

# Title

D. Zack Garza

Tuesday 25<sup>th</sup> August, 2020

## Contents

<b>1 Tuesday, August 25</b>	<b>1</b>
1.1 Proof of Nullstellensatz . . . . .	3

## 1 Tuesday, August 25

Let  $k = \bar{k}$  and  $R$  a ring containing ideals  $I, J$ .

**Definition 1.0.1** (Radical).

Recall that the *radical* of  $I$  is defined as

$$\sqrt{I} = \left\{ r \in R \mid r^k \in I \text{ for some } k \in \mathbb{N} \right\}.$$

**Example 1.1.**

Let  $I = (x_1, x_2^2) \subset \mathbb{C}[x_1, x_2]$ , so  $I = \{ f_1 x_1 + f_2 x_2 \mid f_1, f_2 \in \mathbb{C}[x_1, x_2] \}$ . Then  $\sqrt{I} = (x_1, x_2)$ , since  $x_2^2 \in I \implies x_2 \in \sqrt{I}$ .

Given  $f \in k[x_1, \dots, x_n]$ , take its value at  $a = (a_1, \dots, a_n)$  and denote it  $f(a)$ . Set  $\deg(f)$  to be the largest value of  $i_1 + \dots + i_n$  such that the coefficient of  $\prod x_j^{i_j}$  is nonzero.

**Example 1.2.**

$$\deg(x_1 + x_2^2 + x_1 x_2^3) = 4$$

**Definition 1.0.2** (Affine Variety).

1. Affine  $n$ -space  $\mathbb{A}^n = \mathbb{A}_k^n$  is defined as  $\{ (a_1, \dots, a_n) \mid a_i \in k \}$ .

Remark: not  $k^n$ , since we won't necessarily use the vector space structure (e.g. adding points).

2. Let  $S \subset k[x_1, \dots, x_n]$  to be a set of polynomials. Then define  $V(S) = \{ x \in \mathbb{A}^n \mid f(x) = 0 \} \subset \mathbb{A}^n$  to be an *affine variety*.

---

**Example 1.3.**

- $\mathbb{A}^n = V(0)$ .
- For any point  $(a_1, \dots, a_n) \in \mathbb{A}^n$ , then  $V(x_1 - a_1, \dots, x_n - a_n) = \{a_1, \dots, a_n\}$  uniquely determines the point.
- For any finite set  $r_1, \dots, r_k \in \mathbb{A}^1$ , there exists a polynomial  $f(x)$  whose roots are  $r_i$ .

**Remark 1.**

We may as well assume  $S$  is an ideal by taking the ideal it generates,  $S \subseteq \langle S \rangle = \left\{ \sum g_i f_i \mid g_i \in k[x_1, \dots, x_n], f_i \in S \right\}$ . Then  $V(\langle S \rangle) \subset V(S)$ .

Conversely, if  $f_1, f_2$  vanish at  $x \in \mathbb{A}^n$ , then  $f_1 + f_2, gf_1$  also vanish at  $x$  for all  $g \in k[x_1, \dots, x_n]$ . Thus  $V(S) \subset V(\langle S \rangle)$ .

**Lemma 1.1.**

1. If  $S_1 \subseteq S_2$  then  $V(S_1) \supseteq V(S_2)$ .
2.  $V(S_1 \cup S_2) = V(S_1 S_2) = V(S_1) \cap V(S_2)$ .

We thus have a map

$$V : \{\text{Ideals in } k[x_1, \dots, x_n]\} \longrightarrow \{\text{Affine varieties in } \mathbb{A}^n\}.$$

**Definition 1.1.1** (The Ideal of a Set).

Let  $X \subset \mathbb{A}^n$  be any set, then *the ideal of  $X$*  is defined as

$$I(X) := \left\{ f \in k[x_1, \dots, x_n] \mid f(x) = 0 \forall x \in X \right\}.$$

**Example 1.4.**

Let  $X$  be the union of the  $x_1$  and  $x_2$  axes in  $\mathbb{A}^2$ , then  $I(X) = (x_1 x_2) = \{x_1 x_2 g \mid g \in k[x_1, x_2]\}$ .

Note that if  $X_1 \subset X_2$  then  $I(X_1) \supset I(X_2)$ .

**Proposition 1.2** (*The Image of  $V$  is Radical*).

$I(X)$  is a radical ideal, i.e.  $I(X) = \sqrt{I(X)}$ .

This is because  $f(x)^k = 0 \forall x \in X$  implies  $f(x) = 0$  for all  $x \in X$ , so  $f^k \in I(X)$  and thus  $f \in I(X)$ .

