# Lecture VII: Hilbert Nullstellensatz

**Recall:** Basic duality for affine subvarieties of $\mathbb{A}^n$:

GEOMETRY | ALGEBRA

$$\left\{ \begin{matrix} \text{Subvarieties} \\ \text{of } \mathbb{A}^n \end{matrix} \right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{ \begin{matrix} \text{radical ideals } \mathfrak{a} \\ \text{of } \mathbb{K}[x_1, \ldots, x_n] \end{matrix} \right\}$$

**Proposition:** (1) If $W \subseteq \mathbb{A}^n$ is a subvariety, then $V(I(W)) = W$

(2) For any ideal $\mathfrak{a} \in \mathbb{K}[x_1, \ldots x_n]$ $\quad I(V(\mathfrak{a})) \supseteq \sqrt{\mathfrak{a}}$

• Natural questions for $\overline{\mathbb{K}} = \mathbb{K}$:

① [Consistency] Can we determine if a solution set is empty or not?
A: YES (Hilbert's Nullstellensatz)

② [Finiteness] Can we determine number of solutions? If finite, can we compute them?

→ ③ [Dimension] Can we determine the "dimension" of a solution set? (HARD!)

④ [Local Parameterization] Can we parameterize a subvariety of $\mathbb{A}^n$ by a map $\mathbb{K}^m \overset{\varphi}{\dashrightarrow} \mathbb{K}^n$ with rational functions?
A: NOT always!

⑤ [Implicitization] Can we determine equations cutting out the image of a rat'l map $\varphi: \mathbb{K}^m \dashrightarrow \mathbb{K}^n$? A: YES, using elimination!

• Gröbner bases will help answer some of these questions.

## §1. Hilbert Nullstellensatz:

Hilbert's Nullstellesatz (Null = Zeroes, Stellen = Location, Satz = Theorem/Statement) will ensure the basic duality is a 1-to-1 correspondence when $\mathbb{K} = \overline{\mathbb{K}}$.
The statement has 2 versions: a strong one & a weak one (special case $V = \emptyset$)

**Hilbert's Nullstellensatz:** (Strong version) If $\mathbb{K} = \overline{\mathbb{K}}$ & $\mathfrak{a} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal, then
$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

Remark: We know $I(X)$ is radical for any variety & $I(V(\mathfrak{a})) \supseteq \mathfrak{a}$, so the inclusion ($\supseteq$) is always true (we don't need $\overline{\mathbb{K}} = \mathbb{K}$ for this part)

The next statement characterizes empty varieties (and justifies the terminology)

Weak Hilb. Nullstellensatz: If $\mathbb{K} = \overline{\mathbb{K}}$ & $\mathfrak{a}$ is an ideal of $\mathbb{K}[x_1, \ldots x_n]$ we have

$$V(\mathfrak{a}) = \emptyset \iff \mathfrak{a} = (1) = \mathbb{K}[x_1, \ldots x_n]$$

Remark: Can think of this as a Fundamental Theorem of Algebra for multivariable polynomials over $\mathbb{C}$.

Proof: ($\Leftarrow$) is direct

($\Rightarrow$) Follows from the Strong Nullstellensatz. Indeed, if $V(\mathfrak{a}) = \emptyset$, then $\sqrt{\mathfrak{a}} = I(V(\mathfrak{a})) = I(\emptyset) = R$. This says that $1 \in \sqrt{\mathfrak{a}}$ ie $\exists N \geq 1$ with $1 = 1^N \in \mathfrak{a}$, so $\mathfrak{a} = (1)$ as we wanted.

- Interestingly enough, we can show that both statements are equivalent:

Lemma 1: Weak Nullstellensatz $\Rightarrow$ Strong Nullstellensatz

Proof Since $\mathbb{K}[x_1, \ldots, x_n]$ is Noetherian, we will write $\mathfrak{a} = (f_1, \ldots, f_s)$ for some choice of polynomials $f_1, \ldots, f_s$

Fix $f \in I(V(\mathfrak{a}))$. We want to find $m \geq 1$ with $f^m \in \mathfrak{a}$, ie $\exists g_1 \ldots g_s$ with
$$f^m = \sum_{j=1}^{s} g_j f_j$$

We prove this with an ingenious trick (Rabinowitch's Trick [1929]) introducing an extra dummy variable:

Consider the ideal
$$\underset{\substack{\cup\!\!\!\mid \\ \mathfrak{a}\,\mathbb{K}[x_1, \ldots, x_n, y]}}{\tilde{\mathfrak{a}}} = (f_1(\underline{x}), \ldots, f_s(\underline{x}), 1 - y f(\underline{x})) \subseteq \mathbb{K}[x_1, \ldots, x_n, y]$$

Claim: $V(\tilde{\mathfrak{a}}) = \emptyset$

Pf/ We argue by contradiction & pick $c = (a_1, \ldots, a_n, b) = (\underline{a}, b) \in V(\tilde{\mathfrak{a}})$

Thus, $\underline{a}$ satisfies 2 conditions from the generators of $\tilde{\mathfrak{a}}$:

(1) $f_1(\underline{a}) = \cdots = f_s(\underline{a}) = 0$, so $\underline{a} \in V(f_1 \ldots f_s) = V((f_1 \ldots f_s)) = V(\mathfrak{a})$

(2) $1 - b f(\underline{a}) = 0$. so $f(\underline{a}) \neq 0$ ie $f \notin I(\{\underline{a}\})$

Thus: $f \notin \underbrace{I(\{a\}) \supseteq I(V(\mathfrak{a}))}_{\text{by (1)}}$ & $f \in I(V(\mathfrak{a}))$ by hypothesis Contr! $\square$

By the Weak Nullstellensatz applied to $\tilde{\mathfrak{a}}$ we get $\tilde{\mathfrak{a}} = (1) \in \mathbb{K}[x_1 \ldots x_n, y]$

That means $\exists\, h_1 \ldots h_n$, $h \in \mathbb{K}[\underline{x}, y]$ with

$$(*) \quad 1 = \sum_{i=1}^{s} h_i(\underline{x}, y)\, f_i(\underline{x}) + h_{(\underline{x},y)}\,(1 - y f(\underline{x}))$$

Set $m = \max\{\deg_y(h_1), \ldots, \deg_y(h_s), \deg_y h\} \geq 0$ & multiply both sides of $(*)$ by $f^m_{(x)}$:

$$f^m_{(\underline{x})} = \sum_{i=1}^{s} (f^m_{(x)} h_i(\underline{x}, y))\, f_i(\underline{x}) + f^m_{(\underline{x})} h_{(\underline{x},y)}\,(1 - y f(x)).$$

Then setting $y = \frac{1}{f(x)}$ gives:

$$f^m_{(\underline{x})} = \sum_{i=1}^{s} \underbrace{f^m_{(x)} h_i\left(\underline{x}, \tfrac{1}{f(x)}\right)}_{\in \mathbb{K}[x] \text{ by choice of } m} f_i(x) + \underbrace{f^m_{(\underline{x})} h\left(\underline{x}, \tfrac{1}{f(\underline{x})}\right)}_{\in \mathbb{K}[x] \text{ by choice of } m} \cdot 0$$

Hence, $f^m \in (f_1, \ldots, f_s)\,\mathbb{K}[x] = \mathfrak{a}$, as we wanted. $\square$

## §2 Proofs of the Weak Nullstellensatz:

There are several proofs of this statement:

① Elementary proof using Gröbner basis (will do this in a future lecture) [Glebsky (2012)]

② Special case: characterization of maximal ideals of $\mathbb{K}[x_1 \ldots x_n]$ for $\mathbb{K} = \overline{\mathbb{K}}$.
(Commutative Algebra heavy proof using Going-up Theorem + Noether Normalization)

Next, we outline proof ① for the non-trivial implication of the WN statement.

Proof ② will be discussed next time.

**Proof 1:** We will show the contrapositive, ie $\mathfrak{a} \subsetneq (1) \Rightarrow V(\mathfrak{a}) \neq \emptyset$.

The argument will involve intersecting $\mathfrak{a}$ with hyperplanes $x_n = a_n$, $x_{n-1} = a_{n-1}$, ..., $x_1 = a_1$ for suitable $a_n, a_{n-1}, \ldots, a_1 \in \mathbb{K}$ so that each ideal

$$\mathfrak{a}_j = (\mathfrak{a} + \langle x_n - a_n, \ldots, x_j - a_j \rangle) \cap \mathbb{K}[x_1, \ldots, x_{j-1}]$$

remains proper.

By induction, it suffices to show this for one step. Fix $a_n = a \in \mathbb{K}$

**Claim 1:** $\mathfrak{a}_n = \{ \overline{f} \mid f \in \mathfrak{a} \}$ where $\overline{f}(x_1 \ldots x_{n-1}) = f(x_1 \ldots x_n, a)$

Pf/ We show the double inclusion:

($\subseteq$) If $g \in (\mathfrak{a} + (x_n - a)) \cap \mathbb{K}[x_1 \ldots x_{n-1}]$, then

$$g(x_1 \ldots x_{n-1}) = \underset{\in \mathfrak{a}}{f(x_1 \ldots x_n)} + h(x_1 \ldots x_{n-1})(x_n - a) \quad \text{is indep of } x_n.$$

Evaluating both sides at $x_n = a$ gives $g(x_1 \ldots x_{n-1}) = \overline{f} + h(x_1 \ldots x_{n-1}) \cdot 0 = \overline{f}$ ✓

($\supseteq$) Writing $f(x_1 \ldots x_n) = \sum_{j=0}^{m} f_j(\underline{x'}) x_n^j \in \mathfrak{a}$ for $x' = (x_1, \ldots x_{n-1})$

gives $f(x', x_n) = \sum_{j=0}^{m} f_j(x') \sum_{k=0}^{j} \binom{j}{k} a^{j-k} (x_n - a)^k$

(Write $x_n = (x_n - a) + a$)

$$= \sum_{j=0}^{m} f_j(x) a^j + \sum_{j=1}^{m} f_j(x') \sum_{k=1}^{j} \binom{j}{k} a^{j-k} (x_n - a)^k$$

(k=0 for all j) (k>0 terms for all j>1)

$$= \overline{f}(x') + (x_n - a) \underbrace{\left( \sum_{j=1}^{m} \left( \sum_{k=1}^{j} \binom{j}{k} a^{j-k} (x_n - a)^{k-1} \right) f_j(x') \right)}_{=: g(x)}$$

<u>Conclude</u>: $\underset{\mathbb{K}[x']}{\overline{f}(x')} = \underset{\mathfrak{a} + (x_n - a)}{f(x) - g(x)(x_n - a)}$, so $\overline{f} \in \mathfrak{a}_n$

**Claim 2:** If $\overline{\mathbb{K}} = \mathbb{K}$ and $\mathfrak{a} \subsetneq \mathbb{K}[x_1 \ldots x_n]$, then there is $a \in \mathbb{K}$ such that $\mathfrak{a}_n \subsetneq \mathbb{K}[x_1 \ldots x_{n-1}]$

**Remark:** Proof of Claim 2 requires us to pick a suitable set of generators for $\mathfrak{a}$ (a Gröbner basis with respect to the lexicographic order). We will prove this claim in a future homework, after we've seen Gröbner bases.

• Induction on $n$ combined with Claim 2 allow us to pick values $a_n, \dots, a_1$ so that $\mathfrak{a}_1 \left(= \{ f(a_1, \dots, a_n) \quad f \in \mathfrak{a} \} \text{ by Claim 1}\right)$ is a proper ideal of $\mathbb{K}$. Since $\mathbb{K}$ is a field, we get $\mathfrak{a}_1 = (0)$ ie $f(\underline{a}) = 0 \ \forall f \in \mathfrak{a}$. This shows $\exists \, \underline{a} \in V(\mathfrak{a})$, ie $V(\mathfrak{a}) \neq \emptyset$. $\square$