S$

[transitivity] If $a \leq b$ and $b \leq c$ then $a \leq c$.

Define $a \simeq b$ if $a \leq b$ and $b \leq a$.

A partial order is a preorder s.t.

if $a \simeq b$ then $a = b$.

Lemma: If $\leq$ is a preorder, then $\simeq$ is an equiv on S.

And $S/\simeq$ is partially ordered by $\leq$.

Given a preorder $\leq$,

a and b are comparable if $a \leq b$ or $b \leq a$ (or both).

and incomparable if $a \not\leq b$ and $b \not\leq a$

A preorder is total if there are no incomparable pairs.

A total order is total and a partial order.

Law of excluded middle: $\forall a, b$

exactly one of:

$a < b$, $a = b$, or $a > b$.

$< \leq$ and $\neq$.

E.g.: • $\leq$ on $\mathbb{Z}$ is a total order.

• divisibility on $\mathbb{N}$ is a partial order.

• divisibility on $\mathbb{Z}$ is a preorder (not partial order).

• $\lesssim$, $\approx$ on $\mathbb{F}[\vec{x}]$ is a total preorder.

A preorder is <u>well</u> if "least elt" ✓

- every nonempty subset contains an elt w/ nothing smaller.

equiv:

- every decreasing sequence $a_1 \geq a_2 \geq \dots$ eventually stabilizes ← $\exists N$ s.t. $a_N \approx a_{N+1} \approx a_{N+2} \approx \dots$] ↙ i.e. no infinite strictly decreasing sequences.

"well order" usually includes total order.

Recursion:
- initial step
- $n \to n+1$ recursion step.

very good for $\mathbb{N}$ indexing the cases.

Induction:
- base case
- induction case.

Strong recursion:
- replace by something smaller

If well ordered: always terminate

Strong induction:
- explain how to convert any counter example to a smaller one.

give proofs.