Algebraic sets + the Nullstellensatz

While it is possible to state + prove the Nullstellensatz purely algebraically, it is important to give some geometric context, so we first briefly introduce some classical AG concepts:

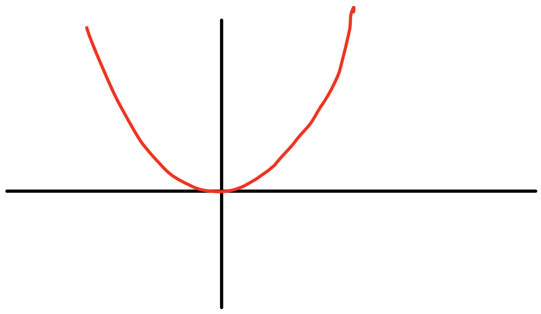
Let k be a field.

Def: If $S \subseteq k[x_1, \dots, x_m] = R$, then

$$Z(S) := \{ (a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \ \forall \ f \in S \}$$

This is called an <u>algebraic set</u> in k^n (which in this context can be written $\mathbb{A}^n$).

Ex: ① If $S = \{x^2 - y\} \subseteq \mathbb{R}[x,y]$,

$Z(S) =$ 

② If $S = \{x^2 + 1\} \subseteq \mathbb{R}[x]$, then $Z(S) = \emptyset$

③ If $S = \{x^2 + 1\} \subseteq \mathbb{C}[x]$, then $Z(S) = \{i, -i\}$

Check: ① $Z(f_1, \dots, f_m) = Z(I) = Z(\sqrt{I})$, where $I = (f_1, \dots, f_m)$

② If $S \subseteq S' \subseteq k[x_1, \dots, x_n]$, then $Z(S') \subseteq Z(S)$.

Def: If $X \subseteq k^n$, $I(X) = \{ f \in k[x_1, \dots, x_n] \mid f(p) = 0 \ \forall \ p \in X \}$.

Def: An ideal $I \subseteq R$ is <u>radical</u> if $\sqrt{I} = I$.

Check: $I(X)$ is a (radical) ideal, and $Z(I(Z(J))) = Z(J)$, for any ideal $J \subseteq k[x_1, \dots, x_n]$.

Notice that if $(a_1, \dots, a_n) \in k^n$, $R = k[x_1, \dots, x_n]$, then the map

$$\begin{aligned} R &\longrightarrow R \\ x_i &\longmapsto x_i - a_i \end{aligned}$$

is an isomorphism, and thus induces an isomorphism

$$R/(x_1, \dots, x_n) \xrightarrow{\cong} R/(x_1 - a_1, \dots, x_n - a_n).$$

The evaluation map $\begin{aligned} R &\to k \\ f &\mapsto f(0, \dots, 0) \end{aligned}$ is a surjection w/ kernel $(x_1, \dots, x_n)$,

so $(x_1 - a_1, \dots, x_n - a_n)$ is always a max'l ideal.

That is, there's an injection $\mathbb{A}^n \to \operatorname{Spec}(R)$, with image contained in the set of max'l ideals.

In fact, if $X = Z(I) \subseteq \mathbb{A}^n$, then $(a_1, \dots, a_n) \in X \iff f(a_1, \dots, a_n) = 0 \ \forall \ f \in I$

$\iff (x_1 - a_1, \dots, x_n - a_n) \in V(I)$.

i.e. the algebraic sets of $\mathbb{A}^n$ are the closed sets of Spec(R) intersected w/ the image of $\mathbb{A}^n$; and in this way $\mathbb{A}^n$ inherits the Zariski topology.

In fact, if $k = \bar{k}$, and $X \subseteq \mathbb{A}^n$ an algebraic set, we'll see (by the Nullstellensatz) that there is a one-to-one correspondence between points of X and closed points (i.e. max'l ideals) in $\mathrm{Spec}(R/I(X))$.

Note: If $k \neq \bar{k}$, we can have more max'l ideals in Spec(R). For instance, $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, so (x^2+1) is maximal!

How are I and Z related?

Lemma: Let $R = k[x_1, \dots, x_n]$, $J \subseteq R$ an ideal, and $X = Z(J)$.

a.) $\sqrt{J} \subseteq I(X)$, and

b.) $X = Z(I(X))$.

