Math 202C Lecture 1 4/2/18

Grading 100% HW

Qual
202 A 40%
B 40%
C 20%

April	M	W	F
		UPenn	
	2	⊗	6
	9	11	⊗ Nashville AMS Meeting
	16	18	20
	23	25	27

§ 1 Polynomials Rings $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots)$

Let $x_1, \ldots, x_n$ be variables, k a field. A polynomial in $x_1, \ldots, x_n$ over k is a finite expression of the form

$$f = f(x_1, \ldots, x_n) = \sum_{\alpha_1, \ldots, \alpha_n \geq 0} c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \text{ where } c_{\alpha_1, \ldots, \alpha_n} \in k.$$

Write $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$, so $f = \sum_{\alpha} c_\alpha \cdot x^\alpha$.

$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is a monomial, c_α is a coefficient, and $c_\alpha \cdot x^\alpha$ is a term.

$k[x_1, \ldots, x_n] = \{\text{all polynomials in } x_1, \ldots, x_n / k\}$ (a commutative ring and a k-vector space).

Def Let R be a (commutative, associative with 1) ring. Basis $\{x^\alpha : \alpha \in \mathbb{Z}_{\geq 0}^n\}$

An ideal is a subset $I \subseteq R$ s.t.

① $(I, +)$ is a subgroup of $(R, +)$

② If $r \in R$ and $i \in I$ then $r \cdot i \in I$.

- $0, R$ (trivial)

Ex - $R = \mathbb{C}[x,y]$,

$$I = \{ f \in R : f(a,b) = 0 \text{ for all } (a,b) \in \mathbb{Z}^2 \}.$$

Check I is an ideal in R.

Def Let R be a ring, $S \subseteq R$. The ideal gen'd by S is

$$\langle S \rangle := \{ f_1 \cdot g_1 + \cdots + f_r \cdot g_r : f_i \in R, g_i \in S \}.$$

Check! $\hookrightarrow = \bigcap_{S \subseteq I \subseteq R,\ I \text{ an ideal}} I$.

"Smallest ideal containing S."

Ex $R = \mathbb{C}[x,y]$

$$I = \langle x^2 + 3xy, y^2, x^2y, y^3 \rangle$$

$$= \langle x^2 + 3xy, y^2, x^2y \rangle \quad (\text{Redundancy})$$

Def Let $I \subseteq R$ be an ideal. A subset $S \subseteq R$ is a basis of I if $I = \langle S \rangle$. (eg $I = \langle I \rangle$.)

I is finitely generated if $\exists$ a finite subset $S \subseteq R$ s.t. $I = \langle S \rangle$.

Ex $R = \mathbb{C}[x_1, x_2, x_3, \dots]$

$= \{$ all polynomials in $x_1, x_2, \dots$ / $\mathbb{C}\}$

$I = \langle x_1, x_2, \dots \rangle$ is not finitely gen'd. (Check!)

Hilbert's Basis Theorem

Let $I \subseteq k[x_1, -, x_n]$ be an ideal. Then I has a finite basis.

(So can write $I = \langle f_1, \dots, f_r \rangle$ for some $f_1, -, f_r \in k[x_1, -, x_n]$.)

Q Given an ideal $I \subseteq k[x_1, -, x_n]$ with $I = \langle f_1, -, f_r \rangle$ and $f \in k[x_1, -, x_n]$, do we have $f \in I$? ($\Leftrightarrow \exists\ g_1, -, g_r \in k[x_1, -, x_n]$ st $f = g_1 f_1 + \text{—} + g_r f_r$.)

eg $3x^2yz + 7x^3z^2 + 8xy \overset{?}{\in} \langle 3xyz + 2y^2,\ 7xy + 8z^2,\ x^2 + 3xyz \rangle$.

Q Let $S, T \subseteq k[x_1, -, x_n]$. Do we have $\langle S \rangle = \langle T \rangle$?

Obs If $I \subseteq k[x_1, -, x_n]$ is an ideal, then $k[x_1, -, x_n]/I$ is a k-vector space.

$= \{f + I : f \in k[x_1, -, x_n]\}$

k-Spanning Set: $\{ x^\alpha + I : \alpha \in (\mathbb{Z}_{\geq 0})^n \}$.

k-basis? eg $k[x,y]/\langle x^2, xy, y^2 \rangle \overset{k\text{-basis}}{\rightsquigarrow} \{\overline{1}, \overline{x}, \overline{y}\}$

Q How to find a k-vector space basis for $k[x_1, -, x_n]/I$?

Def Let k be a field. Affine n-space over k is

$$\mathbb{A}^n_k := \{(\alpha_1, \alpha_2, \ldots, \alpha_n) : \alpha_i \in k\}.$$

Given a poly. $f(x_1, -, x_n) \in k[x_1, -, x_n]$, we get a function

$$f : k^n \longrightarrow k$$
$$(a_1, \ldots, a_n) \longmapsto f(a_1, \ldots, a_n).$$

Rmk - If $|k|$ is finite, then $f(x) \in k[x]$, $f(x) = \prod_{a \in k} (x-a)$ has $f(c) = 0$ for all $c \in k$, but $f \neq 0$ in $k[x]$.

- If $|k| = \infty$ and $f, g \in k[x_1, -, x_n]$ then

$$f = g \iff f = g \text{ (as functions } k^n \to k).$$

(as polynomials)

Def Let $S \subseteq k[x_1, -, x_n]$. The variety of S is $\mathbb{V}(S) \subseteq \mathbb{A}^n_k$, where $\mathbb{V}(S) = \{(a_1, -, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}$.

Ex · Over $\mathbb{R}$, $\mathbb{V}(x^2 + y^2 - 1) =$  $\subset \mathbb{R}^2$ $\mathbb{V}(x^2+y^2+1) = \emptyset$ ↑ not over $\mathbb{C}$!

$\mathbb{V}(x^2 + y^2 - 1, x) =$  $\subset \mathbb{R}^2$. $\{(0, \pm 1)\}$.

· $\mathbb{V}(\emptyset) = k^n$, $\mathbb{V}(1) = \emptyset$.

~~Def A subset $V \subseteq k^n$ is a variety if $\exists\ S \subseteq k[x_1,\dots,x_n]$ such that $V = \mathbb{V}(S)$.~~

Math 202C Lecture 2 4/6/18

Last Time $k[x_1,\dots,x_n]$ (k a field)

Ideals $I \subseteq \underbrace{k[x_1,\dots,x_n]}_{R}$ ⌜$(I,+)$ is a subgp of $(R,+)$, $r \in R,\ i \in I \Rightarrow ri \in I$⌟

$$\langle S \rangle = \{ r_1 s_1 + \cdots + r_\ell s_\ell : r_i \in R,\ s_i \in S \}$$

Affine n-space $\equiv k^n$

If $S \subseteq k[x_1,\dots,x_n]$, $\mathbb{V}(S) = \{ (c_1,\dots,c_n) \in k^n : f(c_1,\dots,c_n) = 0 \text{ for all } f \in S \}$.

Obs • $\mathbb{V}(S) = \mathbb{V}(\langle S \rangle)$ • $S \subseteq T \Rightarrow \mathbb{V}(S) \supseteq \mathbb{V}(T)$

Def A subset $V \subseteq k^n$ is a variety if $\exists\ S \subseteq k[x_1,\dots,x_n]$ s.t. $V = \mathbb{V}(S)$.

Fact $\{$all varieties in $k^n\}$ give the closed sets for a topology on k^n. "Zariski topology"

⌜① $\emptyset, k^n$ are varieties, ② if $V_1,\dots,V_m$ are varieties so is $V_1 \cup \cdots \cup V_m$, ③ if $\{V_\alpha\}$ is a family of varieties, then $\bigcap_\alpha V_\alpha$ is a variety.⌟

Def Given any subset $X \subseteq k^n$, the Zariski closure of X is

$$\overline{X} = \text{smallest variety containing } X = \bigcap_{X \subseteq V \subseteq k^n,\ V \text{ a variety}} V.$$

Ex ~~If $X = \mathbb{R} \subseteq \mathbb{C}$, then consider not,~~

Ex Let $n=1$. Then varieties in k^1 are...

k^1 $(\mathbb{V}(0))$, $\emptyset$ $(\mathbb{V}(1))$, any finite set $\{c_1,-,c_r\}\subseteq k$ $\mathbb{V}((x-c_1)-(x-c_1))$.

So if $k=\mathbb{C}$ then $\overline{\mathbb{Z}} = \mathbb{C}$ (Zariski closure!)

Q Given a subset $S \subseteq k[x_1,-,x_n]$, how do we "find" (eg draw) $\mathbb{V}(S) \subseteq k^n$?

Def Let $X \subseteq k^n$. The ideal of X is $\mathbb{I}(X) \subseteq k[x_1,-,x_n]$ given by $\mathbb{I}(X) = \{ f \in k[x_1,-,x_n] : f(c_1,-,c_n)=0 \ \forall\ (c_1,-,c_n)\in X\}$.

Obs ① $\mathbb{I}(X) = \mathbb{I}(\overline{X})$, ② $X \subseteq Y \Rightarrow \mathbb{I}(X) \supseteq \mathbb{I}(Y)$.

$V = \mathbb{V}(I)$: Ideals $I \subseteq k[x_1,-,x_n]$ → Varieties $V \subseteq k^n$

$I = \mathbb{I}(V)$: Varieties → Ideals

§ 2.1 Division in $k[x]$

Recall Polynomial division:

$$\begin{array}{r} x^2+2 \\ x^2-2 \overline{)\ x^4+1} \\ \underline{x^4-2x^2} \\ 2x^2+1 \\ \underline{2x^2-4} \\ 5 \end{array}$$

Recall $\deg(a_k x^k + \cdots + a_0) = k$ (with $a_k \neq 0$)

$$\Rightarrow \quad x^4+1 = (x^2+2)(x^2-2)+5$$

Division Thm Let $f, g \in k[x]$ with $g \neq 0$. $\exists!\ q, r \in k[x]$ s.t.

$$\boxed{f = q\cdot g + r}$$ where $\deg(r) < \deg(g)$ or $r=0$.

Fact · Let $I \subseteq k[x]$ be an ideal. $\exists\ g \in I$ st $I = \langle g \rangle$. 「$k[x]$ is a PID」

· If $f, g \in k[x]$ with $g \neq 0$ & $f = q \cdot g + r$ ($\deg r < \deg g$ or $r = 0$)

then $f \in \langle g \rangle \iff r = 0$.

Recall A polynomial $f = a_k x^k + \cdots + a_1 x + a_0 \in k[x]$ ($a_k \neq 0$) is monic if $a_k = 1$.

· We have $\langle f \rangle = \langle g \rangle$ for $f, g \in k[x]$ monic

$\iff f = g$.

· If $\deg f = k$, then $\{\bar{1}, \bar{x}, \ldots, \overline{x^{k-1}}\}$ is a k-basis for $k[x]/\langle f \rangle$.

Q How to extend this to n variables $x_1, \ldots, x_n$ ($n > 1$)?

§ 2.2 Monomial Orders

Q In $k[x,y]$, is "leading" $x^2 + y^2$ or "leading" $y^2 + x^2$?

Def Let S be a set. A (total) order on S is a binary rln $<$ s.t.

① $x \not< x$ for all $x \in S$,

② $(x < y$ and $y < z) \Rightarrow x < z$ for all $x, y, z \in S$.

③ If $x, y \in S$, then $x < y$, $y < x$, or $x = y$.

An order $<$ is a well order if for any nonempty $T \subseteq S$, T has a smallest element.

eg $(\mathbb{Z}_{\geq 0}, <)$ well order

($<$ = usual)

$(\mathbb{Z}, <)$ not a well order

$(\mathbb{Q}_{\geq 0}, <)$ not a well order b/c $\mathbb{Q}_{>0}$ has no smallest elt.

