

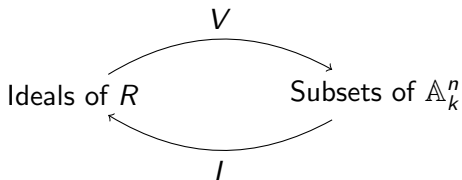
# MAS439 Lecture 12

## Nullstellensatz

November 16th

## Where were we?

We had maps  $V$  and  $I$  that related the geometry of affine space and ideals of  $R = k[x_1, \dots, x_n]$ :



Today, we're going to see how close to inverse we can make  $V$  and  $I$ .

We can't get every subset of  $\mathbb{A}_k^n$

Recall that we called a subset  $X \subset \mathbb{A}_k^n$  *algebraic* if  $X = V(J)$  for some ideal  $J$ . That is, algebraic subsets are exactly those in the image of  $V$ .

Since every ideal  $J \subset k[x_1, \dots, x_n]$  is finitely generated, algebraic subsets were exactly those subsets that were cut out by setting a finite number of polynomials equal to 0.

## We can't get every ideal, either

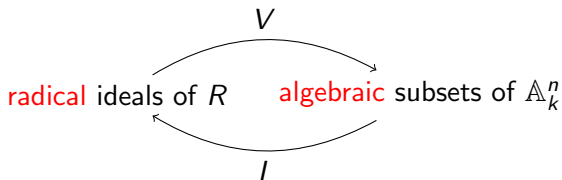
Let  $X$  be a subset of  $I$ , and consider the ideal

$$I(X) = \{f \in R : f(x) = 0 \forall x \in X\}$$

We note that  $I(X)$  is a radical ideal, since

$$\begin{aligned} f^n \in I(X) &\iff f(x)^n = 0 \forall x \in X \\ &\iff f(x) = 0 \forall x \in X \\ &\iff f \in I(X) \end{aligned}$$

The best we could hope for



Now it seems we have a chance...

## We still haven't done enough:

Consider the following two ideals of  $\mathbb{R}[x]$ :  $I = (x^2 + 1)$  and  $J = \mathbb{R}[x]$  itself.

We have  $V(I) = \emptyset = V(J)$ .

Hence,  $V$  is not injective, and can't have an inverse.

## Another failure:

Now, let  $k = \mathbb{F}_p$ , and consider the polynomial  $x^p - x$ .

Fermat's little theorem tells us that we always have  $a^p \cong a \pmod{p}$ , and hence we see that  $x^p - x$  vanishes at every point of  $\mathbb{A}_k^1$ . Thus, we have shown:

$$V(x^p - x) = \mathbb{A}_k^1 = V(0)$$

Again,  $V$  is not injective.

# Fixing the problem

Both problems can be dealt with at the same time if we consider a special class of fields  $k$ .

## Definition

A field  $k$  is *algebraically closed* if every non-constant polynomial  $f \in k[x]$  has a root in  $k$ .

Once we have one root, we can use polynomial division and induction to show that if  $k$  is an algebraically closed field then every polynomial  $f \in k[x]$  can be written (uniquely, up to reordering) in the form

$$f(x) = c \cdot (x - a_1) \cdots (x - a_n)$$

for  $c, a_i \in k$ .



# Examples of fields, algebraically closed and not

- ▶  $\mathbb{Q}$  and  $\mathbb{R}$  are **not** algebraically closed:  $x^2 + 1$  has no roots in either.
- ▶  $\mathbb{C}$  is algebraically closed. This is the fundamental theorem of algebra.
- ▶ A finite field  $k$  is never algebraically closed: the polynomial

$$f(x) = 1 + \prod_{a \in k} (x - a)$$

is not a constant, but has no roots, because  $f(a) = 1$  for all  $a \in k$ .

# A big word for a big theorem

## Theorem (Hillbert's *Nullstellensatz*)

Let  $k$  be an algebraically closed field, and  $I \subset k[x_1, \dots, x_n]$  an ideal. Then

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

You will prove the Nullstellensatz next semester?

## A german lesson

- ▶ Null=nothing (zero)
- ▶ Stellen=placement, location (locus)
- ▶ satz=statement (Theorem)

so “Nullstellensatz” = “zero locus theorem”

# Nullstellensatz is what we needed

## Theorem

*Let  $k$  be algebraically closed. Then the two maps  $I$  and  $V$  are inverse bijections between radical ideals of  $R$  and algebraic subsets of  $\mathbb{A}_k^n$ .*

## Proof.

If  $J$  is a radical ideal, then the Nullstellensatz says that  $I(V(J)) = J$ .

Now, suppose  $X \subset \mathbb{A}_k^n$  is algebraic; hence by definition  $X = V(J)$  for some ideal  $J$ , which we can take to be radical. But then

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



## An example:

Recall your homework question, where you considered the ideal  $J = (x^2 + y^2 - 2, xy - 1)$ .

Geometrically, this consists of the points  $(1, 1)$  and  $(-1, -1)$ .

However, we saw that  $(x - y)$  vanishes at both of these points, but isn't in  $J$ ; i.e., we have  $I(V(J)) \neq J$ . We did see that  $(x - y)^2 \in J$ , consistent with  $I(V(J)) = \sqrt{J}$ .

The algebraic fact that  $J$  isn't radical turns out to have something to do with the fact that  $V(x^2 + y^2 - 2)$  and  $V(xy - 1)$  don't intersect nicely...

## Restricting our bijection

Radical ideals were in bijection with algebraic subsets. Every maximal ideal is radical – what can we say about the algebraic subsets they correspond to?

Since  $V$  and  $I$  are order reversing, we see that if  $\mathfrak{m}$  is a maximal ideal, then  $V(\mathfrak{m})$  must be a minimal algebraic subset.

But any point  $(a_1, \dots, a_n) \in \mathbb{A}_k^n$  is algebraic, as it is  $V(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ . Hence, the minimal algebraic subsets are points, and we have:

