# The Nullstellensatz

$k$ a field.

$$(*) \quad \left\{ \begin{array}{c} \text{Ideals of} \\ k[X_1, \dots, X_n] \end{array} \right\} \begin{array}{c} I \mapsto V(I) \\ \longrightarrow \\ \longleftarrow \\ I(X) \leftarrow\!\shortmid X \end{array} \left\{ \begin{array}{c} \text{Subsets of} \\ \mathbb{A}^n \end{array} \right\}$$

<u>Theorem</u>: Suppose $k$ is algebraically closed. Then $(*)$ gives inclusion reversing mutually inverse bijections.

$$\{\text{Radical ideals}\} \rightleftarrows \{\text{Zariski closed subsets}\}$$

---

<u>Cor</u>: The maximal ideals of $k[X_1, \dots, X_n]$ are all of the form

$$\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$$

for $(a_1, \dots, a_n) \in \mathbb{A}^n$.

Note $\quad \mathfrak{m} = \ker(\mathrm{eval}_{(a_1, \dots, a_n)})$

$$\mathrm{eval}_{(a_1, \dots, a_n)} : k[X_1, \dots, X_n] \to k$$
$$X_i \mapsto a_i$$

i.e. $\quad f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n)$.

<u>Cor</u>: If $I$ is any ideal such that $V(I) = \phi$, then $I = (1)$.

<u>Cor</u>: If $I$ is any ideal such that $f \equiv 0$ on $V(I)$, then $f^n \in I$ for some $n$.

---

What does the Nullstellensatz "say?"
Think of an ideal $I \subset k[x_1, \dots, x_n]$ as a "system of equations" and $V(I)$ as its set of solutions.

Nullstellensatz: if $k$ is alg closed then a system of equations & its set of solutions are equivalent pieces of data.

<u>Baby example</u>:— $k[x]$

Up to multiplicites (i.e. taking radicals) & scaling a polynomial is determined by its <u>roots</u>.

Now, we will prove the Nullstellensatz.
The crux is the following purely algebraic fact about field extensions.

<u>Theorem</u>: Let $k \subset K$ be a field extension. If $K$ is a finitely generated $k$-algebra, then $K/k$ is algebraic.

<u>Contrapositive</u>: If $K/k$ is not algebraic, then $K$ is NOT a finitely generated $k$ algebra.

<u>Proof</u>: <u>Warmup</u>. – $K = k(x)$ is <u>NOT</u> a finitely generated $k$ algebra.
(Look at denominators).

<u>Warm up</u>: $K = k(x_1, \dots, x_n)$ is <u>NOT</u> a finitely generated $k$-algebra.
(Same proof).

<u>Key fact</u>: $k[x_1, \dots, x_n]$ is a UFD. So every $f \in k(x_1, \dots, x_n)$ has a unique expression as num/den where num, den are in $k[x_1, \dots, x_n]$ & $\gcd(\text{num}, \text{den}) = 1$.

Terminology (Non-standard)
Let $p \in k[X_1, \dots, X_n]$ be irreducible.
Call $f \in k(X_1, \dots, X_n)$ "$p$-integral"
if $p$ does not divide the denominator of $f$.

Observe : $f_1, f_2$ $p$-integral $\Rightarrow f_1 f_2, f_1 + f_2$ also $p$-integral.

Now if $f_1, \dots, f_\ell \in k(X_1, \dots, X_n)$ are finitely many elements, then we can find a $p$ such that all $f_i$ are $p$-integral. (There are infinitely many irred. polynomials!). Then the $k$-algebra generated by $f_1, \dots, f_\ell$ consists of $p$-integral elements. So it cannot contain $1/p$, i.e. it cannot be all of $k(X_1, \dots, X_n)$. So $k(X_1, \dots, X_n)$ is not finitely generated as a $k$-algebra.

Full proof :– Assume $K$ is a finitely generated field over $k$. (Otherwise it's clearly not fin gen as $k$ alg.) Then we have

$$k \subset L \subset K$$

$L = k(x_1, \dots, x_n)$ & $K/L$ is finite.

In particular $K$ is a fin dim $L$-vector space. Fix an isomorphism

$$K = L \oplus L \oplus \cdots \oplus L \quad (r \text{ times})$$

Let $e_i \in K$ the image of $(0,\ldots,0,1,0,\ldots,0)$ (1 in $i^{th}$ place.) Then every $g \in K$ is

$$g = g_1 e_1 + \cdots + g_r e_r$$

where $g_i \in L$.

