Groebner basis theory

Books:
Eisenbud Chapter 15
Dummit and Foote Section 9.6

We have seen how effective it is to compute with monomial ideals of $S = k[x_1, \dots, x_n]$

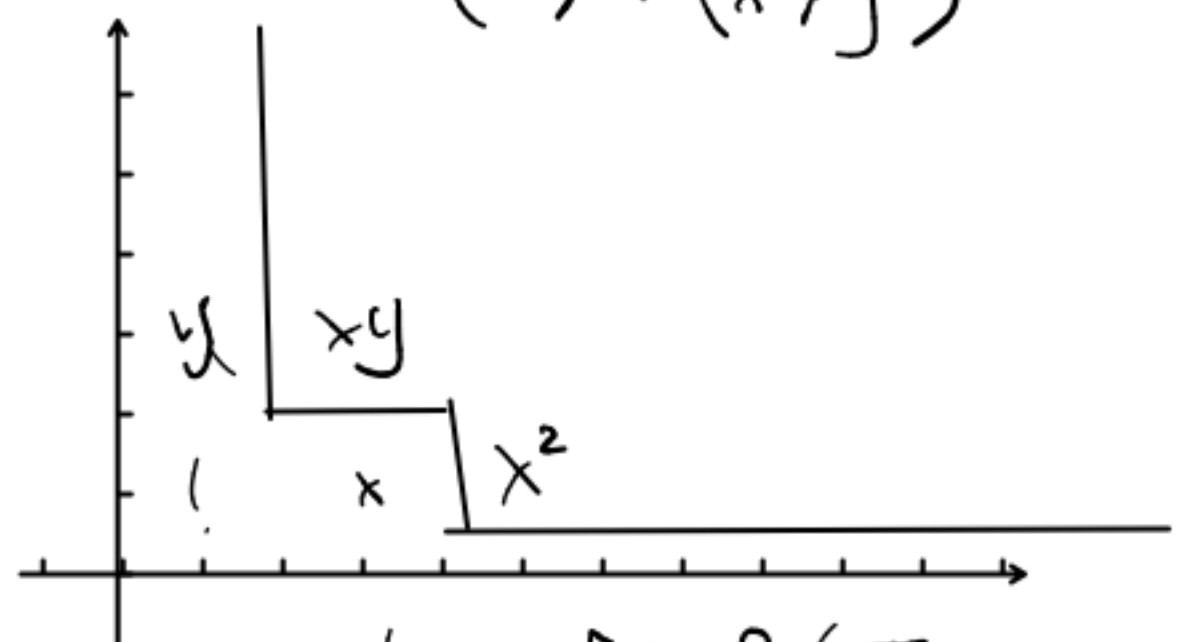
Definition. A <u>monomial</u> of S is a product $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} = x^a$ where $a = (a_1, \dots, a_n) = \partial(x^a)$ is the <u>multidegree</u>.

Perhaps it is sometimes a scalar multiple?
A scalar multiple is called a <u>term</u>.

A monomial ideal I is one generated by monomials.
It has a k-basis of monomials.

We have seen e.g. we can compute intersections of m. ideals.

$$(x^2, xy) = (x) \cap (x^2, xy, y^2)$$
$$= (x) \cap (x^2, y)$$



We see a basis for S/I
e.g. $\bar{1}, \bar{x}, \bar{y}, \bar{y}^2, \dots$

We can easily compute the Hilbert function & Poincaré series of S/I.

We see that monomial ideals are finitely generated.

In fact we ~~know~~ ideals of S are all finitely gen'd.

Gordan's 1900 proof of Hilbert's basis theorem used this.

Proof of Hilbert's basis theorem

Definition. A basis for an ideal is a set of ideal generators ~~for~~ the ideal.

Hilbert's Basis Theorem.
If R is a Noetherian ring then so is the polynomial ring R[x].
Every ideal of R[x] has a finite basis.

Proof.
Let $I \subset R[x]$ be an ideal.
Let
$L = \{$leading coefficients of elements of $I\}$
Claim: this is an ideal of R.
(Proof $f = ax^d + \text{lower} \in I$
$g = bx^e + \text{lower} \in I$
then $ra - b$ is either 0 or the leading coeff of $rx^e f - x^d g$)
L is fintely generated by
$a_1, \ldots, a_n \in R$.
Let $f_i \in I$ have leading coeff a_i
Put $e_i = \deg f_i$, $N = \max\{e_1, \ldots, e_n\}$
If $0 \leq d \leq N-1$ put
$L_d = \{$leading coeffs of polys in I of degree $d\}$
This is also an ideal.
$L_d = (b_{d,1}, \ldots, b_{d,n_d})$. $b_{ij} \in R$
Find $f_{d,i} \in I$ of degree d
with leading coeff $b_{d,i}$.

