Lecture VIII: Hilbert Nullstellensatz II

Last time we discussed the following 2 theorems.

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
$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

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 $\mathbb{C}$.

Lemma: Strong & Weak versions are equivalent

We discussed a proof of the Weak Nullstellensatz via slicing with hyperplanes $x_i = a_i$.

TODAY: we'll discuss a different proof using Noether Normalization + Going-Up.

§1. Maximal ideals of $\mathbb{K}[x_1, \ldots x_n]$ when $\overline{\mathbb{K}} = \mathbb{K}$:

Our first result characterizes maximal ideals of $\mathbb{K}[x_1, \ldots, x_n]$ when $\overline{\mathbb{K}} = \mathbb{K}$

Theorem 1: Fix $\mathbb{K} = \overline{\mathbb{K}}$ a field. Then, all maximal ideals of $\mathbb{K}[x_1, \ldots x_n]$ are of the form $\mathfrak{m}_{\underline{a}} = (x_1 - a_1, \ldots, x_n - a_n)$ for some $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}}$

The rest of today will be devoted to proving this statement. But first, we discuss 2 key consequences of this statement.

Corollary 1: Weak Nullstellensatz

Proof: Since $\mathfrak{a} \subsetneq \mathbb{K}[x_1, \ldots, x_n]$ is a proper ideal we can find $\mathfrak{m} \subsetneq \mathbb{K}[\underline{x}]$ maximal ideal with $\mathfrak{a} \subseteq \mathfrak{m}$. By Theorem 1 $(\overline{\mathbb{K}} = \mathbb{K})$ we have $\mathfrak{m} = \mathfrak{m}_{\underline{a}}$ for some $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$.
Taking $V(\;)$ we get the reverse inclusion $V(\mathfrak{a}) \supseteq V(\mathfrak{m}_{\underline{a}}) = \{a\}$, so $V(\mathfrak{a}) \neq \emptyset$, as we wanted to show. □

Corollary 2: Fix an affine subvariety $W \subseteq \mathbb{A}^n_{\mathbb{K}}$. If $\overline{\mathbb{K}} = \mathbb{K}$, there is a 1-to-1 correspondence between:

$$\boxed{\begin{array}{ccc} \{ \text{(closed) points of } W \} & \xleftrightarrow{\text{1-to-1}} & \left\{ \begin{array}{l} \text{maximal ideals of } \mathbb{K}[x_1,\dots,x_n] \\ \text{containing } I(W) \end{array} \right\} \\ \underline{a} & \longmapsto & m_{\underline{a}} \\ V(m) & \longleftarrow & m \end{array}}$$

Remark: We emphasize closed points because in scheme theory there are other points on an affine scheme $=$ Spec(A) for A a ring.

$$\boxed{\text{Points of Spec}(A) \xleftrightarrow{\text{1-to-1}} \text{Prime ideals of } A}$$

So if A is not Artinian, we have prime ideals that are not maximal. In particular we will have generic points, ie those where $\overline{\{pt\}} = \text{Spec}(A)$ (eg $(0) \subseteq A$ if A is an integral domain)

§2 Proof of Theorem 1:

- It is clear that all $m_{\underline{a}}$'s are maximal because $\mathbb{K}[x_1,\dots,x_n]/m_{\underline{a}} \simeq \mathbb{K}$. via

$$\begin{array}{ccccc} \mathbb{K} & \hookrightarrow & \mathbb{K}[x_1,\dots,x_n] & \twoheadrightarrow & \mathbb{K} \\ 1 & \longmapsto & 1 & & \\ & & x_i & \longmapsto & a_i \\ & & k & \longmapsto & k \end{array}$$

- To finish, pick $m \subseteq \mathbb{K}[x_1,\dots,x_n]$ a maximal ideal. We want to find $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$ with $m = m_{\underline{a}}$. Since m is maximal, we get that

(1) $m \cap \mathbb{K} = \{0\}$

(2) the quotient ring $L := \mathbb{K}[x_1,\dots,x_n]/m = \mathbb{K}[\overline{x}_1,\dots,\overline{x}_n]$ is a field

Combining (1) & (2) we see that

$$\begin{array}{ccccc} \mathbb{K} & \hookrightarrow & \mathbb{K}[x_1,\dots,x_n] & \twoheadrightarrow & L \\ 1 & \longmapsto & 1 & & \\ & & x_i & \longmapsto & \overline{x}_i \end{array}$$

induces $\mathbb{K} \xhookrightarrow{\varphi} L$, ie $L|\mathbb{K}$ is a field extension.

