Hilbert's Nullstellensatz

Corollary 3 (Hilbert's Nullstellensatz, weak form): let $\mathbb{K}$ be an algebraically closed field and $R := \mathbb{K}[x_1, \dots, x_n]$ be the polynomial ring in n variables. Then every maximal ideal $\mathfrak{m}$ of R is of the form $\mathfrak{m} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in \mathbb{K}$.

Proof: Note that $S := R/\mathfrak{m}$ is a field, and also a finitely generated $\mathbb{K}$-algebra (since R is). By corollary 2, S is an algebraic extension of $\mathbb{K}$. Since $\mathbb{K}$ is algebraically closed, we have $S \simeq \mathbb{K}$, and $\mathfrak{m}$ is the kernel of the map $\varphi_{\mathfrak{m}} : R \to S \simeq \mathbb{K}$. As $\varphi_{\mathfrak{m}}(x_i) = \alpha_i$ for some $\alpha_i \in \mathbb{K}$, we have $I := (x_1 - \alpha_1, \dots, x_n - \alpha_n) \subset \mathfrak{m}$. Since I is maximal, we have $I = \mathfrak{m}$ and we are done. $\square$

Corollary 4 (Nullstellensatz, alternate weak form): let $\mathbb{K}$ be algebraically closed and $f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n]$.
$1 \in (f_1, \dots, f_m) \iff V(f_1, \dots, f_m) = \emptyset$.

Proof: $(\Leftarrow)$ $1 \notin (f_1, \dots, f_m) \Rightarrow (f_1, \dots, f_m) \subset \mathfrak{p}$ maximal ideal $\Rightarrow \exists \bar{\alpha} := (\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ s.t. $\mathfrak{p} = (x_i - \alpha_i)_{i=1}^n$
corollary 3

$\Rightarrow f_i(\bar{\alpha}) = 0 \quad \forall i \in [m] \Rightarrow V(f_1, \dots, f_m) \ni (\alpha_1, \dots, \alpha_n)$
$\therefore V(f_1, \dots, f_m) \neq \emptyset$.

$(\Rightarrow)$ $1 \in (f_1, \dots, f_m) \Rightarrow \exists g_1, \dots, g_m \in \mathbb{K}[x_1, \dots, x_n]$ s.t.
$1 = \sum_{i=1}^m f_i g_i \Rightarrow$ for any $\bar{\alpha} \in \mathbb{K}^n$ $\quad 1 = \sum_{i=1}^m f_i(\bar{\alpha}) \cdot g_i(\bar{\alpha})$

$\Rightarrow \exists i \in [m]$ s.t. $f_i(\bar{\alpha}) \neq 0$. $\Rightarrow V(f_1, \dots, f_m) = \emptyset$. $\square$

Corollary 5 (Nullstellensatz, strong form): let $\mathbb{K}$ be an algebraically closed field and $R := \mathbb{K}[x_1, \dots, x_n]$ be the polynomial ring in n variables. Let $g, f_1, \dots, f_m \in R$. Then

$$g \in \operatorname{rad}(f_1, \dots, f_m) \iff V(g) \supseteq V(f_1, f_2, \dots, f_m).$$

Proof: $(\Rightarrow)$ $g \in \operatorname{rad}(f_1, \dots, f_m) \Rightarrow \exists N \in \mathbb{N}, g_1, \dots, g_m \in R$ s.t. $g^N = \sum_{i=1}^m f_i g_i \quad \therefore \bar{\alpha} \in V(f_1, \dots, f_m) \Rightarrow g(\bar{\alpha})^N = 0$
$\Rightarrow \bar{\alpha} \in V(g)$.

$(\Leftarrow)$ Let $I = (f_1, \dots, f_m, 1 - yg) \in \mathbb{K}[x_1, \dots, x_n, y] =: S$.
$V(g) \supseteq V(f_1, \dots, f_m) \Rightarrow V(f_1, \dots, f_m, 1 - yg) = \emptyset \Rightarrow$
corollary 4
$1 \in (f_1, \dots, f_m, 1 - yg) \Rightarrow$
$\exists h_1, \dots, h_m, h \in S$ s.t.

$$1 = (1 - yg)h + \sum_{i=1}^m f_i h_i \quad (*)$$

Let $D \in \mathbb{N}$ be s.t. $D \geq \max\{\deg_y h + 1, \max_{i \in [m]}\{\deg_y h_i\}\}$

$\Rightarrow$ in $(*)$ substituting $y = \frac{1}{g}$ and multiplying both sides by g^D we get $g^D = \sum_{i=1}^m f_i \cdot \underbrace{g^D \cdot h_i(\bar{x}, 1/g)}_{g_i(\bar{x})}$

with $g_i(\bar{x}) \in R$ by choice of D $\therefore g \in \operatorname{rad}(f_1, \dots, f_m)$. $\square$

Corollary 6 (Nullstellensatz, alternate strong form): let $\mathbb{K}$ be an algebraically closed field, $R = \mathbb{K}[x_1, \dots, x_n]$ be a polynomial ring and $I \subset R$ be an ideal. Then

$$\operatorname{rad}(I) = \bigcap_{\substack{\mathfrak{p} \supset I \\ \mathfrak{p} \text{ maximal}}} \mathfrak{p}.$$

Proof: $(\subset)$ this follows since every $\mathfrak{p}$ on the RHS contains I (and thus $\operatorname{rad}(I)$, since $\mathfrak{p}$ maximal).
$(\supset)$ $\bar{\alpha} \in V(I) \Rightarrow \mathfrak{m}_{\bar{\alpha}} := (x_1 - \alpha_1, \dots, x_n - \alpha_n) \supset I$ (and thus $\operatorname{rad}(I)$). Now, $g \in \bigcap_{\substack{\mathfrak{p} \supset I \\ \mathfrak{p} \text{ maximal}}} \mathfrak{p} \Rightarrow$

$g \in \mathfrak{m}_{\bar{\alpha}} \quad \forall \bar{\alpha} \in V(I) \Rightarrow V(g) \supset V(I) \Rightarrow g \in \operatorname{rad}(I)$. $\square$
corollary 5