Recall $\{\text{all monomials in } k[x_1, \dots, x_n]\} \longleftrightarrow (\mathbb{Z}_{\geq 0})^n$

$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \longleftrightarrow (\alpha_1, \dots, \alpha_n) = \alpha$

Def A (total) order $<$ on monomials in $k[x_1, \dots, x_n]$ is a monomial order if

(1) $<$ is a well order, and

(2) if m, m', m'' are monomials, $m < m' \Rightarrow m \cdot m'' < m' \cdot m''$.

Ex (1) The lexicographic order $<_{lex}$

$x_1^{a_1} \cdots x_n^{a_n} <_{lex} x_1^{b_1} \cdots x_n^{b_n}$ if $\exists$ i s.t.

$a_1 = b_1, \ a_2 = b_2, \ \dots, \ a_{i-1} = b_{i-1}, \ a_i < b_i$.

So in $k[x,y]$, $1 < y < y^2 < \cdots < x < xy < xy^2 < \cdots < x^2 < x^2y < \cdots$

$f(x,y) = x^3 + 2xy^2 + x^2 \overset{lex}{\Rightarrow} x^3 + x^2 + 2xy^2$.

---

* The degree of a monomial is $\deg(x_1^{a_1} \cdots x_n^{a_n}) = a_1 + \cdots + a_n$.

The multidegree is $\text{multideg}(x_1^{a_1} \cdots x_n^{a_n}) = (a_1, \dots, a_n)$.

Def The graded lexicographic order $\prec$

$$m \prec_{grlex} m' \iff \deg(m) < \deg m' \text{ or } \left(\deg m = \deg m' \text{ and } m <_{lex} m'\right).$$

So $f(x,y) = \underbrace{x^2 + y^2 + y^{1000}}_{lex} = \underbrace{y^{1000} + x^2 + y^2}_{grlex}$

Def The graded reverse lexicographic order $\prec$

$$x_1^{a_1} \cdots x_n^{a_n} \prec_{grevlex} x_1^{b_1} \cdots x_n^{b_n} \iff$$

$a_1 + \cdots + a_n < b_1 + \cdots + b_n$ OR $a_1 + \cdots + a_n = b_1 + \cdots + b_n$ & $\exists\, i$ s.t. $a_{i+1} = b_{i+1}, \ldots, a_n = b_n$ and $a_i < b_i$.

Def Fix a monomial order $<$. Given $0 \neq f \in k[x_1, \ldots, x_n]$ with $f(x_1, \ldots, x_n) = c_m \cdot m + \sum_{m' < m} c_{m'} \cdot m'$ $\left(c_m \in k^*, m, m' \text{ monomials}, c_m \neq 0\right)$

the leading term is $LT(f) = c_m \cdot m$

the leading monomial is $LM(f) = m$

the leading coefficient is $LC(f) = c_m \in k$.

§ 2.3 Division in $k[x_1, \ldots, x_n]$

Ex Give $\mathbb{Q}[x,y]$ $<_{lex}$ w/ $x > y$.

Divide $f = xy^2 + 1$ by (f_1, f_2) where $f_1 = xy + 1$, $f_2 = y + 1$

$a_1: y$
$a_2: -1$

$f_1: xy+1$, $f_2: y+1$

$$\begin{array}{r|l} xy^2 + 1 & \\ -xy^2 + y & \\ \hline -y + 1 & \\ -y - 1 & \\ \hline 2 & \end{array}$$

$\Rightarrow$ $f = a_1 f_1 + a_2 f_2 + r$

where $a_1 = y$, $a_2 = -1$, $r = 2$.

Ex $\mathbb{Q}[x,y]$, lex order, $x > y$

Divide $f = x^2y + xy^2 + y^2$ by $(f_1 = xy-1,\ f_2 = y^2-1)$.

$a_1 : x+y$

$a_2 : 1$

$f_1 : xy-1$

$f_2 : y^2-1$

$$\begin{array}{r|l} x^2y + xy^2 + y^2 & r \\ \hline x^2y - x & \\ \hline xy^2 + x + y^2 & \\ xy^2 - y & \\ \hline x + y^2 + y & \longrightarrow\ x \\ \hline y^2 + y & \\ y^2 - 1 & \\ \hline y + 1 & \longrightarrow\ x + y + 1 \end{array}$$

$f = a_1f_1 + a_2f_2 + r$, $a_1 = x+y$, $a_2 = 1$, $r = x+y+1$.

DIVISION ALGORITHM in $k[x_1, \dots, x_n]$.

Input: Monomial order $<$, $f \in k[x_1, \dots, x_n]$, nonzero $f_1, \dots, f_s \in k[x_1, \dots, x_n]$

Output $a_1, \dots, a_s, r \in k[x_1, \dots, x_n]$ s.t.

(I) $f = a_1f_1 + \cdots + a_sf_s + r$

(II) $\text{multideg}(a_if_i) \le \text{multideg} f$ for $i = 1, 2, \dots, s$

(III) no term of r is divisible by any of $LT(f_1), \dots, LT(f_s)$.

Math 202c Lecture 3 4/9/2018

Last Time A monomial order $<$ on $(\mathbb{Z}_{\geq 0})^n$ is an order s.t.

① $<$ is a well order,

② if $\alpha, \beta, \gamma \in (\mathbb{Z}_{\geq 0})^n$, $\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$.

Given a m.o. $<$ & $f \in k[x_1, \dots, x_n]$ with $f \neq 0$, write

$$f(x_1, \dots, x_n) = c_\delta x^\delta + \sum_{\alpha < \delta} c_\alpha x^\alpha \quad \text{s.t.} \quad c_\delta \neq 0.$$ Then

$LT(f) := c_\delta x^\delta$, $LM(f) = x^\delta$, $LC(f) = c_\delta$.

§ 2.3 Division in $k[x_1, \dots, x_n]$

Ex $\mathbb{Q}[x,y]$ $<$ = lex. w/ $x > y$. $f = xy^2 + 1$ $f_1 = xy + 1$ $f_2 = y + 1$

Divide f by (f_1, f_2):

$a_1 : y$

$a_2 : -1$

$f_1 : xy+1$

$f_2 : y+1$

$$\begin{array}{r|l} xy^2 + 1 & \\ -xy^2 + y & \\ \hline -y + 1 & \\ -y - 1 & \\ \hline 2 = r & \end{array}$$

$\Rightarrow f = a_1 f_1 + a_2 f_2 + r$

with $a_1 = y$, $a_2 = -1$, $r = 2$.

Ex $\mathbb{Q}[x,y]$, $<$ = lex

$f = x^2y + xy^2 + y^2$

$f_1 = xy - 1$

$f_2 = y^2 - 1$

$a_1 : x + y$

$a_2 : 1$

$f_1 : xy - 1$

$f_2 : y^2 - 1$

$$\begin{array}{r|l} x^2y + xy^2 + y^2 & \\ x^2y - x & \\ \hline xy^2 + x + y^2 & \\ xy^2 - y & \\ \hline x + y^2 - y & \longrightarrow x \\ y^2 - y & \\ y - 1 & \\ \hline -y + 1 & \longrightarrow (x - y + 1) \end{array}$$

r

Multivariate Division

Input: monomial order $<$ on $k[x_1,\dots,x_n]$, $f, \underbrace{f_1,\dots,f_s}_{\neq 0} \in k[x_1,\dots,x_n]$

Output: $a_1,\dots,a_s, r \in k[x_1,\dots,x_n]$ s.t.

(1) $f = a_1 f_1 + \cdots + a_s f_s + r$

(2) $\text{multideg}(a_i f_i) \leq \text{multideg} f$ for $1 \leq i \leq s$

(3) no term in r is divisible by any of $LT(f_1), \dots, LT(f_s)$.

Ex $\mathbb{Q}[x,y]$, $x \overset{\text{lex}}{>} y$ Divide $f = x^2y + xy^2 + y^2$ by (f_1, f_2) where $f_1 = y^2 - 1$, $f_2 = xy - 1$

$a_1 : x + 1$

$a_2 : x$

r

$f_1: y^2-1$
$f_2: xy-1$

$x^2y + xy^2 + y^2$

$x^2y - x$

$xy^2 + x + y^2$

$xy^2 - x$

$2x + y^2 \longrightarrow 2x$

y^2

$y^2 - 1$

$1 \longrightarrow 2x+1$

$f = a_1 f_1 + a_2 f_2 + r$

$2x + 1$.

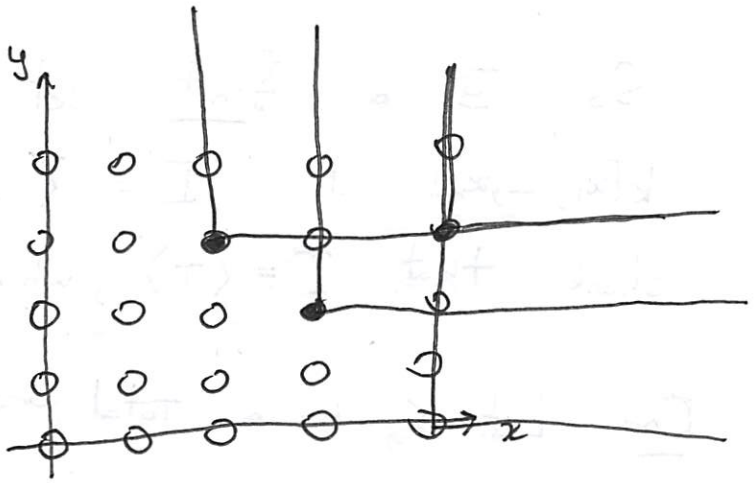
[remainder changed when we did $f_1 \leftrightarrow f_2$!]

§ 2.4 Monomial Ideals

Def An ideal $I \subseteq k[x_1,\dots,x_n]$ is a monomial ideal if $\exists$ a set S of monomials s.t. $I = \langle S \rangle$.

Ex $\langle x^2y^3, x^3y^2, x^4, x^4y^3 \rangle$

↑ redundant



Dickson's Lemma Let $I = \langle S \rangle$ be a monomial ideal in $k[x_n]$. $\exists$ $T \subseteq S$ finite such that $I = \langle T \rangle$.

Pf We induct on n. If $n=1$, then $I = \langle x^k \rangle$ where k is minimal s.t. $x^k \in S$.

If $n > 1$, write $y = x_n$, so $k[x_1, \dots, x_n] = k[x_1, \dots, x_{n-1}, y]$.

Let $J = \langle$ all monomials x^α in $k[x_1, \dots, x_{n-1}]$: $x^\alpha \cdot x^b \in I$ for some $b \geq 0 \rangle$.

By induction, $\exists$ a finite set $\{\alpha_1, \dots, \alpha_m\}$ st $J = \langle x^{\alpha_1}, \dots, x^{\alpha_m} \rangle$. For $1 \leq i \leq m$, $\exists$ b_i st $x^{\alpha_i} \cdot x^{b_i} \in I$; let $b = \max(b_1, \dots, b_m)$. For $0 \leq i \leq b$, let $J_i = \langle$ all monos $x^{\alpha^{(i)}}$ in $k[x_1, \dots, x_n]$: $x^{\alpha^{(i)}} \cdot x^i \in I \rangle$.

By induction, $\exists$ a finite set $\{\alpha_1^{(i)}, \dots, \alpha_{m_i}^{(i)}\}$ st $J_i = \langle x^{\alpha_1^{(i)}}, \dots, x^{\alpha_{m_i}^{(i)}} \rangle$.

We claim that I is gen'd by

$x^{\alpha_1^{(i)}} y^i, \dots, x^{\alpha_{m_i}^{(i)}} y^i$ $(0 \leq i \leq b)$ ⌜from J_i⌟

and $x^{\alpha_1} y^b, \dots, x^{\alpha_m} y^b$ ⌜from J.⌟

So $\exists$ a finite set T' of monomials in $k[x_1, \ldots, x_n]$ st $I = \langle S \rangle = \langle T' \rangle$. Now check that $I = \langle T \rangle$, where $T := S \cap T'$. ▨

Cor Let $<$ be a total order on monomials in $k[x_1, \ldots, x_n]$.

Then $<$ is a monomial order $\iff$

① $1 \leq m$ for all monos m,

② $m < m' \Rightarrow m \cdot m'' < m' \cdot m''$ always.

Pf "$\Rightarrow$" Suppose $<$ is a mon. order & $\exists$ m st $m < 1$.

Then $1 > m > m^2 > m^3 > \ldots$ is an infinite descending chain, so that $<$ is not a well order.

"$\Leftarrow$" Let S be a non-empty set of monomials. By Dickson's Lemma, $\exists$ $T \subseteq S$ finite s.t. $\langle S \rangle = \langle T \rangle$.

Let $m_0 \in T$ be $<$-smallest. If $m^N \in S$, then $m^N \in \langle T \rangle$ so $\exists$ $m' \in T$ st $m' \mid m$.

We have

$$1 \leq \binom{m}{m'} \Rightarrow m' \leq m, \text{ so } m_0 \leq m'$$

implies $m_0 = \min(S)$. Thus $<$ is a well-order. ▨

Math 202C Lecture 4 4/11/2018

Last Time Division in $k[x_n]$ (monomial order $<$)

Input $f, f_1, \dots, f_s \in k[x_n]$ ($f_1, \dots, f_s \neq 0$)

Output $a_1, \dots, a_s, r \in k[x_n]$ s.t.

- $f = a_1 f_1 + \cdots + a_s f_s + r$
- multideg $(a_i f_i) \leq$ multideg f for all i
- no term of r lies in $\langle LT(f_1), \dots, LT(f_s)\rangle$.

Qual Review
Tues 5/22
1-2PM
APM 5218

Dickson's Lemma Let $I = \langle S \rangle$ be a monomial ideal in $k[x_n]$ (S a set of monomials). $\exists\ T \subseteq S$ finite s.t. $I = \langle T \rangle$.

---

§ 2.5 Gröbner Bases

Def Fix a monomial order $<$ on $k[x_n]$ and let $I \subseteq k[x_n]$ be an ideal.

① The initial ideal of I is $LT(I) = \langle LT(f) : f \in I - \{0\}\rangle$.

② A finite subset $G = \{g_1, \dots, g_s\} \subseteq I$ is a Gröbner basis of I if $LT(I) = \langle LT(G)\rangle = \langle LT(g_1), \dots, LT(g_s)\rangle$.

Fact Every ideal $I \subseteq k[x_n]$ has a (finite!) Gröbner basis. (Dickson's Lemma)

Fact If G is a Gröbner basis for I, then $I = \langle G \rangle$.

Pf Clearly $\langle G \rangle \subseteq I$. If $f \in I$, write $G = \{g_1, \dots, g_s\}$ & perform division of f by $(g_1, \dots, g_s)$:

$$f = a_1 g_1 + \cdots + a_s g_s + r \quad , \text{ so } \quad r = f - \sum a_i g_i \in I.$$

If $r \neq 0$ then $LT(r) \in LT(I) = \langle LT(g_1), \dots, LT(g_s) \rangle$. $\not\in$

[**Hilbert's Basis Theorem** Let $I \subseteq k[x_n]$ be any ideal. Then I is finitely gen'd.]

Def Let R be a ring. R is **Noetherian** if whenever

$I_1 \subseteq I_2 \subseteq \dots$ is an ascending chain of ideals,

$\exists\ N$ s.t. $n \geq N \Rightarrow I_n = I_N$.

[$\Leftrightarrow$ every ideal $I \subseteq R$ is finitely gen'd.]

Rmk
- If R is Noeth. & $I \subseteq R$ then R/I is Noeth.
- If R is Noeth, so is $R[x]$.
- If R is Noeth & $S \subseteq R$ is a subring, S is NOT NECESSARILY Noeth!
  - $k[x_1, x_2, \dots] \subseteq k(x_1, x_2, \dots)$
  - $k[x, xy, xy^2, \dots] \subseteq k[x, y]$.

FACT Let $G = \{g_1, \dots, g_s\}$ be a Gröbner basis for $I \subseteq k[x_n]$ & let $f \in k[x_n]$. Write $f = a_1 g_1 + \dots + a_s g_s + r$ for division of f by $(g_1, \dots, g_s)$. Then $f \in I \Leftrightarrow r = 0$.

Pf $\Leftarrow$ ✓

$\Rightarrow$ $r = f - a_1 g_1 - \cdots - a_s g_s \in I$, so if $r \neq 0$

$LT(r) \in LT(I) = \langle LT(g_1), \ldots, LT(g_s) \rangle$. ▨

$f, g_1, \ldots, g_s \in I$

FACT Let $G = \{g_1, \ldots, g_s\}$, $G' = \{g'_1, \ldots, g'_t\}$ be two Gröbner bases for $I \subseteq k[x_n]$ & let $f \in k[x_n]$.

Write $f = a_1 g_1 + \cdots + a_s g_s + r$ (divide by $(g_1, \ldots, g_s)$)

$f = a'_1 g'_1 + \cdots + a'_t g'_t + r'$ (divide by $(g'_1, \ldots, g'_t)$)

Then $r = r'$.

[Similar proof.]

§2.6 Gröbner bases, cont.

Problem Given an ideal $I = \langle S \rangle \subseteq k[x_n]$, how to find a Gröbner basis G of I? ("Uniqueness?")

Problem Given a basis G of I, how to decide if G is Gröbner?

$\langle LT(G) \rangle \stackrel{?}{=} LT(I)$.

Ex $\mathbb{Q}[x,y]$, $<$ = lex.

$I = \langle \underbrace{x^2y^3 + 3x}_{f_1}, \underbrace{x^3y^2 - 2y}_{g_1} \rangle$

Gröbner? No!

$x \cdot f - y \cdot g = 3x^2 - 2y^2$ so that $x^2 \in LT(I)$ but $x^2 \notin \langle x^2y^3, x^3y^2 \rangle$.

Def Let $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $x_1^{\beta_1} \cdots x_n^{\beta_n}$ be monomials in $k[x_n]$. The **least common multiple** is

$$\mathrm{LCM}(x^\alpha, x^\beta) = x^\gamma \quad \text{where } \gamma = (\max(\alpha_1,\beta_1), \dots, \max(\alpha_n,\beta_n)).$$

Given $f, g \in k[x_n] - \{0\}$, Let $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$.

The **S-polynomial** is

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f + \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g. \quad (\text{"Syzygy"})$$

Lemma Suppose we have $\sum_{i=1}^{s} c_i f_i$, $c_i \in k$, $f_i \in k[x_n]$, & $\mathrm{multideg}(f_i) = \delta$ for all i s.t.

⊛ $\mathrm{multideg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$.

Then $\sum_{i=1}^{s} c_i f_i \in k\text{-span}\left\{ S(f_i, f_j) : 1 \le i < j \le s \right\}$.

Pf Write $d_i = \mathrm{LC}(f_i)$. Then by ⊛, $\sum_{i=1}^{s} c_i d_i = 0$.

Write $p_i = f_i / d_i$, so $\mathrm{LC}(p_i) = 1$ &

$$S(f_i, f_j) = \frac{x^\delta}{\mathrm{LT}(f_i)} f_i - \frac{x^\delta}{\mathrm{LT}(f_j)} f_j = \frac{1}{d_i} f_i - \frac{1}{d_j} f_j = p_i - p_j.$$

Now

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{\delta} c_i d_i p_i = \overbrace{c_1 d_1 (p_1 - p_2)}^{S(f_1,f_2)} + \overbrace{(c_1 d_1 + c_2 d_2)(p_2 - p_3)}^{S(f_2,f_3)}$$
$$+ \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) \underbrace{(p_{s-1} - p_s)}_{S(f_{s-1}, f_s)}$$
$$+ \Big(\sum_{i=1}^{s} c_i d_i\Big) p_s \qquad \Big(\sum_{i=1}^{s} c_i d_i = 0\Big). \quad \blacksquare$$

Def Let $F = (f_1, \dots, f_s)$ be a sequence of polys in $k[x_1, \dots, x_n] - \{0\}$ & let $f \in k[x_1, \dots, x_n]$.

$\overline{f}^F$ = remainder upon division of f by $(f_1, -, f_s)$.

Buchberger's Criterion

Let $I = \langle G \rangle \subseteq k[x_1, \dots, x_n]$ be an ideal, where $G = (g_1, -, g_s)$. Then G is a Gröbner basis for $I \iff$ for all $i \neq j$, $\overline{S(g_i, g_j)}^G = 0$.

Pf $\Rightarrow$ $S(g_i, g_j) \in I$ for all $i \neq j$. //

$\Leftarrow$ Let $f \in I - \{0\}$. WTS $LT(f) \in \langle LT(g_1), -, LT(g_s) \rangle$.

$\exists\ h_1, -, h_s \in k[x_1, \dots, x_n]$ s.t.

$$\circledast \qquad f = \sum_{i=1}^{s} h_i g_i .$$

Then $\text{multideg}(f) \leq \text{multideg}(h_i g_i)$, for all i. If $\text{multideg}(f) = \text{multideg}(h_{i_0} g_{i_0})$ for any i_0, then $LM(f) = LM(h_{i_0}) \cdot LM(g_{i_0}) \in \langle LM(g_1), -, LM(g_s) \rangle$ & we are done.

So ~~we may assume~~ let $\delta := \max\{\text{multideg}(h_i g_i) : i = 1, \dots, s\}$ & choose $\circledast$ s.t. δ is minimal. Suppose $\text{multideg} f < \delta$.

Now

$$\circledast\circledast \quad f = \sum_{i=1}^{s} h_i g_i = \sum_{\text{mdeg}(h_i g_i) = \delta} LT(h_i) g_i + \sum_{\text{md}(h_i g_i) = \delta} (h_i - LT(h_i)) g_i + \sum_{\text{md}(h_i g_i) < \delta}' h_i g_i .$$

Now apply LEMMA to get

(†) $\sum_{\mathrm{md}(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i = \sum_{i,j} c_{ij} S(g_i, g_j)$ for some $c_{ij} \in k$. ∎

Applying $\overline{S(g_i, g_j)}^{G} = 0$:

(††) $\sum_{\mathrm{md} = \delta} \mathrm{LT}(h_i) g_i = \sum_{ijk} a_{ijk} g_{k_{c_{ij}}}$ with

$\mathrm{mdeg}(g_{k_{c_{ij}}} a_{ijk}) \leq \mathrm{mdeg}(S(g_i, g_j)) < \delta$.

Plugging (††) into (**) contradicts our choice of δ. ▨

Math 202c Lecture 5 4/16/18

LAST TIME $k[x_1,\dots,x_n]$, $<$ - term order $I \subseteq k[x_1,\dots,x_n]$ ideal

$LT(I) = \langle LT(f) : f \in I - \{0\} \rangle$.

finite $\rightarrow$ $G = \{g_1,\dots,g_s\} \subseteq I - \{0\}$ is a Gröbner basis of I if $LT(I) = \langle LT(g_1),\dots,LT(g_s)\rangle$.

* Every ideal has a Gröbner basis.
* G a Gröbner basis $\Rightarrow I = \langle G\rangle$
* If G is a G.b., $f \in k[x_1,\dots,x_n]$, poly. long division

$f \in I \iff r = 0$ in $f = a_1 g_1 + \cdots + a_s g_s + r$ ($G = \{g_1,\dots,g_s\}$)

Def Let $f, g \in k[x_1,\dots,x_n] \neq 0$. Let $x^\gamma = LCM(LM(f), LM(g))$.

$$S(f,g) := \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Lemma Suppose $f_1,\dots,f_s \in k[x_1,\dots,x_n]$, $c_1,\dots,c_s \in k$, & $f = \sum_{i=1}^s c_i \cdot f_i$ w/ $\text{multideg}\, f_i = \delta$ for all i but $\text{multideg}(f) < \delta$. Then $\text{multideg}(S(f_i,f_j)) < \delta \ \forall\, i \neq j$ and $f \in k\text{-span}\{S(f_i,f_j) : i \neq j\}$.

Pf Let $d_i = LC(f_i)$ & $p_i = f_i/d_i$. Then for $i \neq j$,

$$S(f_i,f_j) = \frac{x^\delta}{LT(f_i)} f_i - \frac{x^\delta}{LT(f_j)} f_j = p_i - p_j. \quad \text{Also, } \sum_{i=1}^s c_i d_i = 0.$$

$$\sum_{i=1}^s c_i d_i = 0 \qquad (p_{s-1} - p_s)$$

Now $f = \sum_{i=1}^s c_i f_i = \sum_{i=1}^s c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \left(\sum_{i=1}^{s-1} c_i d_i\right)$

$$= c_1 d_1 \underbrace{S(f_1,f_2)}_{} + \cdots + \sum_{i=1}^{s-1} c_i d_i \underbrace{S(f_{s-1},f_s)}_{}.$$

∎

Notation If $S = (f_1, \dots, f_t)$ is a list of polys in $k[x_n]$, $f \in k[x_n]$ then

$$\overline{f}^{S} \equiv \text{remainder upon dividing } f \text{ by } (f_1, \dots, f_k).$$

Buchberger Criterion:

Let $I = \langle G \rangle$ be an ideal in $k[x_n]$ with $G = (g_1, \dots, g_s)$.

Then G is a Gröbner basis of $I \iff$ for all $i \neq j$, $\overline{S(g_i, g_j)}^{G} = 0$.

Pf $\Rightarrow$ $S(g_i, g_j) \in I$. //

$\Leftarrow$ Let $f \in I^{-\{0\}}$ WTS $LT(f) \in \langle LT(g_1), \dots, LT(g_s) \rangle$.

B/c $I = \langle G \rangle$, $\exists\ h_i \in k[x_n]$ s.t.

$$\circledast \quad f = h_1 g_1 + \cdots + h_s g_s.$$

Let $\delta := \max(\text{multideg}(h_i g_i) : i = 1, \dots, s)$. Then $\delta \geq \text{multideg } f$.

If $\delta = \text{multideg } f$ $\exists\ 1 \leq i \leq s$ st $\text{multideg } f = \text{multideg}(h_i g_i)$

so $LM(f) = LM(h_i)\, LM(g_i) \in \langle LT(g_1), \dots, LT(g_s) \rangle$.

Choose $\circledast$ st δ is minimal & assume $\delta > \text{multideg } f$.

$\circledast$ can be rewritten as

$$\circledast\circledast \quad f = \sum_{\text{mdeg}(h_i g_i) = \delta} LT(h_i) g_i + \sum_{\text{mdeg } h_i g_i \neq \delta} (h_i - LT(h_i)) g_i + \sum_{\text{mdeg}(h_i g_i) < \delta} h_i g_i.$$

We may apply our LEMMA to $\sum_{\text{mdeg}(h_i g_i) = \delta} LT(h_i) g_i$. Also

$$S(LT(h_i) g_i, LT(h_j) g_j) = x^{\delta - \text{mdeg}(S(g_i, g_j))} S(g_i, g_j)\Big], \quad \text{mdeg} < \delta.$$

Application of LEMMA & $\overline{S(g_i,g_j)}^{G} = 0$ gives

(***) $$f = \sum_{\substack{i,j,k \\ mdeg(h_i g_i) = \delta \\ mdeg(h_j g_j) = \delta}} \overbrace{a_{ij}^{k}\, g_k}^{mdeg < \delta} + (\text{terms of } mdeg < \delta).$$

This contradicts our choice of δ. ▨

§2.7 Buchberger's Algorithm

Input A basis $F = \{f_1, \dots, f_t\}$ of an ideal $I \subseteq k[x_1, \dots]$

Output A Gröbner basis $G = \{g_1, \dots, g_s\}$ of I.

① - Initialize $G := F$.

② - For all $g \neq g' \in G$, if $\overline{S(g,g')}^{G} \neq 0$, adjoin $\overline{S(g,g')}^{G}$ to G.

③ Repeat ② until $\overline{S(g,g')}^{G} = 0$ for all $g \neq g'$ in G.

FACT B's A terminates and is correct.

Def A Gröbner basis G is minimal if

① $LC(g) = 1$ for all $g \in G$

② if $g \neq g'$ are in G then $LM(g) \nmid LM(g')$.

Gröbner basis —(remove redundant polys)→ minimal Gröbner basis

Eg $I = \langle f_1, f_2 \rangle \subset k[x,y]$ <grlex

$f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$

B's A → Gröbner basis $\{ f_1, f_2, f_3, f_4, f_5 \}$

$f_3 = -x^2 \cdot f_1 + f_2 = -2xy$

$f_4 = -2y^2 + x$

$f_5 = \frac{1}{2}x \cdot f_4 + y \cdot f_3 = \frac{1}{2}x^2$

→ Minimal Gröbner : $\left\{ x^2, xy, y^2 - \frac{1}{2}x \right\}$

Last Time

$I \subseteq k[x_1,\dots,x_n]$, $1 \le \ell \le n$

$I_\ell := I \cap k[x_{\ell+1},\dots,x_n]$ "Elimination Ideal"

Elimination Theorem

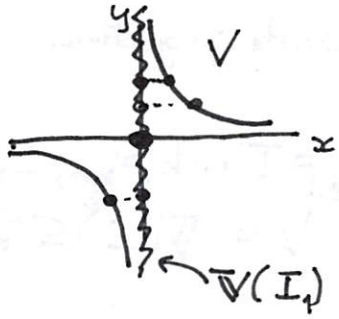
If G is a Gröbner basis for I WRT $<_{lex}$, then

$G_\ell := G \cap k[x_{\ell+1},\dots,x_n]$ is a Gröbner basis for I_ℓ WRT $<_{lex}$.

Q Let $V = \mathbb{V}(I) \subseteq k^n$. Then $\mathbb{V}(I_1) \subseteq k^{n-1}$. "partial solns"

Given $(c_2,\dots,c_n) \in \mathbb{V}(I_1)$, do we have $c_1 \in k$ s.t. $(c_1,c_2,\dots,c_n) \in V = \mathbb{V}(I)$?

Ex $I = \langle x\cdot y - 1\rangle \subseteq \mathbb{C}[x,y]$. $\Rightarrow V = \{(\alpha,\beta) \in \mathbb{C} : \alpha\beta = 1\}$



$I_1 = I \cap \mathbb{C}[y] = 0$

$\Rightarrow \mathbb{V}(I_1) = \mathbb{C}$

So $0 \in \mathbb{V}(I_1)$ but $\nexists\ c \in \mathbb{C}$ st $(c,0) \in V$.

Extension Thm Assume $k = \bar{k}$ is algebraically closed. Let $I = \langle f_1,\dots,f_r\rangle \subseteq k[x_n]$ be an ideal with $V = \mathbb{V}(I) \subseteq k^n$. Let $(c_2,\dots,c_n) \in \mathbb{V}(I_1) \subseteq k^{n-1}$.

For $1 \le i \le s$, write $f_i(x_1,-,x_n) = x_1^{m_i}\cdot g_i(x_2,\dots,x_n) + (\text{terms of } x_1\text{-deg} < m_i)$.

If $\exists\ 1 \le i \le s$ st $g_i(c_2,\dots,c_n) \neq 0$ then $\exists\ c_1 \in k$ st $(c_1,c_2,\dots,c_n) \in k^n$.

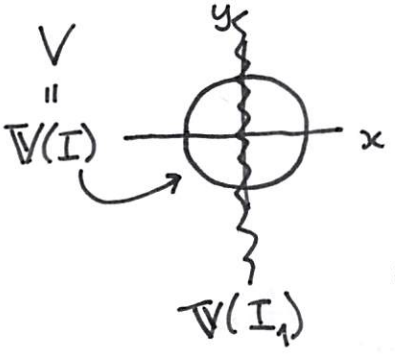
Rmk We need $k = \bar{k}$:

$$I = \langle x^2 + y^2 - 1 \rangle \subseteq \mathbb{R}[x,y]$$

(x-LC $\equiv 1$)

$$I_1 = I \cap \mathbb{R}[y] = 0$$

$$\mathbb{V}(I_1) = \mathbb{R}.$$



But "partial soln" $2 \in \mathbb{V}(I_1)$ doesn't extend ☹

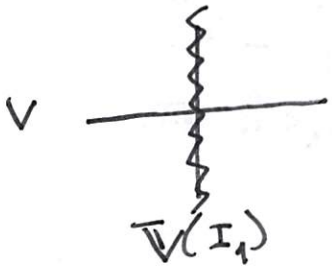
Over $\mathbb{C}$, $(\sqrt{3}i, 2)$

$(-\sqrt{3}i, 2)$ are extensions.

Also converse isn't true:

$$I = \langle xy \rangle \subseteq \mathbb{C}[x,y]$$

$$I_1 = 0 \subset \mathbb{C}[y]$$



(all partial solns extend), even 0.

§3.2 Geometry of Extension

* Let $\pi_\ell : k^n \twoheadrightarrow k^{n-\ell}$

$(c_1, \ldots, c_n) \mapsto (c_{\ell+1}, \ldots, c_n)$. be the coordinate projection.

- If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal and $I_1 = I \cap k[x_2, \ldots, x_n]$, $V = \mathbb{V}(I) \subseteq k^n$,

then $\pi_1(V) \subseteq \mathbb{V}(I_1)$ in k^{n-1}.

↑ partial solns which extend ↑ all partial solns

Q: How big is this gap?

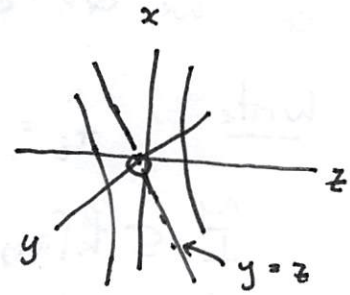
Ex $V \subseteq \mathbb{C}^3$ $\quad I = \langle xy-1, xz-1 \rangle \subseteq \mathbb{C}[x,y,z]$

$\mathbb{V}(xy-1, xz-1)$. $\quad I_1 = I \cap \mathbb{C}[y,z] = \langle y-z \rangle$.

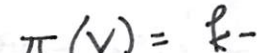
So $\mathbb{V}(I_1) = \{(a,a) : a \in \mathbb{C}\} \subseteq \mathbb{C}^2$.

But $\pi_1(V) = \{(a,a) : a \in \mathbb{C} - \{0\}\}$

$\Rightarrow$ $(0,0)$ is missing from $\pi_1(V)$.



Rmk If $V \subseteq k^n$ is a variety, $\pi_1(V) \subseteq k^{n-1}$ is NOT necessarily a variety.

$V = \mathbb{V}(xy-1) \subseteq k^2$  $\Rightarrow$ 

$\pi_1(V) = k - \{0\}$.

"Geometric" Extension Theorem Assume $k = \bar{k}$. Let $I = \langle f_1, \dots, f_r \rangle \subseteq k[x_1, \dots, x_n]$ be an ideal w/ $f_i(x_1, \dots, x_n) = x_1^{m_i} g_i(x_2, \dots, x_n) +$ (terms of lower x_1-deg)

Let $V = \mathbb{V}(I) \subseteq k^n$. Then

$$\mathbb{V}(I_1) = \underbrace{\pi_1(V)}_{\substack{\text{partial} \\ \text{solns}}} \cup \underbrace{\left(\mathbb{V}(g_1, \dots, g_s) \cap \mathbb{V}(I_1) \right)}_{\substack{\text{partial solns} \\ \text{that extend} \\ ???}}.$$

Assume $k = \bar{k}$ & let $1 \le \ell \le n$.

CLOSURE THM Let $V = \mathbb{V}(f_1, \dots, f_r) \subseteq k^n$ & let $I = \langle f_1, \dots, f_r \rangle \subseteq k[x_1, \dots, x_n]$.