Claim:

$I = (\{f_1, \ldots, f_n\} \cup \{f_{d,i} \mid 0 \le d < N, 1 \le i \le n_d\})$

(Pf. Let I' be the ideal on the right.

$I' \subseteq I$. If $\neq$, pick $f \in I - I'$ of least degree.

If $\deg f \geq N$ then its leading coeff is a combn of $a_1, \ldots, a_n$.

Let g = same combn of $x^{\deg f - \deg f_i} f_i \in I$

Now $f - g \in I - I'$ has smaller degree than f.

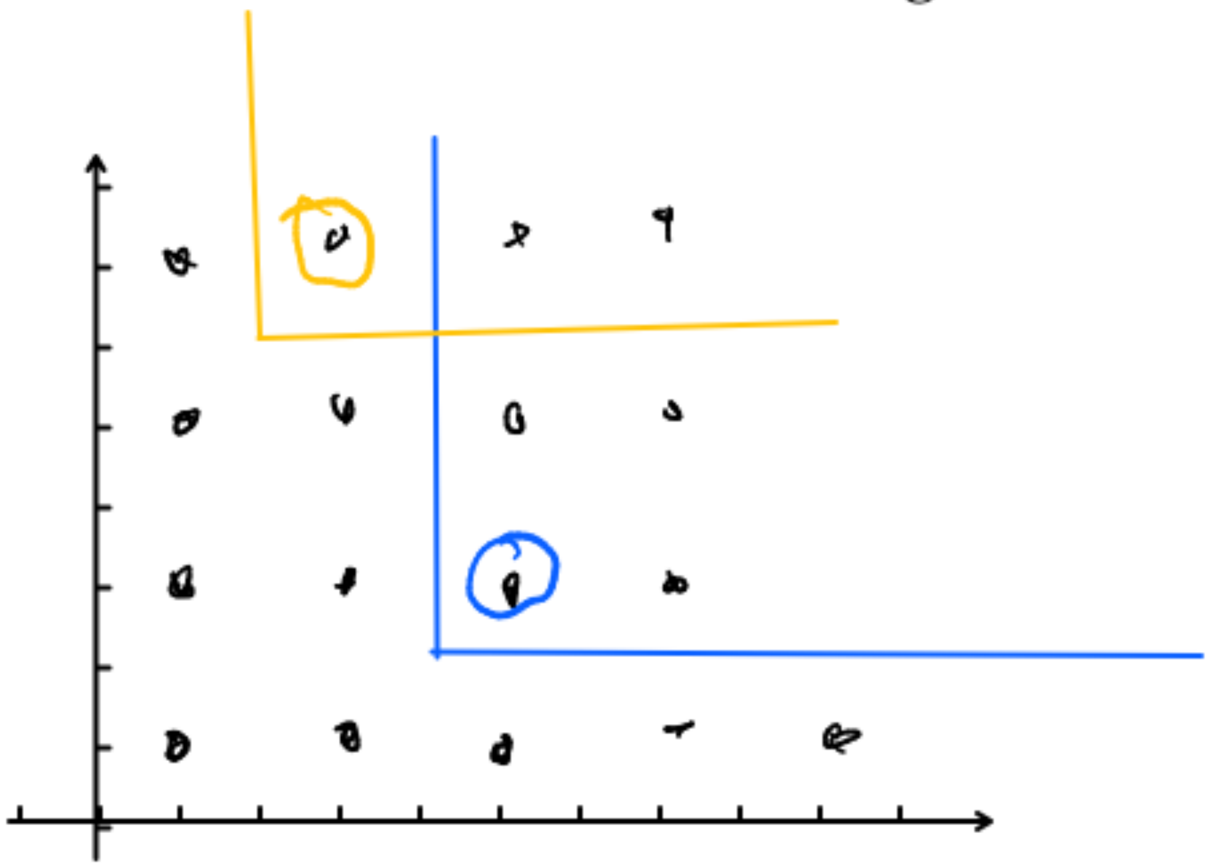
Contradiction.

Similar if $\deg f < N$. Find g = combn of $f_{\deg f, i} \in I'$ with same leading term as f. Now $f - g \in I - I'$ has smaller degree than f. contradiction. $\square$

Pre-class Warm-up!!

Consider the following:

Proposition.
Monomial ideals of $S = k[x_1, \ldots, x_d]$ satisfy ACC:
If J is a monomial ideal of S, every set of monomials that generates it contains a finite set of monomials that generates it.