Pf: a.) If $f \in \sqrt{J}$ then $f^n \in J$, some n. For $P \in Z(J)$,
$f^n(P) = 0 \Rightarrow f(P) = 0 \Rightarrow f \in I(Z(J))$.

b.) Let $P \in X$. Then if $f \in I(X)$, $f(P) = 0$, so $\subseteq$ holds.

On the other hand, by a.),

$$Z(I(X)) \subseteq Z(\sqrt{J}) = X. \quad \square$$

To summarize, here are the relationships we know so far between ideals and algebraic sets:

We have a map $Z: \{\text{ideals in } k[x_1, \dots, x_n]\} \to \{\text{alg. sets in } \mathbb{A}^n_k\}$

- Z is surjective (by def)
- If X is algebraic, $Z(I(X)) = X$, so I is a <u>right</u> inverse.
- $Z(x^2) = Z(x)$, so it's not injective.
- However, $Z(I) = Z(\sqrt{I})$.

If we restrict our attention to radical ideals, is Z a bijection?

<u>No</u>: Let $R = \mathbb{R}[x,y]$. Then x^2+y^2 is irreducible, thus (x^2+y^2) and (x,y) are both prime and thus radical. However, the zero set of each is $(0,0)$.

The Nullstellensatz says that if k is algebraically closed, we do get a bijection:

<u>Hilbert's Nullstellensatz</u>: Let k be algebraically closed and $I \subseteq k[x_1, \dots, x_n]$ an ideal. Then $I(Z(I)) = \sqrt{I}$.

(Thus I is a left inverse when Z is restricted to radical ideals)

In order to prove this, we first need the following.

Weak Nullstellensatz: If k is algebraically closed and $I \subsetneq k[x_1, \dots, x_n]$ a proper ideal, then $Z(I) \neq \emptyset$.

Pf: Find a maximal ideal $m \supset I$. Then $Z(m) \subseteq Z(I)$.

> **Claim:** Any maximal ideal $m \subseteq k[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$, $a_i \in k$.
> (we'll prove this later, after more theory.)

So $Z(m) = \{(a_1, \dots, a_n)\}$. In particular, $Z(I) \neq \emptyset$. $\square$

Proof of Nullstellensatz: We know $\sqrt{I} \subseteq I(Z(I))$.

Let $I = (f_1, \dots, f_r)$. Suppose $g \in I(Z(I))$.

Let $R = k[x_1, \dots, x_n]$ and $S = k[x_1, \dots, x_{n+1}]$.

Define $J = (f_1, \dots, f_r, x_{n+1} g - 1) \subseteq S$.

What is $Z(J) \subseteq \mathbb{A}^{n+1}$? If $P \in Z(J)$ then $f_i(P) = 0 \ \forall \ i$, so $g(P) = 0$.

Thus, $x_{n+1}g-1$ evaluated at P is not 0. $\Rightarrow Z(J)=\emptyset$.

The weak Nullstellensatz implies that $J=S$, so $1\in J$.

$$\Rightarrow \sum a_i f_i + b(x_{n+1}g-1) = 1 \quad \text{for some} \quad a_1,\dots,a_r,b\in S.$$

Let N be the highest power of x_{n+1} appearing in the equation, and set $y=\frac{1}{x_{n+1}}$

Multiplying both sides of the equation by y^N and cancelling all the x_{n+1}'s yields

$$\sum \tilde{a}_i f_i + \tilde{b}(g-y) = y^N, \quad \text{where } \tilde{a}_1,\dots,\tilde{a}_r,\tilde{b}\in k[x_1,\dots,x_n,y].$$

Substituting $\underbrace{g \text{ for } y}_{\text{do you see why we're allowed to do this?}}$, we get $g^N = F+0$ where $F\in I$,

so $g\in\sqrt{I}$. □

This thus implies that for $k=\bar{k}$, there is a one-to-one correspondence

$$\left\{\begin{array}{c}\text{radical ideals}\\ I\subseteq k[x_1,\dots,x_n]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{algebraic sets}\\ X\subseteq \mathbb{A}^n\end{array}\right\}$$

$$I \longmapsto Z(I)$$

$$I(X) \longleftarrow X$$