Our correspondence is thus

$$\begin{aligned} \{\text{Ideals in } k[x_1, \dots, x_n]\} &\xrightarrow{V} \{\text{Affine Varieties}\} \\ \{\text{Radical Ideals}\} &\xleftarrow{I} \{?\}. \end{aligned}$$

**Proposition 1.3 (Hilbert Nullstellensatz (Zero Locus Theorem)).**

- a. For any affine variety  $X$ ,  $V(I(X)) = X$ .
- b. For any ideal  $J \subset k[x_1, \dots, x_n]$ ,  $I(V(J)) = \sqrt{J}$ .

Thus there is a bijection between radical ideals and affine varieties.

**1.1 Proof of Nullstellensatz****Remark 2.**

Recall the Hilbert Basis Theorem: any ideal in a finitely generated polynomial ring over a field is again finitely generated.

We need to show 4 inclusions, 3 of which are easy.

a:  $X \subset V(I(X))$ :

- If  $x \in X$  then  $f(x) = 0$  for all  $f \in I(X)$ .
- So  $x \in V(I(X))$ , since every  $f \in I(X)$  vanishes at  $x$ .

b:  $\sqrt{J} \subset I(V(J))$ :

- If  $f \in \sqrt{J}$  then  $f^k \in J$  for some  $k$ .
- Then  $f^k(x) = 0$  for all  $x \in V(J)$ .
- So  $f(x) = 0$  for all  $x \in V(J)$ .
- Thus  $f \in I(V(J))$ .

c:  $V(I(X)) \subset X$ :

- Need to now use that  $X$  is an affine variety.
  - Counterexample:  $X = \mathbb{Z}^2 \subset \mathbb{C}^2$ , then  $I(X) = 0$ . But  $V(I(X)) = \mathbb{C}^2$ , but  $\mathbb{C}^2 \not\subset \mathbb{Z}^2$ .
- By (b),  $I(V(J)) \supset \sqrt{J} \supset J$ .
- Since  $V(\cdot)$  is order-reversing, taking  $V$  of both sides reverses the containment.
- So  $V(I(V(J))) \subset V(J)$ , i.e.  $V(I(X)) \subset X$ .

d:  $I(V(J)) \subset \sqrt{J}$  (hard direction)

**Theorem 1.4 (1st Version of Nullstellensatz).**

Suppose  $k$  is algebraically closed and uncountable (still true in countable case by a different proof).

Then the maximal ideals in  $k[x_1, \dots, x_n]$  are of the form  $(x_1 - a_1, \dots, x_n - a_n)$ .

*Proof.*

Let  $\mathfrak{m}$  be a maximal ideal, then by the Hilbert Basis Theorem,  $\mathfrak{m} = \langle f_1, \dots, f_r \rangle$  is finitely generated.

Let  $L = \mathbb{Q}[\{c\}_i]$  where the  $c_i$  are all of the coefficients of the  $f_i$  if  $\text{char}(K) = 0$ , or  $\mathbb{F}_p[\{c\}_i]$  if  $\text{char}(k) = p$ . Then  $L \subset k$ .

Define  $\mathfrak{m}_0 = \mathfrak{m} \cap L[x_1, \dots, x_n]$ . Note that by construction,  $f_i \in \mathfrak{m}_0$  for all  $i$ , and we can write  $\mathfrak{m} = \mathfrak{m}_0 \cdot k[x_1, \dots, x_n]$ .

**Claim:**  $\mathfrak{m}_0$  is a maximal ideal.

If it were the case that

$$\mathfrak{m}_0 \subsetneq \mathfrak{m}'_0 \subsetneq L[x_1, \dots, x_n],$$

then

$$\mathfrak{m}_0 \cdot k[x_1, \dots, x_n] \subsetneq \mathfrak{m}'_0 \cdot k[x_1, \dots, x_n] \subsetneq k[x_1, \dots, x_n].$$

So far: constructed a smaller polynomial ring and a maximal ideal in it.

Thus  $L[x_1, \dots, x_n]/\mathfrak{m}_0$  is a field that is finitely generated over either  $\mathbb{Q}$  or  $\mathbb{F}_p$ .

**Theorem 1.5 (Noether Normalization).**

Any finitely-generated field extension  $k_1 \hookrightarrow k_2$  is a finite extension of a purely transcendental extension, i.e. there exist  $t_1, \dots, t_\ell$  such that  $k_2$  is finite over  $k_1(t_1, \dots, t_\ell)$ .

Thus  $L[x_1, \dots, x_n]/\mathfrak{m}_0$  is finite over some  $\mathbb{Q}(t_1, \dots, t_n)$ , and since  $k$  is uncountable, there exists an embedding  $\mathbb{Q}(t_1, \dots, t_n) \hookrightarrow k$ .

Use the fact that there are only countably many polynomials over a countable field.

This extends to an embedding of  $\varphi : L[x_1, \dots, x_n]/\mathfrak{m}_0 \hookrightarrow k$  since  $k$  is algebraically closed. Letting  $a_i$  be the image of  $x_i$  under  $\varphi$

■