Use Dickson's Lemma:
Given infinitely many vectors $v_1, v_2, \ldots$ in N^r, there exists $i < j$ with $v_i \leq v_j$, where $\leq$ means coordinate-by-coordinate comparison.

This means $\mathbb{N}^r$

Any sequence in $\mathbb{N}$ contains a weakly increasing sequence. (Find a smallest element in the sequence. In the elements ~~that~~ follow, find a smallest element. Repeat)

Now find a weakly increasing sequence of first coordinates. Among those, find a weakly increasing sequence in the second coordinate. Repeat

If a generating set have no finite subset we could find a sequence contradicting Dickson.

Monomial orders

Recall: $S = k[x_1, \ldots, x_n]$.
A monomial is an expression $x^a = x_1^{a_1} \cdots x_n^{a_n}$
A term is a scalar multiple of a monomial.

Definition.
A monomial ordering is one of the following equivalent relations on the set of monomials:

1. A well-ordering $\geq$ on {monomials} such that $u \geq v$ implies $mu \geq mv$ always.

2. A total order on {monomials} such that $u \geq v$ implies $mu \geq mv$, and $m \geq 1$ always.

Is it obvious that 1. $\Rightarrow m \geq 1 \ \forall m$?

Examples of monomial orders:

The lexicographic order:
$x_1 > x_2 > \cdots > x_n$
$x_1^{a_1} \cdots x_n^{a_n} \geq x_1^{b_1} \cdots x_n^{b_n}$
$\Leftrightarrow$ the earliest $a_i \neq b_i$ has $a_i \geq b_i$

Homogeneous lexicographic
$u > v \Leftrightarrow \deg u > \deg v$
or $\deg u = \deg v$ and $u >_{lex} v$.

More definitions. Let $f \in S$

Fix a monomial ordering on S = k[x_1, ... ,x_n].

Extend the order to terms.

The leading term (or initial term) LT(f) is

the largest term in f.

If I is an ideal of S, the ideal of leading terms is

LT(I) = (LT(f) | f is in I)

= the ideal generated by the leading terms of polynomials in I.

It is a monomial ideal.

Is it obvious that every monomial in LT(I) is the LT f some $f \in I$?

Examples (page 318 of D & F)

S = k[x,y]. Lexicographic order x > y.

Let f = x^3y - xy^2 + 1, g = x^2y^2 - y^3 - 1

LT	x^3y	x^2y^2
∂	$(3,1)$	$(2,2)$

Observe yf - xg = x + y lies in J = (f,g)

LT = x

We see: LT(J) ≠ (LT(f), LT(g)). $\not\ni x$

Question: if y > x, what are LT(f) and LT(g) ?

$\mathrm{LT}(f) = -xy^2$, $\mathrm{LT}(g) = -y^3$

Proposition (Macaulay, see 15.3 of Eisenbud)
Let J be an ideal of S.
The (images of the) monomials of S not in LT(J) are a k-linear basis for S / J.

Proof. Let B be the set of monomials not in LT(J)

They are lin. ind modulo J

If $p = \sum_{m_i \in B} u_i m_i \in J$, $u_i \in k$.