(1) $\mathbb{V}(I_\ell)$ is the Zariski closure of $\pi_\ell(V)$ in $k^{n-\ell}$.

(2) If $V \neq \emptyset$, $\exists$ a variety $W \subsetneq \mathbb{V}(I_\ell)$ s.t. $\mathbb{V}(I_\ell) - W \subseteq \pi_\ell(V)$. ("small")

Pf (Of ②, when $\ell = 1$, assuming ① + Extension Thm).

We know that

$$\mathbb{V}(I_1) = \pi_1(V) \cup \left(\mathbb{V}(g_1, \ldots, g_r) \cap \mathbb{V}(I_1) \right),$$

so we are done unless (*) $\mathbb{V}(I_1) \subseteq \mathbb{V}(g_1, \ldots, g_r)$, so assume (*).

Write $f_i = x_1^{m_i} \cdot g_i + (\text{lower } x_1\text{-deg terms})$. and introduce.

$$\tilde{I} \subseteq k[x_1, \ldots, x_n]$$

$$\| \quad \langle f_1, f_2, \ldots, f_r, g_1, g_2, \ldots, g_r \rangle.$$

Since By (*), $\mathbb{V}(\tilde{I}) = V$ Furthermore, if

$$\tilde{f}_1 = f - x_1^{m_1} \cdot g_1, \quad \ldots, \quad \tilde{f}_r = f_r - x_1^{m_r} \cdot g_r:$$

$$\tilde{I} = \langle f_1, \ldots, f_r, g_1, \ldots, g_r \rangle = \langle \tilde{f}_1, \ldots, \tilde{f}_r, g_1, \ldots, g_r \rangle.$$

Again by the Extension Thm,

$$\mathbb{V}(I_1) = \mathbb{V}(\tilde{I}_1) = \pi_1(V) \cup \left(\mathbb{V}(\tilde{g}_1, \ldots, \tilde{g}_r) \cap \mathbb{V}(\tilde{I}_1) \right)$$

$\mathbb{V}(I_1) = \mathbb{V}(\tilde{I}_1)$: part ① of closure thm $\Rightarrow$ smallest var. containing $\pi_1(V)$

where $\tilde{g}_i$ is st $\tilde{f}_i = x_1^{\tilde{m}_i} \cdot \tilde{g}_i +$ terms of lower x_1-degree.

Unless $\mathbb{V}(I_1) \subseteq \mathbb{V}(\tilde{g}_1, \ldots, \tilde{g}_r)$ we are done. Otherwise, iterate.

At some point, we would get

$V = \mathbb{V}(h_1, \ldots, h_s)$ so that $\pi_1(V) = \mathbb{V}(I_1)$.

$h_1, \ldots, h_s \in k[x_2, \ldots, x_n]$

Math 202C Lecture 8 4/25/2018

Last Time

Extension Thm $k=\bar{k}$. Let $I = \langle f_1, \dots, f_r \rangle \subseteq k[x_1,\dots,x_n]$, $V = \mathbb{V}(I) \subseteq k^n$. Define $g_1, \dots, g_r \in k[x_2,\dots,x_n]$ by

$$f_i(x_1,\dots,x_n) = x_1^{m_i} \cdot g_i(x_2,\dots,x_n) + \text{terms of } x_1\text{-deg. } < m_i.$$

Let $(c_2,\dots,c_n) \in \mathbb{V}(I_1)$. If $\exists\ 1 \le i \le r$ st $g_i(c_2,\dots,c_n) \neq 0$ then $\exists\ c_1 \in k$ st $(c_1,c_2,\dots,c_n) \in V$.

($k=\bar{k}$)

CLOSURE THM Let $1 \le \ell \le n$, $\pi_\ell : k^n \longrightarrow k^{n-\ell}$ be proj'n

① $\mathbb{V}(I_\ell)$ is the Zariski closure of $\pi_\ell(V)$.

② If $V \neq \emptyset$, $\exists$ a proper subvariety $W \subsetneq \mathbb{V}(I_\ell)$ s.t. $\mathbb{V}(I_\ell) - W \subseteq \pi_\ell(V)$.

---

§ 3.3 Implicitization

Ex $C = \{(t,t^2,t^3) : t \in \mathbb{R}\} \subseteq \mathbb{R}^3$

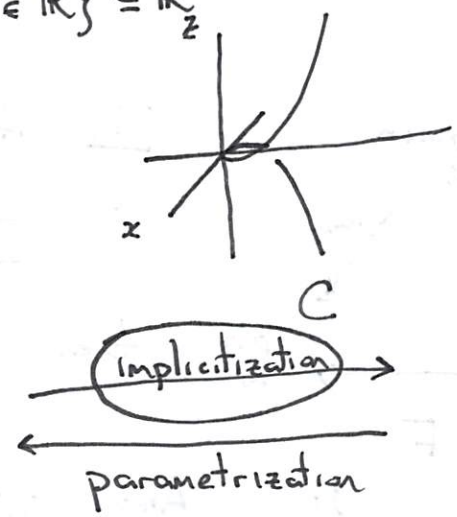
"twisted cubic"

"parametric"

or

$C = \mathbb{V}(x^2-y, x^3-z) \subseteq \mathbb{R}^3$

"implicit"



General setup: k - field

$f_1(t_1,\dots,t_m), \dots, f_n(t_1,\dots,t_m) \in k[t_1,\dots,t_m]$.

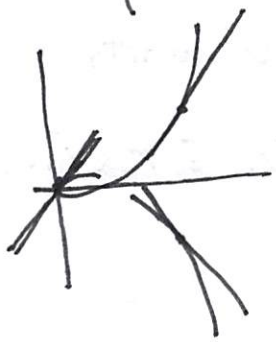
$$F: k^m \longrightarrow k^n$$
$$(t_1,\dots,t_m) \longmapsto (f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)).$$

Q What is the smallest subvar. V of k^n containing $F(k^m)$? ✓ when $|k|=\infty$

$V \stackrel{?}{=} F(k^m)$? X (not always)

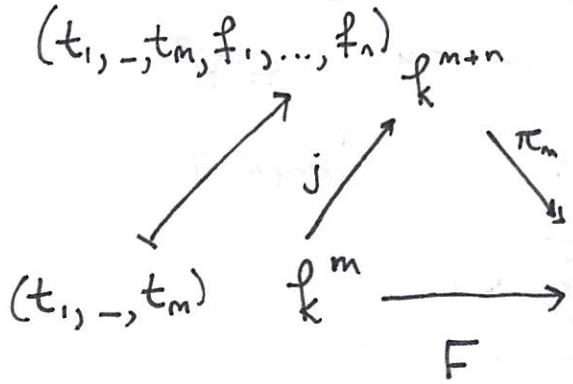
Ex $S = \{(t+u, t^2+2tu, t^3+3t^2u) : u,t \in \mathbb{R}\} \subseteq \mathbb{R}^3$

(Tangent surface to C.)



Equation $f(x,y,z)=0$?

General Case $F = (f_1,\dots,f_n)$, $f_i \in k[t_1,\dots,t_m]$:



Obs If $I \subseteq k[t_1,\dots,t_m,x_1,\dots,x_n]$ is $I = \langle f_1-x_1, \dots, f_n-x_n\rangle$ then

$$\boxed{j(k^m) = \mathbb{V}(I) \subseteq k^{m+n}}.$$

Also, $F(k^m) = \pi_m \circ j(k^m) = \pi_m(\mathbb{V}(I))$,

so that $\boxed{F(k^m) \subseteq \mathbb{V}(I_m)}$.

Q Given $f, g \in k[x]$, can we decide whether $\gcd(f,g) = 1$ <u>without</u> using <u>Euclidean algorithm</u>?

Prop Let $f(x), g(x) \in k[x]$ be st $\deg f = \ell$, $\deg g = m > 0$. Then f, g have a common factor in $k[x]$ $\iff$

$\exists$ $A, B \in k[x]$ s.t.

① A, B not both 0

② $\deg A \leq m-1$, $\deg B \leq \ell - 1$

③ $Af + Bg = 0$.

$\Rightarrow$ $f = h \cdot f_1$, $g = h \cdot g_1$ $\Rightarrow$

$$g_1 f + (-f_1) g = h f_1 g_1 - h f_1 g_1 = 0$$

so $A = g_1$, $B = -f_1$.

$\Leftarrow$ Suppose $B \neq 0$ & $Af + Bg = 0$. If $\gcd(f,g) \neq 1$, $\exists$ $\tilde{A}, \tilde{B} \in k[x]$ st $\tilde{A}f + \tilde{B}g = 1$. Then

$$B = B \cdot 1 = B \cdot (\tilde{A}f + \tilde{B}g) \underset{\uparrow}{=} \tilde{A}Bf - \tilde{B}Af = (\tilde{A}B - \tilde{B}A)f,$$

$$Bg = -Af$$

so $\deg B \geq \deg f = \ell$. $\#$

Q How to find $A(x)$, $B(x)$

A Linear Algebra! (Resultants...)

A domain R is a **Unique factorization domain** (**UFD**) if for any nonzero, nonunit $f \in R$

① $f = g_1 \cdots g_r$ for some irreducibles $g_1, \ldots, g_r$.

② if $f = g_1' \cdots g_s'$ is any other such factorization, then $s = t$ and up to rearrangement $g_i = u_i \cdot g_i'$ for some units $u_i \in R$.

Ex ① $R = \mathbb{Z}$: $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = (-2) \cdot (-3) \cdot 2$

② In $\mathbb{Q}[x]$: $f(x) = x^4 - 4 = (x^2+2)(x^2-2)$

In $\mathbb{R}[x]$: $= (x^2+2)(x-\sqrt{2})(x+\sqrt{2})$

In $\mathbb{C}[x]$: $= (x-\sqrt{2}\,i)(x+\sqrt{2}\,i)(x-\sqrt{2})(x+\sqrt{2})$

F ③ $\mathbb{Z}[\sqrt{-5}]$ is NOT a UFD: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

FACT R a UFD $\Rightarrow R[x]$ a UFD.

So $k[x_1, \ldots, x_n]$ is a UFD.

Gauss's Lemma Let $f, g \in k[x_1, \ldots, x_n]$ have positive x_1-degree.

Then f, g have a common factor $h \in k[x_1, \ldots, x_n]$ of positive x_1-deg

$\iff$ f, g have a common factor in $k(x_2, \ldots, x_n)[x_1]$.

Since $\forall\ F(k^m) \subseteq Z_k = V_k(g_1,\dots,g_s)$, the fcns

$$g_i \circ F : k^m \longrightarrow k \quad (1 \le i \le s)$$

satisfy $g_i \circ F = 0$ on k^m. Since k is infinite, $g_i \circ F \equiv 0$ is the zero polynomial in $k[t_1,\dots,t_m]$.

Thus $g_i \circ F : \bar{k}^m \to \bar{k}$ is also the zero fcn, so

$$F(\bar{k}^m) \subseteq V_{\bar{k}}(g_1,\dots,g_s) = Z_{\bar{k}}.$$ By Closure Thm,

$$V_{\bar{k}}(I_m) \subseteq V_{\bar{k}}(g_1,\dots,g_s).$$ Looking at solns $/k$,

$$V_k(I_m) \subseteq V_k(g_1,\dots,g_s) = Z_k. \quad \blacksquare$$

§ 3.5 Factorization Theory

Recall • A ring R is an (integral) domain if for any $f,g \in R$, $f \cdot g = 0 \Rightarrow f = 0$ or $g = 0$.

e.g. $\mathbb{Z}$, $k[x]$, $k[x_1,\dots,x_n]$, $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}/6\mathbb{Z}$ ($2 \cdot 3 = 0$)

• If R is a ring, $u \in R$ is a unit if $\exists\ v \in R$ st $uv = 1$.

• A nonzero, nonunit $f \in R$ is irreducible if

$f = g \cdot h \Rightarrow$ g or h is a unit.