Claim: $L|\mathbb{K}$ is an algebraic extension

- Assuming the claim, we can prove the theorem. Indeed, since $L|\mathbb{K}$ is algebraic and $\overline{\mathbb{K}}=\mathbb{K}$, we get $L=\mathbb{K}$, ie φ is surjective.

Choosing $a_1,\dots,a_n\in\mathbb{K}$ with $\varphi(a_j)=\overline{x_j}$ for all $j=1,\dots,n$ we get

$$x_j-a_j\in\mathfrak{m}\quad\forall j=1,\dots,n;$$

ie $\mathfrak{m}_{\underline{a}}\subseteq\mathfrak{m}$. Since $\mathfrak{m}_a$ is maxl & $\mathfrak{m}$ is a proper ideal, we conclude that $\mathfrak{m}_{\underline{a}}=\mathfrak{m}$, as we wanted to show. □

Proof of the Claim: We do this in 3 steps.

STEP 1: Find an intermediate field $\mathbb{K}\subset S\subset L$ where

$$\begin{array}{cl} L & \\ | & \Big\} \text{ finite extension (so, algebraic!)} \\ S & \\ | & \Big\} \text{ purely transcendental} \\ \mathbb{K} & \end{array}$$

and $S=\mathbb{K}(y_1,\dots,y_k)$ for some $y_1,\dots,y_k\in L$ algebraically independent over $\mathbb{K}$

STEP 2: Show S is a finitely generated $\mathbb{K}$-algebra.

STEP 3: Conclude that $k=0$. when $\mathbb{K}$ is infinite (ok if $\overline{\mathbb{K}}=\mathbb{K}$)

- STEP 1 will be addressed by Noether Normalization
- STEP 2 ——————— an auxiliary lemma. (Use that $L|S$ finite)
- Next, we discuss STEP 3:

Pick $z_1,\dots,z_\ell\in S\subseteq L$ be a collection of generators of S as a $\mathbb{K}$-algebra, ie $S=\mathbb{K}[z_1,\dots,z_\ell]$ modulo relations.

The definition of S gives us $z_j=\dfrac{P_j(y_1,\dots,y_k)}{Q_j(y_1,\dots,y_k)}$ for $j=1,\dots,\ell$.

where $P_j,Q_j\in\mathbb{K}[y_1,\dots,y_k]$

- **Claim**: The polynomial ring $\underbrace{\mathbb{K}[y_1,\dots,y_k]}_{\text{UFD}}$ for $k\geq 1$ has finitely many irreducibles.

Pf/ Pick any irreducible polynomial $f \neq 0$ in $\mathbb{K}[y_1,\ldots,y_k] \subseteq S$ field, so $\frac{1}{f} \in S$

- We can find a polynomial $A_{(\underline{z})} \in \mathbb{K}[z_1,\ldots,z_\ell]$ so that $\frac{1}{f} = A(z_1,\ldots,z_\ell)$
- By definition of $z_1,\ldots,z_n$ we get $\frac{1}{f} = \frac{P(y_1,\ldots,y_k)}{Q(y_1,\ldots,y_k)}$ where $Q \mid Q_1^{d_1} \cdots Q_\ell^{d_\ell}$ ($d_i = \deg_{z_i}(A)$ for $i=1,\ldots,\ell$).

In particular $f \mid Q_j$ for some $j = 1,\ldots,\ell$

Conclusion: $f \in \bigcup_{j=1}^{\ell} \{\text{irreducible factors of } Q_j\}$, which is a finite list. ✓

- But $\mathbb{K}$ is infinite & $\{y_1 - \lambda\}_{\lambda \in \mathbb{K}}$ are all irreducibles over $\mathbb{K}[y_1,\ldots,y_k]$

This contradicts the claim which is valid for $k \geq 1$. Thus, $\boxed{k=0}$ □

- Next, we state the auxiliary lemma needed for STEP 2.

For the application, we take $R = \mathbb{K}$, $S = \mathbb{K}(y_1,\ldots,y_k)$ & $A = L = \mathbb{K}[\bar{x}_1,\ldots,\bar{x}_n]$

Lemma 1: Let R be a Noetherian commutative ring & $S \supset R$ any subring of a f.g. R-algebra A. If A is finitely generated as an S-module, then S is a finitely generated R-algebra.

