1 Introduction.

The purpose of this talk is to provide a fairly simple proof of Hilbert’s nullstellensatz. Nullstellensatz is a German word, roughly translating to ”zero locus theorem.” As such, the nullstellensatz ensures a correspondence between special subsets of our geometric space, $k^n$, and structured subsets of our algebraic structure $k[X_1, \ldots, X_n]$. More specifically, we can establish a correspondence between affine algebraic subsets $V$ of $k^n$ and certain ideals $I$ of $k[X_1, \ldots, X_n]$. The upshot is that this lays the groundwork for the further development of modern algebraic geometry.

2 Preliminary Algebro-Geometric Themes.

We are interested in studying affine algebraic sets. That is, subsets of $k^n$ (affine space) that are the vanishing set of some collection of polynomials in $k[X_1, \ldots, X_n]$.

Definition. Given a subset $S \subset k[X_1, \ldots, X_n]$, we define the affine algebraic set defined by $S$ to be the vanishing set of $S$:

$$V(S) := \{x \in k^n : f(x) = 0 \text{ for all } f \in S\}.$$ 

Next, we define a rather dual notion: namely the ideal of a subset $V \subset k^n$. Intuitively, this is just an algebraically structured subset of $k[X_1, \ldots, X_n]$ so that any element of this subset vanishes on $V$. Do note that this does not imply that $V$ is an affine algebraic set. It is simply contained in the vanishing set of this ideal.

Definition. Given a subset $V \subset k^n$, we define the ideal of $V$ by

$$I(V) = \{f \in k[X_1, \ldots, X_n] : f(x) = 0 \text{ for all } x \in V\}.$$ 

Now, we have these correspondences:

$$\text{Algebra} \xrightarrow{V} \text{Geometry}$$

$$\text{Algebra} \xleftarrow{I} \text{Geometry}.$$ 

We might ask how they interact with each other. For instance, how does $V(I(V))$ relate to $V$? How does $I(V(I))$ relate to $I$? It turns out that in $V(I(V)) = V$, so that $V$ is basically a left-inverse for the operator $I$. 
**Proposition.** Given an algebraic subset \( V \subset \mathbb{k}^n \), we have that \( V(I(V)) = V \). (Note that there is an abuse of notation in the sense that the outer \( V \) is thought of as an operator of sorts.)

**Proof.** Observe that given \( A, B \subset \mathbb{k}^n \), we have that \( A \subset B \) implies that \( I(A) \supset I(B) \). This is quite intuitive, actually. The larger we demand our set to be, the harder it is to make a collection of polynomials vanish on all of it.

By definition, \( V \subset V(I(V)) \): If \( x \in V \), then we know that any \( f \in I(V) \) satisfies \( f(x) = 0 \), so that \( x \in V(I(V)) \).

Now, we want to show that \( V \supset V(I(V)) \). Observe that \( V \), being affine algebraic, is of the form \( V = V(J) \), for some ideal \( J \subset \mathbb{k}[X_1, \ldots, X_n] \). Then, we have that \( J \subset I(V) \), since any \( f \in J \) vanishes on \( V \). Therefore, \( V = V(J) \supset V(I(V)) \).

It isn’t too hard to see that \( I \subset I(V(I)) \). If \( f \in I \), then given \( x \in V(I) \), we know that \( f(x) = 0 \). So, \( f \in I(V(I)) \). One might ask: is it true that \( I \supset I(V(I)) \)? The answer, unfortunately, is that this is false in general. We start running into some serious problems when we work over a field \( \mathbb{k} \) which is not algebraically closed.

**Example.** Take \( \mathbb{k} = \mathbb{R} \). Consider the polynomial \( f(X, Y) = X^2 + Y^2 + 1 \in \mathbb{R}[X, Y] \). It’s not hard to see that this polynomial has no solutions in \( \mathbb{R}^2 \). So, \( V(f) = \emptyset \). On the other hand, \( I(V(f)) = \mathbb{k}[X_1, \ldots, X_n] \neq (f) \).

So, it seems like the chief obstruction to the realization of our goal of this correspondence between algebra and geometry is the ability of \( I \) to fail to contain \( I(V(I)) \). The nullstellensatz will tell us that if we improve field of consideration to an algebraically closed field, we can remedy this problem, by considering slightly different ideals.