Back to example

$$I \subseteq \mathbb{R}[\overset{u}{t}, \overset{t}{x}, x, y, z] \qquad I = \langle t+u-x,\ t^2+2tu-y,\ t^3+3t^2u-z \rangle$$

$<_{lex}$

We want $I_2 = I \cap \mathbb{R}[x,y,z]$ $\Rightarrow$ FIND Gröbner basis:

$$G = \{ \underbrace{f_1, f_2, f_6}_{\text{involves } u,t}, \underbrace{f_7}_{\text{involves } t} \}$$

$$f_7 = x^3z - \frac{3}{4}x^2y^2 - \frac{3}{2}xyz + y^3 + \frac{1}{4}z^4$$

Q $\quad \overline{S} = \mathbb{V}(f_7)$ in $\mathbb{R}^3$?

$\quad\ S = \mathbb{V}(f_7)$ in $\mathbb{R}^3$?

THM Let k be an infinite field & let $f_1, \dots, f_n \in k[t_1, \dots, t_m]$.

Let $F = (f_1, \dots, f_n) : k^m \longrightarrow k^n$. Set $I = \langle f_1 - x_1, \dots, f_n - x_n \rangle$

$\subseteq k[t_1, \dots, t_m, x_1, \dots, x_n]$.

Then $\mathbb{V}(I_m)$ is the smallest subvar. of k^n containing $F(k^m)$.

Pf Certainly $F(k^m) \subseteq \mathbb{V}(I_m)$; if $k = \bar{k}$ we are done by Closure Thm. Otherwise, embed $k \subseteq \bar{k}$ inside an alg. closure.

Let $Z \subseteq k^n$ be a subvar. st $F(k^m) \subseteq Z$. WTS $\mathbb{V}(I_m) \subseteq Z$. Write $Z = \mathbb{V}(g_1, \dots, g_s)$, $g_i \in k[x_1, \dots, x_n]$.

Look at $Z_{\bar{k}} = \{ (c_1, \dots, c_n) \in \bar{k}^n : g_i(c_1, \dots, c_n) = 0 \ \forall\ 1 \le i \le s \}$

$Z_k = Z$, $\mathbb{V}_{\bar{k}}(I_m)$, $\mathbb{V}_k(I_m)$.

$\uparrow$ $I_m = \langle h_1, \dots, h_t \rangle$ $h_i \in k[x_1, \dots, x_n]$.

Math 202C Lecture 9 4/27/18

LAST TIME $k[x]$ is a UFD for k a field.

$\Rightarrow$ given $f(x), g(x) \in k[x]$, have $\gcd(f,g) \in k[x]$.

Q If $\deg f, \deg g > 0$, is $\gcd(f,g) = 1$?

A1 Euclidean Algorithm. A2 Resultants.

FACT Let $f, g \in k[x]$ with $\deg f = \ell > 0$, $\deg g = m > 0$.

Then f, g have a common factor $h \in k[x]$ w/ $\deg h > 0$ $\Leftrightarrow$
$\exists$ $A, B \in k[x]$ s.t.

① $Af + Bg = 0$

② A, B not both 0

③ $\deg A < m$, $\deg B < \ell$.

Pf $\Rightarrow$ Write $f = h \cdot f_1$, $g = h \cdot g_1$. Then

$$g_1 \cdot f + (-f_1) \cdot g = g_1 f_1 h - f_1 g_1 h = 0.$$

$\Leftarrow$ By ② may assume $B \neq 0$. If $\gcd(f,g) = 1$, $\exists$ $\tilde{A}, \tilde{B} \in k[x]$ st $\tilde{A}f + \tilde{B}g = 1$, so $B \cdot g = -A \cdot f$

$$B = B \cdot 1 = B \cdot (\tilde{A}f + \tilde{B}g) \overset{\downarrow}{=} B\tilde{A}f - A\tilde{B}f = (\tilde{A}B - A\tilde{B})f.$$

Since $B \neq 0$, $\deg B \geq \deg f = \ell$. $\#$

Q Given f, g, how to find A, B? A Linear algebra!

Write $f(x) = a_0 x^\ell + a_1 x^{\ell-1} + \cdots + a_\ell$ $\quad a_0 \neq 0$

$g(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_m$ $\quad b_0 \neq 0$

$A(x) = c_0 x^{m-1} + \cdots + c_{m-1}$

$B(x) = d_0 x^{\ell-1} + \cdots + d_{\ell-1}$

"$\ell + m$ unknowns"

$Af + Bg = 0 \Leftrightarrow$

$$[x^{\ell+m-1}] \quad a_0 c_0 + b_0 d_0 = 0$$
$$[x^{\ell+m-2}] \quad a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 = 0$$
$$\vdots$$
$$[x^0] \quad a_\ell c_{m-1} + b_m d_{\ell-1} = 0$$

Def Let $f, g \in k[x]$ be polys w/ $\deg f = \ell > 0$, $\deg g = m > 0$.

Write $\begin{cases} f(x) = a_0 x^\ell + \cdots + a_\ell \\ g(x) = b_0 x^m + \cdots + b_m \end{cases}$ $a_0, b_0 \neq 0$. The <u>Sylvester matrix</u> is

$$Syl(f,g;x) = \begin{bmatrix} a_0 & & & & b_0 & & \\ a_1 & a_0 & & & b_1 & & \\ \vdots & a_1 & \ddots & & \vdots & \ddots & \\ a_\ell & \vdots & \ddots & a_0 & b_m & & b_0 \\ & a_\ell & & a_1 & & \ddots & b_1 \\ & & \ddots & \vdots & & & \vdots \\ & & & a_\ell & & & b_m \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \ell + m$$

$\underbrace{\qquad\qquad}_{m} \qquad \underbrace{\qquad\qquad}_{\ell}$

The <u>resultant</u> is $Res(f,g;x) := \det Syl(f,g;x)$.

Ex

$$Res(3x^2 - 2x + 1,\ 2x^3 + 2x^2 - x + 1) = \det \begin{bmatrix} 3 & & & 2 & & \\ -2 & 3 & & 2 & 2 & \\ 1 & -2 & 3 & -1 & 2 & 2 \\ & 1 & -2 & 3 & -1 & 2 \\ & & 1 & -2 & & -1 \\ & & & 1 & & \end{bmatrix}$$

$$= \det \begin{bmatrix} 3 & & & 2 & & \\ -2 & 3 & & 2 & 2 & \\ 1 & -2 & 3 & -1 & 2 & \\ & 1 & -2 & 1 & -1 & \\ & & 1 & & 1 & \end{bmatrix}$$

Fact Let $f, g \in k[x]$ be non-constant.

f, g have a common factor h w/ $\deg h > 0$ $\iff$ $Res(f,g;x) = 0$.

Thm Let $f, g \in k[x]$ be non-constant. $\exists$ $A, B \in k[x]$ s.t. $(*)$ $A \cdot f + B \cdot g = Res(f,g;x)$.

Furthermore, each coeff. of A or B is a <u>polynomial</u> in the coeffs of f, g w/ coeffs in $\mathbb{Z}$.

If $\mathrm{Res}(f,g;x) = 0$, take $A = B = 0$. So assume $\mathrm{Res}(f,g;x) \neq 0$.

Pf Let's look at (**) $\tilde{A} f + \tilde{B} g = 1$, $\deg \tilde{A} < \deg g \equiv m$

$\deg \tilde{B} < \deg f \equiv \ell$.

Now if $\tilde{A}(x) = c_0 x^{m-1} + \cdots + c_{m-1}$, $\tilde{B}(x) = d_0 x^{\ell-1} + \cdots + d_{\ell-1}$,

(**) reads:

$$(\dagger) \qquad \underset{(\ell+m)\times(\ell+m)}{\mathrm{Syl}(f,g;x)} \begin{bmatrix} c_0 \\ \vdots \\ c_{m-1} \\ d_0 \\ \vdots \\ d_{\ell-1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \Big\} \ell+m$$

We may find the unknowns $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{\ell-1}$ with Craner's Rule.

This gives formulas of the form

$$\frac{(\text{a poly. in coeffs of } f,g \text{ w/ } \mathbb{Z} \text{ coeffs})}{\mathrm{Res}(f,g;x)}$$

for each of the c_i, d_i. So if we multiply both sides of (**) by $\mathrm{Res}(f,g;x)$, we get an expression (*) of the desired form. ▨

§ 3.6 Pf of Extension Thm

* Let $f(x_1,\ldots,x_n)$, $g(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$ have positive x_1-deg.

Write

$$f(\underline{x}_n) = a_0 x_1^{\ell} + \cdots + a_\ell$$

$$g(\underline{x}_n) = b_0 x_1^{m} + \cdots + b_m$$

for $a_i, b_i \in k[x_2,\ldots,x_n]$ s.t. $a_0, b_0 \neq 0$.

The resultant is

$$\mathrm{Res}(f,g;x_1) = \det \begin{bmatrix} \overbrace{\begin{matrix} a_0 & & \\ | & \ddots & \\ a_\ell & & a_0 \\ & \ddots & | \\ & & a_\ell \end{matrix}}^{m} & \overbrace{\begin{matrix} b_0 & & \\ | & \ddots & \\ b_m & & b_0 \\ & \ddots & | \\ & & b_m \end{matrix}}^{\ell} \end{bmatrix} \in k[x_2,\ldots,x_n].$$

eg $f = y \cdot x^2 + (3y+1)x + 2$

$g = y^3 x + 1 \quad \Rightarrow \operatorname{Res}(f,g;x) = \det \begin{bmatrix} y & y^3 & \\ 3y+1 & 1 & y^3 \\ 2 & & 1 \end{bmatrix} \in k[y].$

FACT Let $f, g \in k[x_1, x_2, \_, x_n]$ have positive x_1-degree.

Then $\operatorname{Res}(f,g;x_1) \in \langle f, g \rangle \cap k[x_2, \_, x_n]$.

(Use previous thm.)

Extension Thm Assume $k = \bar{k}$. Let $I = \langle f_1, \_, f_r \rangle \subseteq k[x_n]$;

write $f_i(x_1, \_, x_n) = x_1^{m_i} \cdot g_i(x_2, \_, x_n) +$ lower x_1-degree terms.

Let $V = \mathbb{V}(I) \subseteq k^n$ & let $(c_2, \_, c_n) \in \mathbb{V}(I_1)$. If $\exists$ $1 \le i \le r$ st $g_i(c_2, \_, c_n) \neq 0$ then $\exists$ $c_1 \in k$ st $(c_1, c_2, \_, c_n) \in V$.

Pf Define $\varphi : k[x_1, \ldots, x_n] \longrightarrow k[x_1]$

$f(x_1, x_2, \_, x_n) \longmapsto f(x_1, c_2, \ldots, c_n)$. Then φ is a ring map and (check!) $\varphi(I)$ is an ideal in $k[x_1]$. Since $k[x_1]$ is a PID, $\exists$ $u(x_1) \in k[x_1]$ s.t. $\varphi(I) = \langle u(x_1) \rangle$.

CASE I $u(x_1) \equiv 0$ or $\deg u > 0$.

In this case, b/c $k = \bar{k}$, $\exists$ $c_1 \in k$ s.t. $u(c_1) = 0$. Now $(c_1, c_2, \_, c_n) \in V$. //

CASE II $u(x_1) \equiv u_0$ is a nonzero constant.

By defn of φ, $\exists$ $f \in I$ s.t. $f(x_1, c_2, \ldots, c_n) \equiv u_0$. Also, $\exists$ $1 \le i \le r$ s.t. $g_i(c_2, \_, c_n) \neq 0$. Consider

$h(x_2, \_, x_n) := \operatorname{Res}(f_i, f; x_1) \in k[x_2, \_, x_n]$.

