Hilbert's Nullstellensatz

given $V \subseteq k^n$ a variety

$$I(V) = \{ f \in k[x_1, \dots, x_n] \mid f(a) = 0 \ \forall a \in V \}$$

given an ideal $J \subseteq k[x_1, \dots, x_n]$

$$V(J) = \{ a \in k^n \mid f(a) = 0 \ \forall f \in J \}$$

question is if $J = (f_1, \dots, f_s)$

How do we relate J and $I(V(J))$?

$\boxed{\text{Ex}}$ • $V(x) = V(x^2) = \{0\}$

(x), (x^2) are different

• $I_1 = (1) = \mathbb{R}[x]$, $I_2 = (1+x^2) \subseteq \mathbb{R}[x]$, $I_3 = (1+x^2+x^4) \subseteq \mathbb{R}[x]$

$$V(I_1) = V(I_2) = V(I_3) = \phi .$$

<u>Thm.</u> (The Weak Nullstellensatz)
Let k be an alg. closed field and let $I \subseteq k[x_1, \dots, x_n]$ be an ideal s.t. $V(I) = \phi$. Then $I = (1) = k[x_1, \dots, x_n]$

<u>Proof:</u>

Prove the contrapositive: $I \subsetneq k[x_1, \dots, x_n] \Rightarrow V(I) \neq \emptyset$

find a point in $V(I)$

Let $a \in k$

ideal in $k[x_1, \dots, x_{n-1}]$

$$I_{x_n = a} = \{ f(x_1, \dots, x_{n-1}, a) \mid f \in I \}$$

Claim: $I \subsetneq k[x_1, \dots, x_n]$ a proper ideal

$\Rightarrow \exists\, a \in k$ s.t. $I_{x_n=a} \subsetneq k[x_1, \dots, x_{n-1}]$ is also proper

[i.e. can get proper ideal by eval. a proper ideal]

Once this proved $\Rightarrow$ induction gives $a_1, \dots, a_n \in k$

s.t. $I_{x_n=a_n, \dots, x_1=a_1} \subsetneq k$, but only ideals in a field are $\{0\}$ and k

$\Rightarrow I_{x_n=a_n, \dots, x_1=a_1} = \{0\} \Rightarrow$ all poly in I vanish at $(a_1, \dots, a_n)$

$\Rightarrow (a_1, \dots, a_n) \in V(I) \quad \therefore V(I) \neq \emptyset.$

Case 1 $\quad I \cap k[x_n] \neq \{0\}$

Let $f^{\neq 0} \in I \cap k[x_n]$, $f \neq c \in k$ since $I \neq (1)$

$$\boxed{\text{Since } k \text{ alg. closed } \quad f = c \prod_{i=1}^{r} (x_n - b_i)^{m_i}}$$

Suppose $I_{x_n = b_i} = k[x_1, \dots, x_{n-1}] \quad \forall i$

$\Rightarrow \forall i \;\exists\, B_i \in I$ s.t. $B_i(x_1, \dots, x_{n-1}, b_i) = 1$

$\Rightarrow \forall i$

$$1 = B_i(x_1, \dots, x_{n-1}, b_i) = B_i(x_1, \dots, x_{n-1}, x_n - (x_n - b_i))$$

$$= B_i(x_1, \dots, x_n) + \underset{\uparrow \text{ some poly}}{A_i} \cdot (x_n - b_i)$$

$$\therefore \quad 1 = \prod_{i=1}^{r} (A_i \cdot (x_n - b_i) + B_i)^{m_i}$$

$$= A \prod_{i=1}^{r} (x_n - b_i)^{m_i} + B$$

For $A = \prod A_i^{m_i}$, $B \in I$

but $f = C \prod (x_n - b_i)^{m_i} \in I \quad \therefore \prod_{i=1}^{r} (x_n - b_i)^{m_i} \in I$

$$\therefore \quad \left(A \prod_{i=1}^{r} (x_n - b_i)^{m_i} + B\right) \in I$$

$\therefore \quad 1 \in I$ which is a contradiction.

$\therefore \quad I_{x_n = b_i} \neq k[x_1, \dots, x_{n-1}]$ for some i

$a = b_i$.

<u>Case 2</u>: $I \cap k[x_n] = \{0\}$

- $\{g_1, \dots, g_t\}$ a GB of I with lex $x_1 > \dots > x_n$

write

$$g_i = \overbrace{c_i(x_n) \underset{\text{monomial in } x_1, \dots, x_{n-1}}{x^{\alpha_i}}}^{\text{Leading term}} + \text{terms} < x^{\alpha_i}$$

$c_i(x_n) \in K[x_n]$ non-zero

Pick an $a \in K$ s.t $c_i(a) \neq 0$ $\forall i$

(we can do this since alg. closed fields are infinite Ex 4)

$\overline{g_i} = g_i(x_1, \dots, x_{n-1}, a)$ forms a basis for $I_{x_n=a}$

$LT(\overline{g_i}) = c_i(a) x^{\alpha_i}$ since $c_i(a) \neq 0$

and since $x^{\alpha_i} \neq 1$ since if $g_i = c_i \in I \cap K[x_n] = \{0\}$
$\Rightarrow c_i = 0$

but this is not tre. since chosen a s.t $c_i(a) \neq 0$.

$\therefore$ $LT(\overline{g_i})$ is non-constant $\forall i$

- $\overline{g_i}$ form a GB of $I_{x_n=a}$

$\Rightarrow$ $1 \notin I_{x_n=a}$ since $LT(\overline{g_i})$ can not divide 1 (since non constant) and everything in $LT(I)$ must be div. by $LT(\overline{g_i})$

$\therefore$ $I_{x_n=a} \neq K[x_1, \dots, x_n]$

This proves the theorem.

Consider

$$S = c_i(x_n) c_j(x_n) S(g_i, g_j) \overset{\in I}{=} \sum_{l=1}^{t} A_l g_l$$

Since have lcm rel

$$\operatorname{lcm}(g_i, g_j) = \operatorname{lcm}(c_i x^{\alpha_i}, c_j x^{\alpha_j}) > LT(S(g_i, g_j))$$

Evaluating at $x_n = a$ $\quad \overline{S} = c_i(a)\, c_j(a)\, S(\overline{g_i}, \overline{g_j})$

and

$$\operatorname{lcm}(x^{\alpha_i}, x^{\alpha_j}) = \operatorname{lcm}(LM(\overline{g_i}), LM(\overline{g_j}))$$
$$> LT(\overline{A_l}\, \overline{g_l})$$

$\therefore$ we have an lcm rep of $S(\overline{g_i}, \overline{g_j})$

$\therefore$ these are a GB. $\blacksquare$