$LT(p) \in LT(J)$. $LT(p)$ is one of the $m_i \notin LT(J)$. Contradiction

We show They span: $\underbrace{\langle B \rangle}_{\text{span of } B} + J = S$

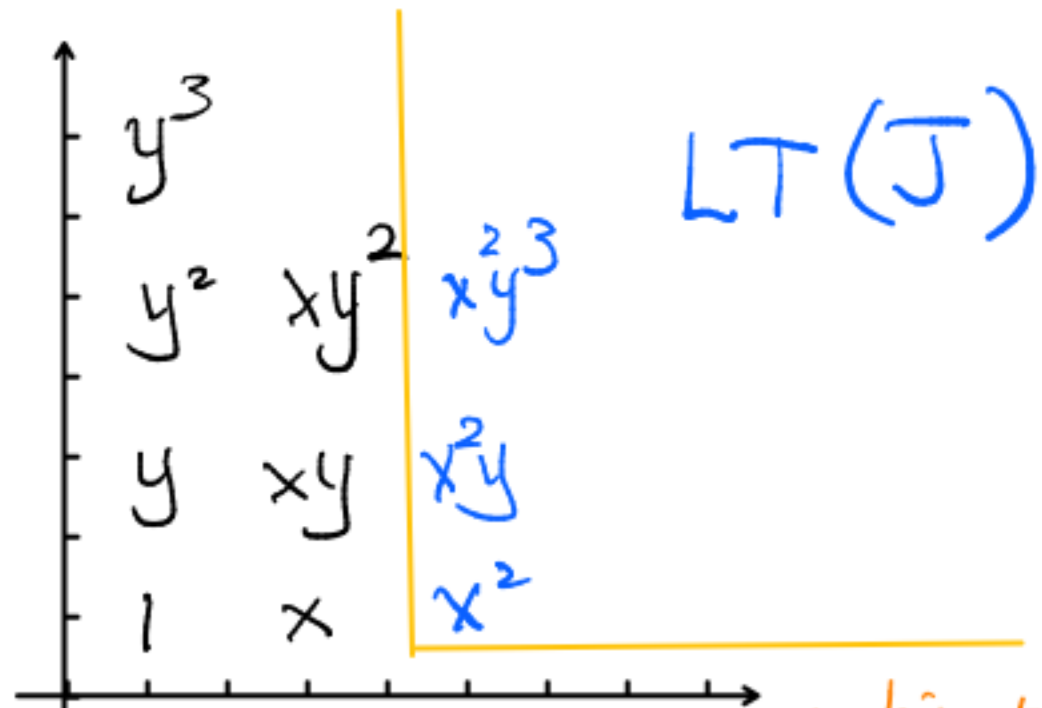
If $\neq S$, pick $f \in S - (\langle B \rangle + J)$ with $LT(f)$ minimal. If $LT(f) \in B$ Then $f - LT(f) \in S - (\langle B \rangle + J)$ has smaller LT. O/w $LT(f) = LT(g)$, $g \in J$. Now $f - g \notin \langle B \rangle + J$, and has smaller LT.

Example: J = (x^2 - y^3)

$x > y$

(x^2)

The monomials not in (x^2) do give a basis for S/J.



Each f in S determines ~~one~~ a linear combination of these basis elements as the coset representative of its coset f + J. Groebner methods give a way to compute this, and in particular determine whether f is in J.

We can compute Samuel functions.

To compute the Samuel function for the maximal ideal $(\bar{x},\bar{y})$ of $k[x,y] / (x^2 - y^3)$, for example, compute the leading term ideal for each of $(x,y)^n + (x^2 - y^3)$. Then get a basis for the quotient by this ideal, whose size is part of the information we need.

Definition.
A Groebner basis for an ideal J in S is a finite set g_1, ... , g_d of elements of J so that the leading terms LT(g_1), ... , LT(g_d) generate LT(J).

Examples.
1. $J = (x^2 - y^3)$ has $x^2 - y^3$ as G. basis because $LT(J) = (LT(x^2-y^3))$

2. $J = (f, g)$ as before doesn't have f, g as a G. basis
In fact $x+y$, and another polynomial in J with $LT = y^4$ is a G. basis.
such as
$g(y^3 - xy^2)(x+y) = y^4 - y^3 - 1$

Proposition. If g_1, ... , g_d is a Groebner basis, it generates J.

Proof.
Let g_1, ... ,g_d be a Groebner basis for J and let L = (g_1, ... ,g_d) be the ideal it generates, so L is contained in J.
Pick f in J - L with least leading term among such f. Write LT(f) = LT(g) for some polynomial g in L. Then f - g lies in J - L has smaller LT, a contradiction.
Note: $LT(L) = LT(J)$ because it is generated by LTs of polynomials in L.

Corollary.

Pre-class Warm-up!!!

Is the following a proof of Hilbert's basis theorem for $S = k[x_1, \ldots, x_d]$?

Theorem.
When k is a field, every ideal of $S = k[x_1, \ldots, x_d]$ is finitely generated.

Proof. Let J be an ideal of S. We have shown that J has a Groebner basis which, by definition, is finite. Therefore J is finitely generated. QED

A Yes ✓

Is this suddenly a much easier proof ?

General polynomial division

Fix a monomial ordering on S.
Let g_1, … , g_m be a set of non-zero polynomials.
Let f be a polynomial in S.
We will work with 'quotients' q_i and a 'remainder' r so that at the end

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

Each q_ig_i has multi degree $\leq \partial(f)$.
The remainder r has no nonzero term divisible by any LT(g_i).

Start with the q_i and r all equal to 0.
Successively test whether the leading term of the dividend f is divisible by the leading terms of the divisors g_1, … ,g_m, in that order.

Step 1. If LT (f) is divisible by LT(g_i), say, LT(f) = a_i LT(g_i), add a_i to the quotient q_i, replace f by the dividend f - a_ig_i (a polynomial with lower order LT) and reiterate the entire process. Go back to g_1.