### 3 A Commutative Algebra Refresher.

We review several concepts and constructions from ring theory necessary for the proof of the nullstellensatz.

**Definition.** Let \( R \) be a ring, and let \( I \subset R \) be an ideal. We define the **radical** of the ideal by

\[
\text{rad}(I) = \{ x \in R : \text{there exists } r \in \mathbb{N} : x^r = 1 \}. 
\]

The radical of the ideal \( I \) is the set of elements that are eventually in \( I \) under exponentiation.

**Proposition.** Given a ring \( R \) and an ideal \( I \subset R \), we have that \( \text{rad}(I) \) is an ideal and \( I \subset \text{rad}(I) \).

**Proof.** First, we check that \( I \) is closed under multiplication from \( R \). Let \( r \in R \), and fix \( x \in \text{rad}(I) \). Let \( n_x \) be the minimal exponent so that \( x^{n_x} \in I \). We have that \( (rx)^{n_x} = r^{n_x}x^{n_x} \in I \), by \( I \) an ideal. Now, let \( x, y \in \text{rad}(I) \) and let \( n_x, n_y \) be defined as \( n_x \) was before. We have that for any \( n \in \mathbb{N} \)

\[
(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. 
\]

We can choose \( n \) large enough so that each term has one of \( k \geq n_x \) or \( n - k \geq n_y \). Finally, note that \( 0 \in I \) so that \( 0^1 \in I \). Therefore, \( 0 \in \text{rad}(I) \). We conclude that \( \text{rad}(I) \) is an ideal and \( I \subset \text{rad}(I) \).

**Example.** Take \( R = \mathbb{Z} \) and \( I = p\mathbb{Z} \). Then we have that

\[
\text{rad}(I) = \{ x \in \mathbb{Z} : \text{there exists } r \in \mathbb{N} : x^r \in p\mathbb{Z} \}
\]
\[ \{ x \in \mathbb{Z} : \text{there exists } r \in \mathbb{N} : p|x^r \} = \{ x \in \mathbb{Z} : p|x \} = p\mathbb{Z}. \]

**Definition.** A subset \( S \) of a ring \( R \) is called **multiplicative** if \( 1 \in S \) and \( a, b \in S \) implies that \( ab \in S \).

**Definition.** Let \( R \) be an integral domain, and take \( S \subset R - \{0\} \) to be a multiplicative subset. \( R_S = S^{-1}R \) is said to be the **localization** of \( R \) at \( S \), defined to be \( R \times S / \sim \), where 
\[
(a, s) \sim (a', s') \iff as' = a's.
\]

Write \((a, s)\) as \( \frac{a}{s} \), and we can define the operations
\[
(a, s) \cdot (a', s') = \frac{a}{s} \cdot \frac{a'}{s'} = \frac{a \cdot a'}{s \cdot s'},
\]
\[
(a, s) + (a', s') = \frac{as' + sa'}{ss'}.
\]

**Example.** If \( S = R - \{0\} \), then \( R_S \) is the field of fractions of \( R \). There exists a homomorphism \( \iota : R \to S^{-1}R \) given by \( \iota(x) = \frac{x}{1} \). Actually, \( \iota(x) \) has inverse \( \frac{1}{x} \). In this sense, \( S^{-1}R \) is the smallest ring containing \( R \) and inverses for \( S \).

### 4 The Theorems.

**Lemma.** Let \( k \) be an uncountable algebraically closed field and let \( K \) be a field extension of \( k \) with dimension at most countable, then \( K = k \).

**Proof of Lemma.** It is sufficient to show that \( K \) is algebraic over \( k \), since \( k \) is algebraically closed. If this is not the case, then \( K \) contains a transcendental element, \( \tau \), and has a subfield \( F \) with \( F \cong k(t) \). Let’s verify the existence of this subfield \( F \). Let \( \tau \) be our transcendental element and let us consider the minimal field extension \( F \) of \( k \) containing \( \tau \). This field extension must contain
\[
\left\{ \sum_{i=0}^{n} \lambda_i \tau^i : n \in \mathbb{N}, \lambda_i \in k \right\}
\]
and the set of formal inverses for this set. Identifying \( \tau \) with \( t \), we have that \( F \cong k(t) \). Now, there exists an uncountable family 
\[
F := \left\{ \frac{1}{t - a} : a \in k \right\} \subset k(t),
\]
moreover the equation
\[
\sum_i \frac{\gamma_i}{t - a_i} = 0
\]
implies that 
\[
(t - a_j) \sum_i \frac{\gamma_i}{t - a_i} = \sum_i \frac{\gamma_i (t - a_j)}{(t - a_i)} = 0.
\]
Take \( t = a_j \), and observe that \( \gamma_j = 0 \). So, the objects in \( F \) are relation free, and thus \text{dim } K \text{ is uncountable, a contradiction.} \]

**Theorem.** (Weak Nullstellensatz) Let \( I \subset k[X_1, \ldots, X_n] \) be an ideal different from \( k[X_1, \ldots, X_n] \), then \( V(I) \neq \emptyset \).

**Proof.** Suppose in addition that \( k \) is uncountable – there is a separate proof for \( k \) countable or finite, which for now we won’t address. Suppose that \( I \) is maximal – if not, embed \( I \) in a maximal ideal. This
is no loss of generality, since if \( m \supset I \) is a maximal ideal, we have that \( V(m) \subset V(I) \). Thus, showing that \( V(m) \neq \emptyset \) will be sufficient.

Anyway, let \( K = k[X_1, \ldots, X_n]/I \) be the corresponding residue field. \( k[X_1, \ldots, X_n] \) is a vector space of at most countable dimension over \( k \), and so the same holds for \( K \).

Now, take evaluations \( X_i \mapsto a_i \in k \). We know that \( K = k \), by the Lemma. So if \( f(X_1, \ldots, X_n) \in I \), we have that \( f(a_1, \ldots, a_n) = 0 \), so that \( (a_1, \ldots, a_n) \in V(I) \). This concludes the proof of the weak nullstellensatz.

\[ \blacksquare \]

**Theorem.** (Nullstellensatz) Let \( I \subset k[X_1, \ldots, X_k] \). Then \( I(V(I)) = \text{rad}(I) \).

**Proof.** Take \( R = k[X_1, \ldots, X_n] \), \( I = (P_1, \ldots, P_r) \), and \( V = V(I) \). We can see that \( \text{rad}(I) \subset I(V(I)) \).

If \( P \in k[X_1, \ldots, X_n] \) such that there exists \( n \in \mathbb{N} \) such that \( P^n \equiv 0 \) on \( V(I) \), then \( P \equiv 0 \) on \( V(I) \). Take \( F \in I(V) \). We want to show that \( F^m \in I \) for \( m \in \mathbb{N} \).

We want to interpret this in terms of the local ring \( R_F \), given by localizing at the multiplicative subset \( S = \{ F^k : k \in \mathbb{N} \} \cup \{ 1 \} \). It is sufficient to show \( IR_F = (1) = R_F \). Because, this is equivalent to being able to choose \( Q_i \in R \) so that

\[ 1 = \sum_i P_i Q_i \]

for some \( m \). Then, \( F^m = \sum_i P_i Q_i \). Now, by introducing an indeterminate object \( T \), and quotienting by the relation \( 1 - TF = 0 \), we have that \( TF = 1 \), so that \( T \) is the formal inverse of \( F \). Then, it is clear that

\[ R_F \cong k[X_1, \ldots, X_n, T]/(1 - TF) \]

So,

\[ IR_F = (1) \iff 1 = \sum_i P_i Q_i + A(1 - TF) \]

where \( A, Q_i \in k[X_1, \ldots, X_n, T] \). Set \( J = (P_1, \ldots, P_r, 1 - TF) \subset k[X_1, \ldots, X_n, T] \). We have that \( V(J) = \emptyset \) in \( k^{n+1} \), since if \( (x_1, \ldots, x_n, t) \in V(J) \), then \( P_i(x_1, \ldots, x_n) = 0 \) which implies that \( (1 - TF)(x_1, \ldots, x_n) \neq 0 \).

The weak nullstellensatz implies that \( J = (1) \) which implies that we can write

\[ 1 = \sum_i P_i Q_i + A(1 - TF) \]

This implies that \( IR_F = (1) \) which shows us that

\[ 1 = \sum_i \frac{P_i Q_i}{F^m} \Rightarrow F^m = \sum_i P_i Q_i \Rightarrow F^m \in I \]

for some \( m \). \( \blacksquare \)