(Recall: B a f.g R-algebra iff $\exists$ $R[z_1,\ldots,z_m] \twoheadrightarrow S$ ring & R-module homomorphism).

Proof: We write $A = \mathbb{K}[\bar{x}_1,\ldots,\bar{x}_n] = \mathbb{K}[x_1,\ldots,x_n]/I$ for some ideal I.

(⚠ The variables $x_1,\ldots,x_n$ have no relation to those in the proof of Theorem 1)

Fix $y_1,\ldots,y_m \in R[\bar{x}_1 \ldots \bar{x}_n]$ generators of this S-module (again, $y_1,\ldots,y_m$ have no relation to those in STEP 1). In particular, we can write

$$\bar{x}_i = \sum_{j=1}^{m} a_{i,j}\, y_j \quad \text{for } a_{i,j} \in S.$$

In addition: $$y_i \cdot y_j = \sum_{k=1}^{m} b_{i,j,k}\, y_k \quad \text{for } b_{i,j,k} \in S$$

Consider the subring $R \subset S_0 \subset S$ generated over R by $\{a_{i,j}, b_{i,j,k}\}_{i,j,k}$

$$\boxed{S_0 := R[a_{i,j}, b_{i,j,k}] \subset S}$$

(the relations among the generators are implicit here)

Summary:

$$\begin{tikzcd} R[\bar{x}_1, \ldots, \bar{x}_n] \arrow[d, dash] \\ S \arrow[d, dash] \\ S_0 \arrow[d, dash] \\ R \end{tikzcd}$$

Noetherian ring by Hilbert basis Thm + quotients of Noeth rings are Noeth.

(2) Noetherian S_0-module

Noetherian ring & f.g R-alg (1)

(1) Since S_0 is a f.g. R-algebra (quotient of a polynomial ring over R), we know S_0 is also a Noetherian ring.

(2) By definition of S_0, $y_1, \ldots, y_m \in R[\bar{x}_1, \ldots, \bar{x}_n]$ generate this ring as an S_0-module.

Consequence: S is an S_0-submodule of the Noetherian S_0-module $R[\bar{x}_1, \ldots, \bar{x}_n]$, so S is f.g as an S_0-submodule.

Claim: S_0 is a f.g R-algebra $\Rightarrow$ S is also a f.g. R-algebra.

Pf/ Write generators of S over S_0 : $\{s_1, \ldots, s_r\}$ & use the fact that S is a ring to conclude:

$$\underset{\text{formal polynomial ring}}{R[a_{i,j}, b_{i,j,k}][s_1, \ldots, s_r]} \twoheadrightarrow S_0[s_1, \ldots, s_r] \twoheadrightarrow \underset{\text{ring}}{S}$$

& map restricted to R is inc: $R \longrightarrow S$. $\square$

- For STEP 1, we need the following statement, whose proof will be given next time.

Theorem 2 (Noether Normalization): Let $\mathbb{K}$ be a field and A a finitely generated $\mathbb{K}$-algebra. Say $A = \mathbb{K}[X_1 \ldots X_n]/I = \mathbb{K}[x_1, \ldots, x_n]$. Assume A is a domain.
Then $\exists\, k = 0, \ldots, n$ & $y_1, \ldots, y_k \in A$ algebraically independent over $\mathbb{K}$

such that A is integral over $\mathbb{K}[y_1,\dots,y_k]$.

(<u>Recall</u>: $r\in A$ is <u>integral over S</u> if $\exists\, f\in S[z]$ monic with $f(r)=0$.)

For the application we observe:

$$\begin{tikzcd}
 & \mathrm{Quot}(A) \arrow[dd, dash, "\text{finite}"] \\
A \arrow[ur, dash] \arrow[dd, dash, "\text{integral}"'] \arrow[r, phantom, "\Longrightarrow"] & \\
 & \mathbb{K}(y_1,\dots,y_r)=\mathrm{Quot}(\mathbb{K}[y_1,\dots,y_r]) \\
\mathbb{K}[y_1,\dots,y_r] \arrow[ur, dash] \arrow[d, dash] & \\
\mathbb{K} \arrow[uur, dash, "\text{purely transcendental because } \{y_1,\dots,y_r\}"'] &
\end{tikzcd}$$