By our fact, ~~Res(f_i, f~~

$h \in \langle f_i, f \rangle \cap k[x_2, \ldots, x_n] \subseteq I_1$ so that

$h(c_2, \ldots, c_n) = 0.$

However,

$$h(c_2, \ldots, c_n) = \det \begin{bmatrix} g_i(c_2, \ldots, c_n) & & & \\ & g_i(c_2, \ldots, c_n) & & \\ & & \ddots & \\ * & & & g_i(c_2, \ldots, c_n) \\ \hline & & & u_0 \\ & & & & \ddots \\ & & & & & u_0 \\ & & & * & & \end{bmatrix}$$

($g_i(c_2, \ldots, c_n) \neq 0$; $u_0 \neq 0$; $\det \neq 0$.)

§ 4.1 Hilbert's Nullstellensatz

Q Given $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, does $f_1 = \cdots = f_r = 0$ have any solns in k^n? (Consistency.)

Weak Nullstellensatz Assume $k = \bar{k}$. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let $V = \mathbb{V}(I) \subseteq k^n$.

Then $V = \emptyset \iff I = k[x_1, \ldots, x_n]$.

[eg $1 \in I$, so have $1 = 0$.]

Rmk False if $k \neq \bar{k}$:

$$\mathbb{V}_{\mathbb{R}}(x^2 + y^2 + 1) = \emptyset \subseteq \mathbb{R}^2.$$

but $\langle x^2 + y^2 + 1 \rangle \neq \mathbb{R}[x, y]$.

So, if $k = \bar{k}$ given $f_1, \dots, f_r \in k[x_n]$,

$$I = \langle f_1, \dots, f_r \rangle \overset{\text{B's A}}{\Rightarrow} \text{reduced Gröbner basis } G$$

$$\mathbb{V}(f_1, \dots, f_r) = \emptyset \iff G = \{1\}.$$

Pf of Weak Nullstellensatz

$\Leftarrow$ ✓

$\Rightarrow$ We induct on n. If $n=1$ this is true b/c $k = \bar{k}$.

Now let $n > 1$ & write $I = \langle f_1, \dots, f_r \rangle$ for some $f_i \in k[x_1, \dots, x_n] - \{0\}$. We may assume $f_1 \notin k$, so $\deg f_1 = N \geq 1$. (total)

Given $a_2, \dots, a_n \in k$, consider the change of variables:

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2 \tilde{x}_1 \\ &\vdots \\ x_n &= \tilde{x}_n + a_n \tilde{x}_1 . \end{aligned}$$

Given $f \in k[x_1, \dots, x_n]$, we get $\tilde{f} \in k[\tilde{x}_1, \dots, \tilde{x}_n]$.

In particular,

$$\begin{aligned} f_1(x_1, \dots, x_n) &= f_1(\tilde{x}_1, \tilde{x}_2 + a_2 \tilde{x}_1, \dots, \tilde{x}_n + a_n \tilde{x}_1) \\ &= c(a_2, \dots, a_n)\, \tilde{x}_1^N + \text{terms of } \tilde{x}_1\text{-degree} < N \end{aligned}$$

for some nonzero polynomial c. Since $|k| = \infty$, can choose $a_2, \dots, a_n \in k$ st $c(a_2, \dots, a_n) \neq 0$.

Let $\tilde{I} = \{\tilde{f} : f \in I\} \subseteq k[\tilde{x}_1, \dots, \tilde{x}_n]$; then $\tilde{I}$ is an ideal & $\mathbb{V}(\tilde{I}) = \emptyset$ (b/c $\mathbb{V}(I) = \emptyset$). Let $\tilde{I}_1 = \tilde{I} \cap k[\tilde{x}_2, \dots, \tilde{x}_n]$.

If $(c_2, \dots, c_n) \in \mathbb{V}(\tilde{I}_1)$, by Ext Thm $\exists\, c_1 \in k$ st $(c_1, c_2, \dots, c_n) \in \mathbb{V}(\tilde{I})$.

So $\mathbb{V}(\tilde{I}_1) = \emptyset$. Thus $1 \in \tilde{I}_1$, so $1 \in \tilde{I}$ and $1 \in I$. ∎

Math 202c Lecture 10 4/30/18

LAST TIME

Weak Nullstellensatz Assume $k=\bar{k}$ & let $I \subseteq k[x_1,\dots,x_n]$ be an ideal. Write $V = \mathbb{V}(I) \subseteq k^n$.

$$V = \emptyset \iff I = \langle 1 \rangle.$$

Pf $\Leftarrow$ ✓

$\Rightarrow$ We induct on n. If $n=1$ & $I \neq \langle 1\rangle$ write $I = \langle f(x_1)\rangle$ where $\deg f > 0$. Now if $f(c_1)=0$ for $c_1 \in k$, $c_1 \in V$.

Assume $n>1$ & write $I = \langle f_1,\dots,f_r\rangle$ for $f_i \in k[x_1,\dots,x_n]$. Given $a_2,\dots,a_n \in k$ consider the change of coordinates

$$\begin{cases} x_1 = x_1' \\ x_2 = x_2' + a_2 x_1' \\ \vdots \\ x_n = x_n' + a_n x_1' \end{cases}.$$

For any poly. $f = f(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$, we get $f^* = f(x_1', \dots, x_n')$

$$= f(x_1', x_2' + a_2 x_1', \dots) \in k[x_n'].$$

Furthermore, $I' := \langle f' : f \in I\rangle$ is an ideal in $k[x_n']$ & $I' = \langle f_1', \dots, f_r'\rangle$. Finally, since $\mathbb{V}(I) = \emptyset$, $\mathbb{V}(I') = \emptyset$.

Let N = total degree of f_1; we may assume $N > 0$.

Now $f_1' = f_1(x_1', x_2' + a_2 x_1', \dots, x_n' + a_n x_1') = c(a_2,\dots,a_n)\cdot x_1'^N + (\text{terms of lower } x_1'\text{-deg.})$

for some nonzero poly. $c \in k[x_2',\dots,x_n']$. Since $k=\bar{k}$, $|k| = \infty$

so we <u>choose</u> $a_2, \dots, a_n \in k$ s.t. $c(a_2, \dots, a_n) \neq 0$.

Consider $I_1' = I' \cap k[x_2', \dots, x_n']$. If $(c_2, \dots, c_n) \in \mathbb{V}(I_1')$, by <u>Extension Thm</u> (since the x_1-top coeff of f_1' is a <u>nonzero constant</u>), $\exists\ c_1 \in k$ st $(c_1, c_2, \dots, c_n) \in \mathbb{V}(I')$. $*$

So $\mathbb{V}(I_1') = \emptyset$. By induction, $1 \in I_1'$, so $1 \in I'$ and $1 \in I$. ▨

<u>Q</u> What happens when $\mathbb{V}(I) \neq \emptyset$.

<u>Ex</u> $I = \langle (x-2)^4, (y-3)^3 \rangle \subseteq \mathbb{C}[x,y]$

$V = \mathbb{V}(I) = \{(2,3)\} \subseteq \mathbb{C}^2$

$f(x,y) = x \cdot (y-3) \in \mathbb{I}(V)$ $\ulcorner 2 \cdot (3-3) = 0 \urcorner$

but $f \notin I$. <u>However</u>, $f^3 = I$.

<u>Strong Nullstellensatz</u> Assume $k = \bar{k}$. Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal & let $V = \mathbb{V}(I) \subseteq k^n$. If $f \in k[x_1, \dots, x_n]$ satisfies $f \in \mathbb{I}(V)$, $\exists\ m \geq 1$ s.t. $f^m \in I$.

<u>Rmk</u> We need $k = \bar{k}$:

$I = \langle x^2 + y^2 \rangle \subseteq \mathbb{R}[x,y]$

$V = \mathbb{V}(I) = \{(0,0)\} \Rightarrow x \in \mathbb{I}(V)$.

But for all $m \geq 1$, $x^m \notin I$.

$\ulcorner$Over $\mathbb{C}$, $(1, i) \in \mathbb{V}_{\mathbb{C}}(x^2+y^2)$ so $x \notin \mathbb{I}_{\mathbb{C}}(\mathbb{V}_{\mathbb{C}}(x^2+y^2))$. $\lrcorner$

Pf Write $I = \langle f_1, \dots, f_r \rangle$ for $f_i \in k[x_1, \dots, x_n]$. Introduce a new variable y and consider $J = \langle f_1, \dots, f_r, 1 - f \cdot y \rangle \subseteq k[x_1, \dots, x_n, y]$.

Since $f \in \mathbb{I}(f_1, \dots, f_r)$, we have $\mathbb{V}(J) = \emptyset \subseteq k^{n+1}$.

By the Weak Nullstellensatz, $1 \in J$, so

$$(*) \quad 1 = g_1(x_1, \dots, x_n, y) \cdot f_1 + \cdots + g_r(x_1, \dots, x_n, y) \cdot f_r + g(x_1, \dots, x_n, y)(1 - y \cdot f)$$

for some $g_1, \dots, g_r, g \in k[x_n, y]$. Substitute $y = 1/f$; get

$$(**) \quad 1 = g_1\left(x_1, \dots, x_n, \tfrac{1}{f}\right) f_1 + \text{———} + g_r\left(x_1, \dots, x_n, \tfrac{1}{f}\right) f_r.$$

Multiply $(**)$ by f^m for $m \geq 1$ large enough to clear denominators to get $f^m \in \langle f_1, \dots, f_r \rangle \subseteq k[x_1, \dots, x_n]$. ▨

§ 4.2 Ideal-Variety Correspondence

Def Let $I \subseteq R$ be an ideal. The radical of I is

$$\sqrt{I} = \{ f \in R : f^m \in I \text{ for some } m \geq 1 \}; \quad I \subseteq \sqrt{I}.$$

I is radical if $I = \sqrt{I}$.

Ex In $\mathbb{R}[x]$, $\langle x^3(x-3)^2 \rangle$ vs $\langle x(x-3) \rangle$

not radical — radical

Rmk - For any subset $X \subseteq k^n$, $\mathbb{I}(X) \subseteq k[x_1, \dots, x_n]$ is radical.

- If $k = \bar{k}$, $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ for all $I \subseteq k[x_1, \dots, x_n]$.

So for ANY field k, have maps

$$\left\{ \begin{array}{l} \text{radical ideals} \\ I \subseteq k[x_1, \dots, x_n] \end{array} \right\} \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} \left\{ \begin{array}{l} \text{varieties} \\ V \subseteq k^n \end{array} \right\}$$

Over ANY field k,

- $I_1 \subseteq I_2 \Rightarrow \mathbb{V}(I_1) \supseteq \mathbb{V}(I_2)$
  $V_1 \subseteq V_2 \Rightarrow \mathbb{I}(V_1) \supseteq \mathbb{I}(V_2)$
- For any variety V, $\mathbb{V}(\mathbb{I}(V)) = V$.

If $k = \bar{k}$:

- ~~$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ for all ideals $I \subseteq k[x_1, \dots, x_n]$~~ &
- the maps $\mathbb{V}, \mathbb{I}$ above are inverse bijns!

§4.3 $I+J$, $I \cdot J$, $I \cap J$

Recall If $I, J \subseteq R$ are ideals, $I \cap J \subseteq R$ is an ideal, as are

$$I + J = \{ f + g : f \in I, g \in J \}$$
$$I \cdot J = \langle f \cdot g : f \in I, g \in J \rangle.$$

Over any field k, if $I, J \subseteq k[x_1, \dots, x_n]$ then

- $\mathbb{V}(I+J) = \mathbb{V}(I) \cap \mathbb{V}(J)$
- $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$
- $\mathbb{V}(I \cdot J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

Rmk If $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$ for $f_i, g_i \in k[x_1, \dots, x_n]$ then

$$\begin{cases} I + J = \langle f_1, \dots, f_r, g_1, \dots, g_s \rangle \\ I \cdot J = \langle f_i \cdot g_j : 1 \le i \le r, \ 1 \le j \le s \rangle . \end{cases}$$

$\Rightarrow$ What about $I \cap J$?