Step 2. If the leading term of the dividend f is not divisible by any of the leading terms LT(g_1), n… , LT(g_m), add the leading term of f to the remainder r, replace f by the dividend f - LT(f), and reiterate the entire process

Example (D & F page 321)

$S = k[x,y]$, lexicographic order with $x > y$.

We divide $f = x^2+x-y^2+y$ $\quad LT(f) = x^2$

by $g_1 = xy+1$, $LT(g_1) = xy$ and

$g_2 = x+y$, $LT(g_2) = x$

Round 1.

LT(f) is not divisible by LT(g_1).

$q_1 = 0$, $q_2 = x$, $r = 0$

Replace f by $f' = f - xg_2 = -xy+x-y^2+y$

Round 2.

LT(f′) = -xy = -LT(g_1).

Replace f′ by f″ = f′ + g_1 = x - y^2 + y + 1.

Now q_1 = -1. Is $LT(f'')$ divis. by $LT(g_1)$? No.

LT(f″) = x = LT(g_2).

Replace f″ by f‴ = f″ - g_2 = -y^2 + 1.

Round 3.

LT(f‴) = -y^2 is not divisible by either LT(g_1) or LT(g_2).

Q_1 and q_2 stay the same.

r becomes -y^2.

Replace f‴ by f⁗ = f‴ + y^2 = 1.

Round 4.

LT(f⁗) = 1 is not divisible by LT(g_1) or LT(g_2).

q_1 and q_2 stay the same.

We stop.

We check that

f = q_1g_1 + q_2g_2 + r

If we change the order of g_1 and g_2,

so g_1 = x+y and g_2 = xy+1, we get

q_1 = x-y+1, q_2 = 0, r = 0

f = (x-y+1)(x+y) in (g_1, g_2).

In the last examples $g_1 = xy+1$, $g_2 = x+y$, note that these are not a Groebner basis for (g_1, g_2), because
$g_1 - yg_2 = 1 - y^2$ has LT $= -y^2$, and this does not lie in $(LT(g_1), LT(g_2))$.

$$= (xy, x) = (x)$$

The division algorithm failed to show that $f = x^2 + x - y^2 + y$ lies in (g_1, g_2), when done with one ordering of g_1 and g_2.

Theorem 23 of D & F.
Fix a monomial ordering.
Suppose {g_1, ... , g_n} is a Groebner basis for J.
Then
a. Every polynomial f can be uniquely written
f = f_J + r
where f_J in J and no nonzero monomial term of r is divisible by any of the leading terms LT(g_1), ... , LT(g_n).

b. Bothe f_J and r can be computed by general polynomial division by g_1, ... , g_n, independently of the order in which they appear.

c. The remainder r provides a unique representative for the coset of f in the quotient S/J

Proof. a. We have seen: the monomials not $LT(J)$ give a basis for S modulo J, so the k-linear combinations of such monomials are a set of coset reps for J in S. We can write any $f = f_J + r$, $f_J \in J$ where r is such a k-linear combn. No monomial term of r lies in $LT(J)$ i.e. is not divisible by any $LT(g_i)$, because they are a Groebner basis.

b. In the computation, at each stage we have $f = f_J' + r'$, $f_J' \in J$. If r' has any monomial in $LT(J)$, it would have been divisible by a $LT(g_i)$, because these generate $LT(J)$.

Finally:

Buchberger's Criterion provides a test for when a basis is a Groebner basis, and Buchberger's Algorithm provides a way to find a Groebner basis.

Let $(g_1, \ldots, g_n) = J$.

For each pair of g_i, g_j

Find minimal terms a, b so that

$a\,LT(g_i) = b\,LT(g_j)$.

Adjoin $a g_i - b g_j$ to the generators if it has a new leading term. Repeat.

Get a Groebner basis.

Let $g_1 = xy+1$ $\quad g_2 = x+y$

LT: xy $\qquad x$

$g_1 - yg_2 = 1-y^2 = g_3$

LT $-y^2$

$yg_1 + xg_3 = x+y$

LT $= x$ $\quad \in (xy, x, -y^2)$

Nothing new.

$y^2 g_2 + x g_3 = y^3 + x$

LT $= x$. Stop.

$J = (xy+1, x+y, 1-y^2)$

is a Groebner basis.

LT $\qquad xy \qquad x \qquad -y^2$

In fact:

$LT(J) = (x, -y^2)$

so $J = (x+y, 1-y^2)$

is a Gröbner basis.

Note

$xy+1 = y(x+y) + (1-y^2)$