Call $g$ $p$-integral if $p$ does not divide the denominator of $g_i$ for any $i$.

Observe: $g_1, g_2$ $p$-integral $\Rightarrow$ $g_1+g_2$ also.
For $g_1 g_2$, we need some more.
Suppose

$$e_i e_j = \sum_l m_{ij}^l e_l \; ; \quad m_{ij}^l \in L$$

and suppose $p$ does not divide the denom. of any of the $m_{ij}^k$.

Then $g_1, g_2$ $p$-integral $\Rightarrow$ $g_1 g_2$ also.

Now, the same proof goes. Finitely many $g_1, \ldots, g_l$ cannot generate $K$. Just pick a $p$ so that $g_1, \ldots, g_l$ are $p$-integral & $p \nmid$ denom of $m_{ij}^l$ $\forall i, j, l$.

Then the sub-algebra generated by $g_1, \dots, g_e$ only contains $p$-integral elts. But $K$ clearly has more.

$\square$

From now on: $k$ alg. closed.

<u>Thm</u>: Let $m \subset k[x_1, \dots, x_n]$ max. ideal. Then $m = (x_1 - a_1, \dots, x_n - a_n)$ for some $(a_1, \dots, a_n)$.

<u>Pf</u>: Consider $K = k[x_1, \dots, x_n]/m$. Then $K$ is a fin.gen. $k$-algebra <u>and</u> a field, so $K/k$ is algebraic. But $k$ is alg closed. So $K = k$.

Consider the composite

$$e : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]/m = k$$

Suppose $e : x_i \mapsto a_i \in k$.

Then $e : f(x_1, \dots, x_n) \mapsto f(a_1, \dots, a_n)$

so $e = \text{eval}(a_1, \dots, a_n)$.

Therefore

$$m = \ker(e) = (x_1 - a_1, \dots, x_n - a_n).$$

$\square$

Thm: If $I \neq (1)$, then $V(I) \neq \emptyset$.
In fact, there is a bijection.

$$\mu : V(I) \xrightarrow{\sim} \text{Max. ideals of } k[x_1, \ldots, x_n] \text{ containing } I.$$

given by

$$(a_1, \ldots, a_n) \mapsto (x_1 - a_1, \ldots, x_n - a_n).$$

Pf: First, if $(a_1, \ldots, a_n) \in V(I)$
then $I \subset \operatorname{Ker}(\operatorname{eval}(a_1, \ldots, a_n))$
$= (x_1 - a_1, \ldots, x_n - a_n)$
so $(x_1 - a_1, \ldots, x_n - a_n)$ is a max. id. containing $I$.

Clearly $\mu$ is injective.
To show surjectivity, let $m$ be a max. ideal containing $I$. Then
$m = \operatorname{Ker} \operatorname{eval}(a_1, \ldots, a_n)$. for some $(a_1, \ldots, a_n) \in \mathbb{A}^n$ by the previous thm.
But $I \subset m \Rightarrow (a_1, \ldots, a_n) \in V(I)$

$\square$.

Thm: If $f \equiv 0$ on $V(I)$, then $f \in \sqrt{I}$. (i.e. $f^N \in I$ for some $N$).

Pf: Consider $J \subset k[x_1, \dots, x_n, y]$

$J = I + (yf - 1)$. —— $\circledast$

Then $V(J) \subset \mathbb{A}^{n+1}$ is empty.

so $J = (1)$

Then

$\circledast \quad 1 = p_1 f_1 + \cdots + p_m f_m + q(yf - 1)$

for some $f_i \in I$ and $p_i, q \in k[x_1, \dots, x_n, y]$.

Consider the map

$\ell : k[x_1, \dots, x_n, y] \longrightarrow k(x_1, \dots, x_n)$ that sends

$x_i \mapsto x_i$ & $y \mapsto 1/f$.

Apply $\ell$ to $\circledast$.

$$1 = p_1(x_1, \dots, x_n, \tfrac{1}{f}) f_1 + \cdots + p_m(x_1, \dots, x_n, \tfrac{1}{f}) f_m$$

Now clear denominators by multiplying throughout by $f^N$: & see that

$$f^N \in I.$$

$\square$.

<u>Remark</u>: Reconsider the system of equations –

$$J = I + (yf - 1).$$

<u>Note</u>: $(x_1, \dots, x_n, y) \in V(J)$

$\Rightarrow$ $(x_1, \dots, x_n) \in V(I)$ and $f(x_1, \dots, x_n) \neq 0$

Conversely if $(x_1, \dots, x_n) \in V(I)$ & $f(x_1, \dots, x_n) \neq 0$ then there is a unique $y$ such that $(x_1, \dots, x_n, y) \in V(J)$.

That is, we have a bijection

$$V(J) \cong \underbrace{V(I) \cap \{f \neq 0\}}_{\text{open subset of } V(I)}.$$

**Thm:** $I(V(I)) = \sqrt{I}$.

**Pf:** $\sqrt{I} \subset I(V(I))$ is clear.

The other inclusion is the previous theorem.

---

**Proof of Null Stellensatz**

$$\{\text{Rad. ideal}\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{Zar closed}\}$$

Let us check $V$ & $I$ are inverses.

Take a radical ideal $J$. Then

$$I(V(J)) = \sqrt{J} = J.$$

So $I \circ V = \mathrm{id}$.

Now take a Zariski closed set $X$.

Then $X = V(J)$ for some ideal $J$.

Note: $V(J) = V(\sqrt{J})$, so we may take $J$ to be radical. Then

$$V(I(X)) = V(I(V(J))) = V(J) = X.$$

So $V \circ I = \mathrm{id}$. $\square$

Rem: In this course, we will mostly take our base field $k$ to be algebraically closed. The Nullstellensatz will play a key role.

But often, it is desirable to allow arbitrary $k$. In that case, given $I \subset k[x_1, \dots, x_n]$ it is better to take $V(I)$ to be in $\mathbb{A}^n_{\bar{k}}$ rather than $\mathbb{A}^n_k$. Thanks to the Nullstellensatz the vanishing set of $I$ in $\mathbb{A}^n_{\bar{k}}$ captures $I$ completely (up to radicals!). In contrast, the vanishing set of $I$ in $\mathbb{A}^n_k$ may not.

Going further, it is often more convenient to have a tighter connection between ideals & zero sets — one that works on the nose for all ideals rather than just radical ideals. To do so, one takes the vanishing set $V(I)$ to be in $\mathbb{A}^n_R$ where $R$ is a <u>variable</u> $k$-algebra. That is, one lets $V(I)$ to be the functor

$$k\text{-alg.} \to \text{Sets}$$

$$R \mapsto V(I,R) \subset \mathbb{A}^n_R = R^n.$$

$$\{(a_1, \dots, a_n) \in R^n \mid f(a_1, \dots, a_n) = 0 \ \forall f \in I\}$$

This leads to the notion of a scheme.
But if $I$ is radical, and $k$ is alg. closed then the functor contains no more info than the set
$V(I) \subset \mathbb{A}^n_k$. (Thanks Nullstellensatz)

---

## Regular Functions

For the moment, our objects of study are affine algebraic sets. Our next goal is to define a good notion of morphisms. We first treat the special case of morphisms to $\mathbb{A}^1$.

Let $X \subset \mathbb{A}^n$ be an affine alg. set. A function $f : X \to \mathbb{A}^1 = k$ is called <u>regular</u> if there exists a polynomial $F \in k[x_1, \dots, x_n]$ such that
$$F(p) = f(p) \quad \forall \; p \in X.$$

<u>Note</u>: $F$ need not be unique.

Let $R$ be the set of regular functions on $X$. Then $R$ contains a copy of $k$ as the constant functions. That is $R$ is a $k$ algebra.

We have a map

$$k[x_1, \dots, x_n] \to R$$
$$F \longmapsto (p \mapsto F(p)).$$

This map is surjective by the def. of $R$. The Kernel of this map is $I(X)$. So by the first iso. thm. we have

$$R \cong k[x_1, \dots, x_n] / I(X).$$

Now let $k$ be algebraically closed. Thanks to the Nullstellensatz, we have the following "algebra-geometry" dictionary.

- Elt of $R$ = Reg. function on $X$
- max ideal of $R$ = Point of $X$
- $\{$max ideals containing a given ideal $J\}$ = Zariski closed subset of $X$.

What kind of ring is $R$?

$R$ is a finitely generated, reduced (nilpotent-free) $k$-algebra.

Conversely, any finitely generated reduced $k$-algebra $R$ is the algebra of regular functions on some affine algebraic set $X$.

How? Write $R = k[x_1, \ldots, x_n] / I$.

Then $I$ is a radical ideal.

Take $X = V(I)$.