Applications of Nullstellensatz.

25 Jan.

k = alg. closed field

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

$(V(I(V)) = V$ affine.)

Prop 4.7

$$\{\text{affine alg. sets in } k^n\} \underset{V(-)}{\overset{I(-)}{\rightleftarrows}} \{\text{radical ideals in } k[x_1,\dots,x_n]\}$$

$V \hookrightarrow I(V)$

$V(I(V)) \hookleftarrow I$ $(= \sqrt{I})$

$V(I) \hookleftarrow I$ ← Nullstellensatz.

$V(I) \hookrightarrow I(V(I))$

Moreover:

(a) V irred $\iff$ $I(V)$ is prime. (from 3.2)

(b) V point. $\iff$ $I(V)$ is max

pf of (b):

$\Rightarrow$ Assume $V = \{x\}$.

$$I(V) \subseteq I(V') \subseteq k[x_1,\dots,x_n]$$

($I(V')$: max.)

$$\{x\} = V \supseteq V' \neq \emptyset$$

($V = V(I(V))$, $V' = V(I(V'))$)

$\Rightarrow V = V'$

$\Rightarrow I(V)$ max. //

$\Leftarrow$ Suppose $I(V)$ max.

Let $x \in V$. Then $\{x\} \subseteq V \Rightarrow I(\{x\}) \supseteq I(V)$

($I(\{x\})$: proper. $I(V)$: max)

$\Rightarrow I(V) = I(\{x\})$.

$\Rightarrow V = \{x\}$. //

Prop 4.8:

V finite $\Leftrightarrow$ $\Gamma(V)$ finite dim k-v.s.

$\Gamma(V) = k[x_1, \dots, x_n]/I(V)$

Pf:

$\Rightarrow$ $V = \{a_1, \dots, a_r\}$

Consider hom $\varphi: k[x_1, \dots, x_n] \longrightarrow k^r$

$F \longmapsto (F(a_1), \dots, F(a_r))$

$\ker\varphi = I(V)$ (check) $\Rightarrow$ $\Gamma(V) = \dfrac{k[x_1, \dots, x_n]}{\ker\varphi} \cong$ image $\subseteq k^r$

$\Rightarrow \Gamma(V)$ fin dim k-v.s.

$\Leftarrow$ Assume $\Gamma(V)$ fin. dim.

In $\Gamma(V) = k[x_1, \dots, x_n]/I(V)$, $\exists\ s \geq 1, a_i \in k$

s.t. $a_s \bar{x}_i^s + a_{s-1}\bar{x}_i^{s-1} + \cdots + a_1 \bar{x}_i + a_0 1 = 0$

lin dep over k.

If $u = (x_1, \dots, x_n) \in V$,

then $a_s x_i^s + \cdots + a_1 x_i + a_0 = 0$ for each i.

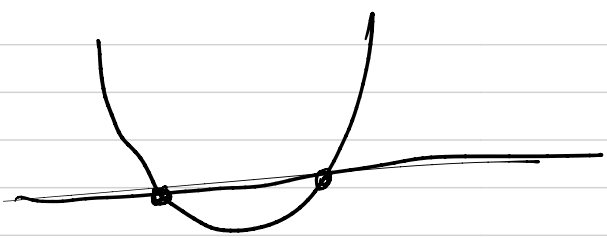
$\Rightarrow$ finite # of choices for x_i

$\Rightarrow$ finite # of choices for u.

$\Rightarrow$ V is finite. //

Exercise:

Find (k-basis for) $S(V) = k[X,Y]/I(V)$



$V = V(Y^2,\ Y-X^2+1) \subseteq k^2$

$I(V) = (Y,\ Y-X^2+1)$

$$k[X,Y]/(Y,\ Y-X^2+1) \cong k[X]/(X^2-1)$$

$k \oplus kx \cong k[X]/(X^2-1)$ as k-vs.

$(1,0)$

$(-1,0)$

RETURN at 11:15

$I(V(Y^2, Y-X^2+1)) = \sqrt{(Y^2, Y-X^2+1)}$?

$\sqrt{J} = \bigcap_{\substack{p \text{ p.i.m.} \\ p \supseteq J}} p$ //

Eisenstein's criterion.

$p \supseteq (Y^2, Y-X^2+1)$

$Y^2 \in p \Rightarrow Y \in p \Rightarrow X^2-1 = (X+1)(X-1)$

$p \supsetneq x+1$ $\qquad$ $p \supsetneq x-1$

$(Y, x+1) \cap (Y, x-1) \overset{\supseteq}{=} (Y, x+1)(Y, x-1)$

$(Y, x+1) + (Y, x-1) = K[x, Y]$ comaximal

(x^2-1, Y)

char $k \neq 2$.

char $k = 2$: $(Y, x+1) \cap (Y, x-1) = (Y, x+1)$

$K[x]/(x^2-1)$

2 dim

if char $k \neq 2$

$K[x]/(x+1) \cong K$.

1 dim

if char $k = 2$

More generally, if $W \subseteq V$ affine alg sets, then $I(W) \supseteq I(V)$

Then in $\Gamma(V)$:

- $I_V(W) \subseteq k[x_1, \dots, x_n] / I(V)$

  "$I(W)/I(V)$"

- $\Gamma(V) / I_V(W) \cong \Gamma(W)$ (check).

Prop 4.9

$$\left\{ \begin{array}{l} \text{affine alg subsets} \\ \text{contained in } V \end{array} \right\} \underset{V(-)}{\overset{I(-)}{\rightleftarrows}} \left\{ \begin{array}{l} \text{radical ideals} \\ \text{of } \Gamma(V) \end{array} \right\}$$

And: a) W irred $\iff$ $I_V(W)$ prime in $\Gamma(V)$

b) W point $\iff$ $I_V(W)$ max in $\Gamma(V)$

c) W irred component of V $\iff$ $I_V(W)$ min prime of $\Gamma(V)$.

Cor: $\{ \text{points of } V \} \overset{1-1}{\longleftrightarrow} \{ \text{max ideals of } \Gamma(V) \}$.

Ex: Find max ideals of

$$k[X,Y] / (XY).$$

max ideals of $k[X,Y]/(XY)$ $\longleftrightarrow$ points of $V(XY) = \{(a,b) \in k^2 \mid ab = 0\}$

$\{(X-a, Y)\} \cup \{(X, Y-b)\}$

$(X-1, Y-1)$ not max?

$(\bar{X}-1, \bar{Y}-1) = k[X,Y]/(XY)$ does not contain (XY)

---

(5) First steps toward Bézout

Thm 5.1: $F, G \in k[X,Y]$, nonzero, no common factor, then $V(F) \cap V(G)$ is finite.

Lemma: There exists a nonzero poly $d \in k[X]$ s.t. $d = AF + BG$ (i.e. $d \in (F,G)$.)

$A \in k[X,Y]$, $B \in k[X,Y]$

Pf of Lemma:

$\widetilde{k(X)[Y]}$ PID

/

$\checkmark$ in here

$$(F, G) = (d) \quad \text{in} \quad k(X)[Y].$$

$$\Rightarrow \quad d \mid F, G$$

$$\Rightarrow \quad F = d \cdot \frac{f}{p(x)} \qquad G = d \cdot \frac{g}{q(x)}$$

$$\Rightarrow \quad \underbrace{p(x)\,F}_{d \mid g} = d \cdot f \qquad \underbrace{q(x)\,G}_{d \mid g} = d g.$$

$\uparrow$ in $k[X,Y]$ $\uparrow$

(UFD) $\quad d \mid p(x)$ or $q(x) \quad \Rightarrow \quad d \in k[X].$

$\square$