Groebner bases

October 28, 2023 3:45 PM

Reference Cox/Little/O'Shea Ch 1, 2, 3.1, 4.1, 5.3

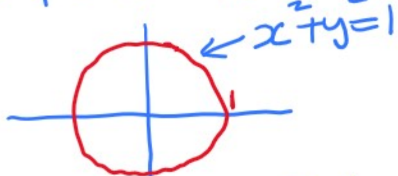
Assignment #4 due tonight @ 11pm.
Assignment #5 due in two weeks.

CLO <u>1.2 Affine Varieties in k^n where k is a field.</u>

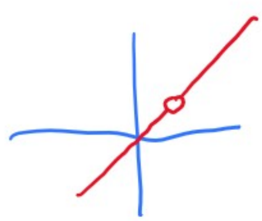
Let $f_1, f_2, \dots, f_s \in k[x_1, \dots, x_n]$, $s > 0$.
Let $\mathbb{V}(f_1, \dots, f_s) = \{ (a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \ \forall\, 1 \le i \le s \}$.
This is the set of solutions of the polynomial system $\{f_1 = 0, \dots, f_s = 0\}$.
E.g. $\mathbb{V}(0) = k^n$, $\mathbb{V}(1) = \{\}$.

Def. Let $S \subset k^n$. S is an affine variety if $\exists f_1, \dots, f_s \in k[x_1, \dots, x_n]$ s.t. $S = \mathbb{V}(f_1, \dots, f_s)$.

Examples in $\mathbb{R}^2$



$= \mathbb{V}(x^2+y^2-1)$



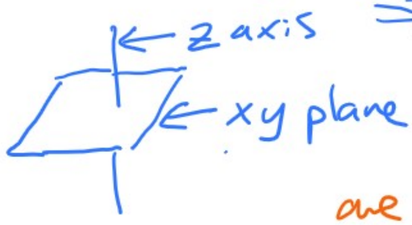
is not an affine variety.

Examples in $\underline{\mathbb{R}^3}$

$\mathbb{V}(x, y) = \{ (0,0,t) : t \in \mathbb{R} \} = z$ axis.

$\mathbb{V}(xz, yz) \Rightarrow \underline{xz = 0}$ and $\underline{yz = 0}$

$\Rightarrow z = 0$ or $x = 0$ and $y = 0$.



$= \underset{\substack{\uparrow \\ \text{xy plane}}}{\mathbb{V}(z)} \cup \underset{\substack{\uparrow \\ z \text{ axis.}}}{\mathbb{V}(x, y)}$

are irreducible varieties.

Can such a decomposition $\mathbb{V}(xz, yz) = \mathbb{V}(z) \cup \mathbb{V}(x, y)$ be computed algorithmically? Yes. <u>GB</u> + <u>factor over k</u>.
Polynomial time? In s, $\deg(f_i)$, n? No.

CLO 1.4 Ideals in $k[x_1, \ldots, x_n]$

Def. (Ideal) Let R be a comm. ring. E.g. $\mathbb{Z}$, $k[x_1, \ldots, x_n]$.
A subset I of R is an ideal of R if
(i) $0 \in I$
(ii) $f, g \in I \Rightarrow f+g \in I$
(iii) $f \in I, h \in R \Rightarrow fg \in I$.

What's the smallest ideal in R? $\{0\}$
what's the largest ideal in R? R.
Trivial Ideals.

Example. $R = \mathbb{Z}$. $I = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ is an ideal.

Def. Ideals in $k[x_1, \ldots, x_n] = R$.
Let $f_1, \ldots, f_s \in R$. Define
$$\langle f_1, \ldots, f_s \rangle = \{ h_1 f_1 + h_2 f_2 + \cdots + h_s f_s : h_i \in R \}.$$

Lemma. $I = \langle f_1, \ldots, f_s \rangle$ is an ideal of R.
Proof. (i) $h_i = 0$: $0 \cdot f_1 + 0 f_2 + \cdots + 0 \cdot f_s = 0 \Rightarrow 0 \in I$.
(ii). Let $f, g \in I \Rightarrow f = \sum_{i=1}^{s} h_i f_i$ and $g = \sum_{i=1}^{s} t_i f_i$
where $h_i, t_i \in R$.
$$f+g = \sum h_i f_i + \sum t_i f_i = \sum (\overset{R}{h_i} + \overset{R}{t_i}) \cdot f_i \Rightarrow f+g \in I.$$
$$\underset{R}{\underbrace{h_i+t_i}}$$
(iii) Let $f \in I, h \in R$. $\Rightarrow f = \sum h_i f_i$
$$\Rightarrow f \cdot h = \left(\sum h_i f_i\right) \cdot h = \sum (\underset{R}{\underbrace{\overset{R}{h_i} \cdot h}}) f_i \in I.$$

Exercise. If I and J are ideals of R.
Prove or disprove $I \cap J$ and $I \cup J$ is an ideal of R.

Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal of $k[x_1, \ldots, x_n]$.
We say $\{f_1, \ldots, f_s\}$ generates I or is a basis for I.

Bases are not unique.

Ex. Let $I = \langle x, y \rangle$ in $k[x,y]$.

Then $x+y \in I$ because $h_1 = 1, h_2 = 1$, $h_1 \cdot x + h_2 \cdot y \in I$.

Consider $J = \langle x, y, x+y \rangle$. I claim $I = J$. Proof.

$(I \subset J)$: $f \in I \Rightarrow f = A \cdot x + B \cdot y = \underline{A} \cdot x + \underline{B} \cdot y + \underline{0} \cdot (x+y) \in J$.

$(J \subset I)$: $f \in J \Rightarrow f = Ax + By + C(x+y)$

$= (A+C)x + (B+C) \cdot y \in I$.

Lemma. Let $I = \langle f_1, \ldots, f_s \rangle$ and $J = \langle g_1, \ldots, g_t \rangle$.

If $f_i \in J$ and $g_i \in I$ then $I = J$.

$(I \subset J)$ Let $f \in I \Rightarrow f = \sum h_i f_i \Rightarrow f = \sum_{i=1}^{s} h_i \left[\sum_{j=1}^{t} a_{ij} g_j \right]$

But $f_i \in J \Rightarrow f_i = \sum_{j=1}^{t} a_{ij} \cdot g_j$ $\quad = \sum_{j=1}^{t} \underbrace{\left[\sum_{i=1}^{s} a_{ij} h_i \right]}_{\in R} g_j \in J$.

$(J \subset I)$. Same argument.

Ex. $I = \langle \overset{f_1}{x+y}, \overset{f_2}{x+z}, \overset{f_3}{y-z} \rangle$.

Notice $f_3 = f_1 - f_2 \Rightarrow f_3 \in \langle \overset{f_1}{x+y}, \overset{f_2}{x+z} \rangle = J$.

$h_1 = 1 \quad h_2 = -1$

Thus $I = \langle x+y, x+z \rangle$. $\quad f_3 = f_1 - f_2 \in J$.

Def. We say $B = \{f_1, \ldots, f_s\}$ is <u>a minimal basis</u> for $I = \langle f_1, \ldots, f_s \rangle$ if $B \setminus \{f_i\}$ is not a basis for I.

Claim $\{x+y, y-z\}$ is a minimal basis for $\langle x+y, y-z \rangle$.

Proof. Is $I = \langle x+y \rangle$? No $y - z \notin \langle x+y \rangle = \{h_1 \cdot (x+y) : h \in R\}$.

as $y-z$ is not a multiple of $x+y$.

Is $I = \langle y-z \rangle$? No $x+y \notin \langle y-z \rangle$.