

Lecture VIII: Hilbert Nullstellensatz II

Last time we discussed the following 2 theorems.

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

Weak Hilb. Nullstellensatz: If $\mathbb{K} = \overline{\mathbb{K}}$ & \mathfrak{a} is an ideal of $\mathbb{K}[x_1, \dots, x_n]$ we have
$$V(\mathfrak{a}) = \emptyset \iff \mathfrak{a} = (1) = \mathbb{K}[x_1, \dots, x_n]$$

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 $\mathbb{K}[x_1, \dots, x_n]$ when $\overline{\mathbb{K}} = \mathbb{K}$:

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

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

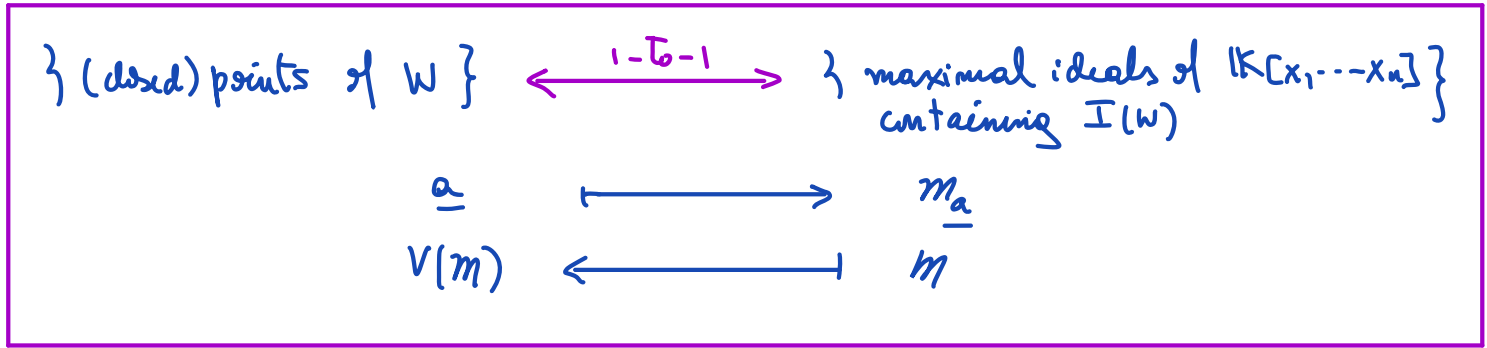
The rest of today will be devoted to proving this statement. But first, we discuss 2 key consequences of this statement.

Corollary 1: Weak Nullstellensatz

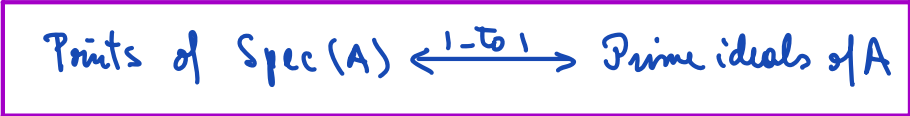
Proof: Since $\mathfrak{a} \subsetneq \mathbb{K}[x_1, \dots, x_n]$ is a proper ideal we can find $\mathfrak{m} \subsetneq \mathbb{K}[x]$ maximal ideal with $\mathfrak{a} \subseteq \mathfrak{m}$. By Theorem 1 we have $\mathfrak{m} = \mathfrak{m}_{\underline{a}}$ for some $\underline{a} \in A_{\mathbb{K}}^n$
($\overline{\mathbb{K}} = \mathbb{K}$)

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. \square

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



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



So if A is not Artinian, we have prime ideals that are not maximal. In particular we will have generic points, i.e. 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 $\underline{m_a}$'s are maximal because $\frac{\mathbb{K}[x_1, \dots, x_n]}{\underline{m_a}} \simeq \mathbb{K}$. via

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

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

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

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

Combining (1) & (2) we see that $\begin{array}{ccccc} \mathbb{K} & \hookrightarrow & \mathbb{K}[x_1, \dots, x_n] & \twoheadrightarrow & L \\ 1 & \mapsto & 1 & & x_i \mapsto \bar{x}_i \end{array}$

induces $\mathbb{K} \xrightarrow{\varphi} L$ i.e. $L|\mathbb{K}$ is a field extension.

Claim: $L|K$ is an algebraic extension

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

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

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

i.e. $\mathfrak{m}_a \subseteq \mathfrak{m}$. Since \mathfrak{m}_a is max & \mathfrak{m} is a proper ideal, we conclude that

$\mathfrak{m}_a = \mathfrak{m}$, as we wanted to show. \square

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

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

$$\begin{array}{l} L \\ | \\ S \\ | \\ K \end{array} \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \begin{array}{l} \text{finite extension (so, algebraic!)} \\ \text{purely transcendental} \end{array}$$

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

STEP 2: Show S is a finitely generated K -algebra.