Trick Let t be a new variable,

$$tI = \{ t \cdot f : f \in I \} \subseteq k[t, x_1, \dots, x_n]$$

$$(1-t)J = \{ (1-t) \cdot g : g \in J \} \subseteq k[t, x_1, \dots, x_n].$$

Check $\cdot \ tI = \langle tf_1, \dots, tf_r \rangle$; $(1-t)J = \langle (1-t)g_1, \dots, (1-t)g_s \rangle$.

$$I \cap J = \underbrace{\left(tI + (1-t)J \right) \cap k[x_1, \dots, x_n]}_{\text{Elimination Ideal!}}.$$

Rmk If $I, J \subseteq R$ are ideals then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

§ 4.4 Zariski Closure, $(I : J)$.

Recall If $X \subseteq k^n$ then $\overline{X}$ = smallest variety in k^n containing X.

* $\overline{X} = \mathbb{V}(\mathbb{I}(X))$.

Closure Thm ①

Assume $k = \bar{k}$ & let $I \subseteq k[x_1, \dots, x_n]$ be an ideal. Let $I_\ell = I \cap k[x_{\ell+1}, \dots, x_n]$, $V = \mathbb{V}(I) \subseteq k^n$, & $\pi_\ell : k^n \twoheadrightarrow k^{n-\ell}$ be proj'n. Then

$$\overline{\pi_\ell(V)} = \mathbb{V}(I_\ell), \text{ inside } k^{n-\ell}.$$

We have $\pi_\ell(V) \subseteq \mathbb{V}(I_\ell)$, so $\overline{\pi_\ell(V)} \subseteq \mathbb{V}(I_\ell)$.

Suppose $f \in \mathbb{I}(\pi_\ell(V))$ for $f \in k[x_{\ell+1}, \dots, x_n]$.

Considering f as an elt of $k[x_1, \dots, x_n]$,

$$f(a_1, \dots, a_\ell, a_{\ell+1}, \dots, a_n) = 0 \quad \forall \ (a_1, \dots, a_n) \in V.$$

By Strong N, $\exists\ m \geq 1$ s.t. $f^m \in I$.

But $f^m \in k[x_{\ell+1}, \dots, x_n]$ so $f^m \in I_\ell$. This means

$$\mathbb{I}(\pi_\ell(V)) \subseteq \sqrt{I_\ell} = \mathbb{I}(\mathbb{V}(I_\ell)), \text{ so}$$

$$\overline{\pi_\ell(V)} = \mathbb{V}(\mathbb{I}(\pi_\ell(V))) \supseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(I_\ell))) = \mathbb{V}(I_\ell).$$

$\blacksquare$

Math 202C Lecture 11 5/2/2018

LAST TIME

Strong Nullstellensatz $k=\bar{k}$. Let $I \subseteq k[x_n]$ be an ideal. Then

$$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}.$$

$\Rightarrow$ radical ideals $I \subseteq k[x_n]$ $\underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}}$ varieties $V \subseteq k^n$

- $\mathbb{V}(\mathbb{I}(V)) = V$ over any field k
- $\mathbb{I}(\mathbb{V}(I)) = I$ if $k=\bar{k}$.

- $\mathbb{V}(I+J) = \mathbb{V}(I) \cap \mathbb{V}(J)$, $\mathbb{V}(I \cdot J) = \mathbb{V}(I) \cup \mathbb{V}(J)$, $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$ (over any field k.)

§ 4.4 Zariski Closure

Recall If $X \subseteq k^n$, $\overline{X}$ = Zariski closure of X = smallest variety $V \subseteq k^n$ s.t. $X \subseteq V$

FACT Over any field k, $\overline{X} = \mathbb{V}(\mathbb{I}(X))$.

CLOSURE THM Assume $k=\bar{k}$ & let $1 \leq \ell \leq n$. Let $I \subseteq k[x_n]$ be an ideal, let $V = \mathbb{V}(I) \subseteq k^n$, let $\pi_\ell : k^n \twoheadrightarrow k^{n-\ell}$ be proj'n, & let $I_\ell = I \cap k[x_{\ell+1}, \dots, x_n]$. We have

$$\overline{\pi_\ell(V)} = \mathbb{V}(I_\ell).$$

Exc $I = \langle xy-1 \rangle \subseteq \mathbb{C}[x,y]$ $\quad I_1 = I \cap \mathbb{C}[y] = 0$.

$$V = \left\{ \left(a, \tfrac{1}{a}\right) : a \in \mathbb{C}^\times \right\}$$

$\pi_1(V) = \mathbb{C}^\times$ $\quad \mathbb{V}(I_1) = \mathbb{C}$

RMK $\pi_\ell(V)$ (variety) is NOT always a variety!

Pf We know $\pi_\ell(V) \subseteq \mathbb{V}(I_\ell)$, so $\overline{\pi_\ell(V)} \subseteq \mathbb{V}(I_\ell)$.

WTS $\mathbb{V}(\mathbb{I}(\pi_\ell(V))) \supseteq \mathbb{V}(I_\ell) \iff \mathbb{I}(\pi_\ell(V)) \subseteq \sqrt{I_\ell}$.

$\mathbb{V}(\mathbb{I}(\pi_\ell(V))) = \overline{\pi_\ell(V)}$

$\iff$: Nullstellensatz; $k = \bar{k}$

So let $f \in k[x_{\ell+1}, \dots, x_n]$ satisfy $f \in \mathbb{I}(\pi_\ell(V))$. So $\forall\ (a_1, \dots, a_n) \in V$, $f(a_{\ell+1}, \dots, a_n) = 0$. If we consider $f \in k[x_1, \dots, x_n]$ this means $f \in \mathbb{I}(V) = \mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ ($k = \bar{k}$).

So $f \in \sqrt{I} \cap k[x_{\ell+1}, \dots, x_n] \subseteq \sqrt{I_\ell}$. ▨

Def Let $I, J \subseteq R$ be ideals. The **colon ideal** (or **ideal quotient**) of I and J is $I : J = \{ f \in R : fJ \subseteq I \}$.

Rmk $I : J$ is an ideal & $I \subseteq (I : J)$.

Ex $I = \langle xy, xz \rangle \subseteq \mathbb{C}[x,y,z]$ — x-axis ∪ yz-plane

$J = \langle y, z \rangle \subseteq \mathbb{C}[x,y,z]$ — x-axis — $(I : J) = \langle x \rangle$ — yz-plane

$K = \langle x \rangle \subseteq \mathbb{C}[x,y,z]$ — yz-plane — $(I : K) = \langle y, z \rangle$ — x-axis.

Fact Let $I, J \subseteq k[x_1, \dots, x_n]$ be ideals. Then

$$\overline{\mathbb{V}(I) - \mathbb{V}(J)} \subseteq \mathbb{V}(I : J).$$

If $k = \bar{k}$ and $I = \sqrt{I}$ then

$$\overline{\mathbb{V}(I) - \mathbb{V}(J)} = \mathbb{V}(I : J).$$

Rmk When $k = \bar{k}$, we have a 1-1 correspondence:

$$\begin{array}{ccc} \text{prime ideals} & \overset{\mathbb{V}}{\rightleftarrows} & \text{irreducible varieties} \\ P \subseteq k[x_1, \ldots, x_n] & \underset{\mathbb{I}}{} & V \subseteq k^n \end{array}$$

Ex If $|k| = \infty$ and $F : k^m \longrightarrow k^n$ is a polynomial mapping then $\overline{F(k^m)}$ is an irreducible subvariety of k^n.

⌜ If not, we could find $f, g \in k[x_1, \ldots, x_n]$ s.t.

$f \cdot g \in \mathbb{I}(F(k^m))$ but $f, g \notin \mathbb{I}(F(k^m))$.

$\Leftrightarrow f \circ F,\ g \circ F \in \mathbb{I}(k^m)$ but $F \circ f, F \circ g \notin \mathbb{I}(\overline{F(k^m)})$.

So ETS k^m is irreducible. This is b/c $\mathbb{I}(k^m) = 0 \subseteq k[t_1, \ldots, t_m]$ is prime. ⌟

Recall An ideal $M \subseteq R$ is maximal if $M \neq R$ and

$$M \subseteq \underset{\text{ideal}}{I} \subseteq R \Rightarrow I = M \text{ or } I = R. \quad (\text{max'l} \Rightarrow \text{prime!})$$

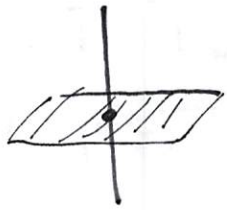
FACT If $k = \bar{k}$, we have a 1-1 corresp.

$$\begin{array}{ccc} \text{maximal ideals} & \overset{\mathbb{V}}{\rightleftarrows} & \text{points} \\ M \subseteq k[x_1, \ldots, x_n] & \underset{\mathbb{I}}{} & (a_1, \ldots, a_n) \in k^n \end{array}$$

§4.5 Irreducible Varieties

Def A variety $V \subseteq k^n$ is *irreducible* if whenever $V = V_1 \cup V_2$ for subvars V_1, V_2 we have $V = V_1$ or $V = V_2$.

eg $V = \{x\text{-axis}\} \cup \{yz\text{-plane}\}$



not irreducible!

↑ ↑

irreducible components.

~~Q Given $I \subseteq k[x_1, \ldots, x_n]$, when is $\mathbb{V}(I)$ irreducible?~~

Def An ideal $P \subseteq R$ is *prime* if $f \cdot g \in P \Rightarrow f \in P$ or $g \in P$.

Fact Let $V \subseteq k^n$ be a variety. V is irreducible $\iff$ $\mathbb{I}(V) \subseteq k[x_1, \ldots, x_n]$ is prime.

Pf $\Leftarrow$ Suppose $V = V_1 \cup V_2$ where $V_1, V_2 \neq V$ are subvarieties. Then $\mathbb{I}(V_1) \not\subseteq \mathbb{I}(V_2)$ & $\mathbb{I}(V_2) \not\subseteq \mathbb{I}(V_1)$.

So choose $f_1 \in \mathbb{I}(V_1) - \mathbb{I}(V_2)$ and $f_2 \in \mathbb{I}(V_2) - \mathbb{I}(V_1)$.

Now $f_1 \cdot f_2 \in \mathbb{I}(V_1 \cup V_2) = \mathbb{I}(V)$ but $f_1, f_2 \notin \mathbb{I}(V)$

so $\mathbb{I}(V)$ is not prime.

$\Rightarrow$ Suppose $f_1 \cdot f_2 \in \mathbb{I}(V)$ but $f_1, f_2 \notin \mathbb{I}(V)$. Then

$$V = (\mathbb{V}(f_1) \cap V) \cup (\mathbb{V}(f_2) \cap V)$$

and $\mathbb{V}(f_i) \cap V \neq V$ for $i = 1, 2$, so V is not irreducible. //

§ 4.6 Irreducible Decomposition

FACT Let k be any field. If $V_1 \supseteq V_2 \supseteq \cdots$ is a descending chain of varieties in k^n then $\exists$ N s.t. $n \geq N \Rightarrow V_n = V_N$.

Pf If $V_1 \supsetneq V_2 \supsetneq \cdots$ then $\mathbb{I}(V_1) \subsetneq \mathbb{I}(V_2) \subsetneq \cdots$ would be an infinite ascending chain of ideals in $k[x_1, \ldots, x_n]$. ▨

FACT Let $V \subseteq k^n$ be a variety. Then we can write $V = \underbrace{V_1 \cup \cdots \cup V_m}_{\text{finite!}}$ for some irred. subvarieties $V_1, \ldots, V_m \subseteq V$.

⌜ If V is irred, done, else $V = V_1 \cup V_2$ for $V_1, V_2 \subsetneq V$. If V_1, V_2 irred, done, else (say) $V_1 = V_1' \cup V_2''$ for $V_1', V_2'' \subsetneq V_1$ & $V = V_1' \cup V_1'' \cup V_2$. This process terminates b/c $\nexists$ an infinite chain $W \supsetneq W' \supsetneq W'' \supsetneq \cdots$ of subvars of k^n. ⌟