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

• STEP 1 will be addressed by Noether Normalization

• STEP 2 ————— an auxiliary lemma. (Use that $L|S$ finite)

• Next, we discuss STEP 3:

Pick $z_1, \dots, z_\ell \in S \subset L$ be a collection of generators of S as a K -algebra, i.e. $S = K[z_1, \dots, z_\ell]$ modulo relations.

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

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

Claim: The polynomial ring $K[y_1, \dots, y_k]$ for $k \geq 1$ has finitely many irreducibles.
UFD

- 3f/ Pick any irreducible polynomial $f \neq 0$ in $K[y_1, \dots, y_k] \subseteq S$ field, so $\frac{1}{f} \in S$.
- We can find a polynomial $A_{(\underline{z})} \in K[z_1, \dots, z_\ell]$ so that $\frac{1}{f} = A_{(\underline{z})}$
 - By definition of z_1, \dots, z_ℓ we get $\frac{1}{f} = \frac{P(y_1, \dots, y_k)}{Q(y_1, \dots, y_k)}$ where $Q \mid Q_1^{d_1} \cdots Q_\ell^{d_\ell}$ ($d_i = \deg_{z_i}(A)$ for $i=1, \dots, \ell$).
 - In particular $f \mid Q_j$ for some $j=1, \dots, \ell$

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

• But K is infinite & $\{y_i - \lambda \mid \lambda \in K\}$ are all irreducibles over $K[y_1, \dots, y_k]$

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

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

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

Lemma 1: Let R be a Noetherian commutative ring & $S > R$ 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 $\exists R[z_1, \dots, z_m] \twoheadrightarrow S$ ring & R -module homomorphism).

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

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

Fix $y_1, \dots, y_m \in R[\bar{x}_1, \dots, \bar{x}_n]$ generators of this S -module (again, y_1, \dots, y_m

have no relation to those in STEP 1). In particular, we can write

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

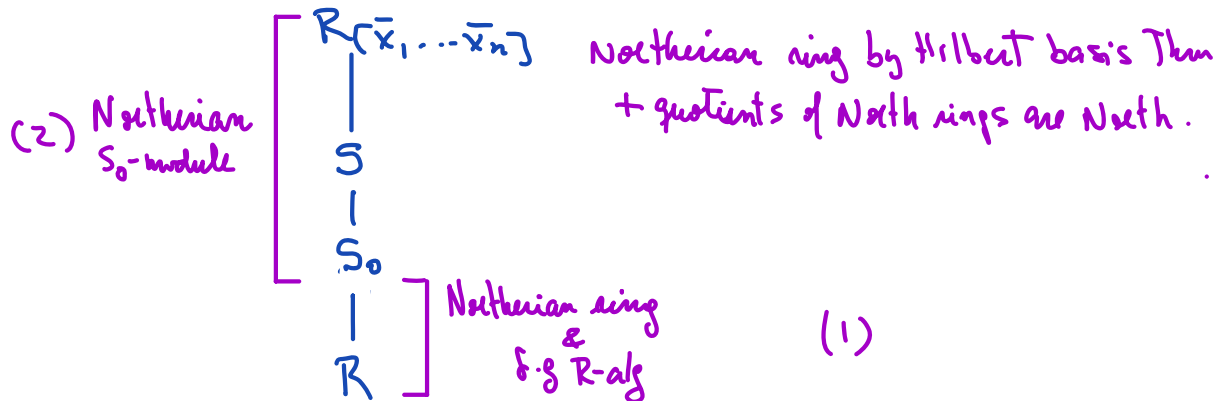
In addition: $y_i \cdot y_j = \sum_{k=1}^m b_{ijk} y_k$ for $b_{ijk} \in S$

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

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

(the relations among the generators are implicit here)

Summary:



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

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

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

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

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

$$\begin{array}{c}
 \mathbb{R}[a_{i,j}, b_{i,j,k}][s_1, \dots, s_r] \longrightarrow S_0[s_1, \dots, s_r] \longrightarrow S \\
 \text{formal polynomial ring} \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \text{ring} \\
 \text{\& map restricted to } \mathbb{R} \text{ is inc: } \mathbb{R} \longrightarrow S. \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \square
 \end{array}$$

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

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

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

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

For the application we observe:

