The Hilbert Nullstellensatz and the Jacobson radical

Liran Shaul

November 22, 2007

Abstract

Our main goal is to prove the Hilbert Nullstellensatz. We start with a very short introduction to algebraic geometry, describing the problem of determining the ideals of algebraic sets. Next, we define the Jacobson radical of a (not necessarily commutative) ring, study its basic properties and prove Nakayama’s lemma. Next, we characterize the invertible and nilpotent elements and the Jacobson radical of a polynomial ring over a commutative ring. Finally, we define the notion of an Hilbert ring, use the Jacobson radical to prove that a polynomial ring in n variables over a field is Hilbert, and use this result to prove the Nullstellensatz.

1 Affine algebraic varieties

Remark In this section all rings are assumed to be commutative.

Let $k$ be a field. We consider the affine n-space over $k$, $A^n = k^n$. We also set $A = k[x_1, \ldots, x_n]$, the ring of polynomials in n variables with coefficients in $k$.

The most basic objects studied in algebraic geometry are sets of common zeroes of polynomials in A. More precisely, let $S \subseteq A$ be a set of polynomials. We define

$$Z(S) = \{x \in A^n : \forall f \in S, f(x) = 0\}$$

Example Take $k = \mathbb{R}$, $n = 2$, $S = \{x^2 + y^2 - 1\}$. Then $Z(S)$ is the unit circle.
**Example** Take \( k = \mathbb{Q} \), \( n=3 \), take \( m \in \mathbb{N} \), \( m > 2 \), and take \( S = \{ x^m + y^m + z^m \} \). Then \( Z(S) \cap \{(x,y,z) \in \mathbb{A}^3 : xyz \neq 0 \} = \emptyset \) is Fermat’s last theorem.

**Lemma 1.1** For \( S \subseteq A \), \( Z(S) = Z((S)) \), where \((S)\) is the ideal generated by \( S \).

**Proof** If \( x \in Z(S) \), \( f \in (S) \), then we may write \( f = \sum a_i f_i \), with \( f_i \in S \). Then \( f(x) = \sum a_i f_i(x) = \sum a_i(x)0 = 0 \). The converse is clear. \(\square\)

Hence, we may concentrate on sets of the form \( Z(I) \) where \( I \) is an ideal of \( A \). We quote the following theorem:

**Theorem 1.2** (Hilbert basis theorem) Let \( R \) be a Noetherian ring (i.e., every ideal of \( R \) is finitely generated). Then \( R[x] \) is also Noetherian.

Hence, \( A \) is a Noetherian ring, so we may also concentrate on sets of the form \( Z(S) \) where \( S \) is a finite set.

Let \( V \subseteq A^n \) be a set of points in the affine space. Define:

\[
I(V) = \{ f \in A : \forall x \in V, f(x) = 0 \}
\]

Then clearly \( I(V) \) is an ideal of \( A \).

**Lemma 1.3** Let \( a_1, \ldots, a_n \in k \). Then the ideal \( m = (x_1 - a_1, \ldots, x_n - a_n) \) in \( k[x_1, \ldots, x_n] \) is maximal.

**Proof** Set \( A = k[x_1, \ldots, x_n] / m \). Looking at the natural map \( \phi : k[x_1, \ldots, x_n] \to A \), we see that \( \phi(k) \cong k \) is a sub-ring of \( A \). On the other hand, since \( \phi(x_i) = \overline{x_i} \), we see that \( A = \phi(k[x_1, \ldots, x_n]) = \phi(k) \), so that \( A = k \) and \( m \) is maximal. \(\square\)

Also, if for some \( n > 1 \), for some \( f, f^n \in I(V) \) then \( f^n(x) = 0 \) for all \( x \in V \), so clearly \( f(x) = 0 \), and \( f \in I(V) \).

We want to understand what kind of ideals are of the form \( I(V) \) for a subset \( V \subseteq A^n \).

The radical of an ideal \( I \), denoted by \( \sqrt{I} \) is an ideal defined by:

\[
\sqrt{I} = \{ x \in A : \exists n \in \mathbb{N}, x^n \in I \}
\]

An ideal \( I \) satisfying \( I = \sqrt{I} \) is called a radical ideal. Hence, \( I(V) \) is a radical ideal. Let us first try to achieve a better understanding of radical ideals.
Lemma 1.4 Let $R$ be a ring. Let $\text{nil}R$ be the set of nilpotent elements in $R$. Then $\text{nil}R$ is an ideal of $R$ which is equal to the intersection of all prime ideals in $R$.

Proof Clearly $\text{nil}R \subseteq p$ for every prime ideal $p$. Conversely, suppose that $a \in R$ is not nilpotent. Let $S = \{1, a, a^2, a^3, \ldots \}$. The set of ideals which does not intersect $S$ is not empty (It contains 0), and using Zorn’s lemma, it is easy to see that it has maximal elements. let $p$ be such a maximal element. Then $a \notin p$. It is enough to show that $p$ is prime. Suppose that $x, y \notin p$. Then $p + (x)$ and $p + (y)$ both intersect $S$. Hence, there exist $p_1, p_2 \in p$, $a, b \in R$ and $s_1, s_2 \in S$ such that $p_1 + ax = s_1$, $p_2 + by = s_2$. But then $S \ni s_1s_2 = (p_1 + ax)(p_2 + by) = p_1p_2 + p_1by + p_2ax + abxy$. Hence, if we had $xy \in p$, then we had $s_1s_2 \in p$, a contradiction. □

Theorem 1.5 Let $R$ be a ring, $I$ an ideal in $R$. Then the radical of $I$ is equal to the intersection of all prime ideals containing $I$.

Proof Let $f : R \to R/I$ be the canonical map. We have: $x \in \sqrt{I}$ if and only if $f(x)$ is nilpotent, if and only if, for every prime ideal $\tilde{p}$ in $R/I$, $f(x) \in \tilde{p}$ if and only if $x \in p$ for every prime ideal $p$ containing $I$. □

2 The Jacobson radical of a ring

Remark We no longer assume that rings are commutative.

Definition Let $R$ be a ring. A (left) $R$-module $M$ is called simple if it has no proper non-zero submodules.

If $M$ is a simple module, $0 \neq m \in M$, then $Rm = M$. Let $I$ be the kernel of the map $\phi : R \to M$, $\phi(a) = am$. Then $I$ is a left ideal of $R$, and $R/I \cong M$. In particular, $I$ is a maximal left ideal of $R$. Conversely, given a maximal left ideal $I$ in $R$, $R/I$ is a simple module.

For a module $M$, we define the annihilator of $M$ by $\text{ann}(M) = \{x \in R : xM = 0\}$. This is a left ideal in $R$. Note that for a simple module $M = R/m$, $\text{ann}(M) = \text{ann}(R/m) = m$.

We want to detect elements in a ring $R$ which behaves almost like zero. The set of such elements will be called the Jacobson radical of the ring $R$ and will be denoted by $\text{rad}R$. Our first definition for $\text{rad}R$: The set of all elements of $R$ which annihilates all simple $R$-modules. In other words:
Definition The Jacobson radical of a ring $R$ is defined by:

$$rad_R = \bigcap_{M \text{ is a simple } R \text{-Module}} \text{ann}(M) = \bigcap_{m \text{ is a maximal left ideal}} m$$

Remark This definition does not look symmetric, as it appears that we prefer left maximal ideals over right maximal ideals. However, it is possible to prove that the intersection of all left maximal ideals if equal to the intersection of all right maximal ideals. We omit the proof since we will not use this fact.

We now give 3 other properties which explains why the elements of the Jacobson radical "behaves like zero":

**Theorem 2.1** Let $R$ be a ring. Then $y \in radR$ if and only if, for every $x \in R$, $1 - xy$ is left invertible (there exist $z \in R$ s.t $z(1 - xy) = 1$).

**Proof** Suppose that $y \in radR$. Then for every maximal left ideal $m$ in $R$, $y \in m$. Hence, $xy \in m$. Hence, $1 - xy \notin m$. Hence, $1 - xy$ does not belong to any maximal left ideal, so it must be left invertible.

Conversely, suppose that $1 - xy$ is left invertible for every $x \in R$. Let $m$ be a left maximal ideal, and suppose by contradiction that $y \notin m$. Then we must have $m + Ry = 1$, so there exist $z \in m$ and $x \in R$ such that $z + xy = 1$. Hence, $z = 1 - xy$, which is left invertible and belongs to $m$, a contradiction. □

Definition An element $x$ of a ring $R$ is called a **non-generator** if for every subset $S \subseteq R$ such that $S \cup \{x\}$ generates $R$ (as a left ideal), $S$ alone already generates $R$.

**Theorem 2.2** The Jacobson radical is exactly the set of all non-generators of the ring.

**Proof** Let $x \in radR$. Suppose that $S = \{s_1, \ldots, s_n\}$ and that $c_1s_1 + c_2s_2 + \ldots c_ns_n + bx = 1$. Then $c_1s_1 + \ldots c_ns_n = 1 - bx$. But $1 - bx$ is left invertible. Let $d = (1 - bx)^{-1}$, then $dc_1s_1 + \ldots dc_ns_n = 1$, so that $x$ is a non-generator. Conversely, suppose that $x$ is a non-generator. Let $m$ be a left maximal ideal. If $x \notin m$ then we must have $m + Rx = 1$, but this means that $m \cup \{x\}$ generates $R$, while $m$ does not generate $R$. This is a contradiction, so we must have $x \in m$ for every left maximal ideal, so that $x \in radR$. □
Finally, we prove the important Nakayama’s lemma, a very useful theorem in ring theory:

**Theorem 2.3** Nakayama’s lemma: Let $R$ be a ring, and $M$ a finitely generated $R$-module. Let $I$ be a left ideal of $R$ which is contained in the Jacobson radical. If $IM = M$ then $M = 0$.

**Proof** Let $a_1, \ldots, a_n$ be a minimal set of generators of $M$. Let $\Sigma$ be the set of all sub-modules of $M$ which contains $a_2, \ldots, a_n$ but does not contain $a_1$, ordered by inclusion. By Zorn’s lemma, $\Sigma$ has maximal elements. Let $N$ be such an element. Then $a_1 \notin N$, and $N$ is maximal with respect to that. Hence, $N$ must be a maximal proper sub-module of $M$. Let $P = M/N$. Then $P$ is a simple module (because every proper nonzero sub-module of $P$ give rise to a sub-module of $M$ containing $N$), so that $IP = 0$. But $IM/N = 0$ implies that $IM \subseteq N$. Hence, if $M \neq 0$ then $IM \neq M$. □

### 3 Polynomial rings and localization

**Remark** Again, we assume that all rings are commutative

#### 3.1 Polynomial rings

In this section we prove some lemmas about polynomial rings in one variable over a ring $R$. Our final goal is to determine the Jacobson radical of $R[x]$ in terms of $R$.

**Lemma 3.1** Suppose that $a \in R^\times$ and that $n \in R$ is nilpotent. Then $a + n \in R^\times$.

**Proof** Since $a + n = a(1 + a^{-1}n)$, and $-a^{-1}n$ is also nilpotent, we may assume that $a = 1$ and prove that $1 - n$ is invertible. Assume that $n^k = 0$. Then we have:

$$(1-n)(1+n+n^2+\ldots+n^{k-1}) = 1+n+n^2+\ldots+n^{k-1}-n-n^2-n^3-\ldots-n^{k-1}=1$$

□

**Lemma 3.2** Let $R$ be a ring. Then $\text{Nil}(R[x]) = (\text{Nil}R)[x]$. In other words, a polynomial in one variable with coefficients in $R$ is nilpotent if and only if all of its coefficients are nilpotent as elements in $R$.  

---

5
Proof If \( f \in (\text{Nil}R)[x] \) then by raising \( f \) in a high enough power we see from the binomial theorem that \( f^N = 0 \). Conversely, suppose that \( f(x) = a_0 + a_1x + \ldots + a_nx^n \) and that \( f^M = 0 \). Hence, \( a_0^M = 0 \). Since the set of all nilpotent elements is an ideal of \( R[x] \), we have that \( h(x) = f(x) - a_0 \) is also nilpotent. Let \( g(x) = a_1 + a_2x + \ldots + a_nx^{n-1} \). Then \( h(x) = xg(x) \).

If \( h^N(x) = 0 \), then \( x^Ng^N(x) = 0 \), so we must have \( g^N(x) = 0 \). Hence, by induction on \( \text{deg}F \), we conclude that \( a_i \) is nilpotent for every \( i \), so that \( f(x) \in (\text{Nil}R)[x] \).

\[ \square \]

Lemma 3.3 An element \( f(x) = a_0 + a_1x + \ldots + a_nx^n \) is invertible if and only if \( a_0 \) is invertible in \( R \) and for every \( i > 0 \), \( a_n \) is nilpotent.

Proof If \( a_0 \) is invertible and for \( 1 \leq i \leq n \) \( a_i \) is nilpotent then \( a_1x + a_2x^2 + \ldots + a_nx^n \) is nilpotent by the previous lemma. Hence, \( f(x) \) is a sum of an invertible element and a nilpotent element, so it is invertible. Conversely, suppose that \( f(x) \) is invertible, and let \( f^{-1}(x) = g(x) = b_0 + b_1x + \ldots + b_mx^m \).

Then \( fg = 1 \) implies that \( a_0b_0 = 1 \), so that \( a_0 \) is invertible.

We now prove by induction on \( r \) that \( a_n^{r+1}b_{m-r} = 0 \):

For \( r = 0 \), since \( 1 = f(x)g(x) = a_nbmx^{n+m} \) (Terms of lower degree, we have \( a_nb_m = 0 \). In general, for \( 0 < r \leq m \), the coefficient of \( x^{n+m-r} \) in \( f(x)g(x) \) (which is zero) is equal to \( a_{n-r}b_m + a_{n-r+1}b_{m-1} + \ldots + a_nb_{m-r} = 0 \).

Multiplying this by \( a_n^r \), and using the induction assumption we obtain that \( 0 = a_{n-r}a_n^rb_m + a_{n-r+1}a_n^rb_{m-1} + \ldots + a_n^{r+1}b_{m-r} = a_n^{r+1}b_{m-r} \) Using this for \( r = m \), we see that \( a_n^{m+1}b_0 = 0 \), but \( b_0 \) is invertible, so that \( a_n^{m+1} = 0 \).

Hence \( a_n \) is nilpotent, and so \( a_nx^n \) is also nilpotent. Hence, using a previous lemma, we see that \( f(x) - a_nx^n \) is also invertible. Continuing by induction we see that \( a_i \) is nilpotent for every \( 1 \leq i \leq n \).

\[ \square \]

We can now describe the Jacobson radical of a polynomial ring:

Theorem 3.4 Let \( R \) be a ring. Then \( \text{rad}R[x] = \text{nil}(R[x]) = (\text{Nil}R)[x] \)

Proof As we proved earlier, for any commutative ring \( A \), the set of nilpotent elements is equal to the intersection of all prime ideals in \( A \). The radical of \( A \) is equal to the intersection of all maximal ideals in \( A \). Since every maximal ideal is prime, we always have (for a commutative ring!): \( \text{nil}A \subseteq \text{rad}A \).

Hence, to prove the theorem, it is sufficient to show the converse.

Let \( f(x) = a_0 + a_1x + \ldots + a_nx^n \in \text{rad}R[x] \). Then \( 1 + xf(x) = 1 + a_0x + a_1x^2 + \ldots + a_nx^{n+1} \) is invertible. Hence, by the previous lemma, each \( a_i \) is nilpotent, so that \( f(x) \) is nilpotent.

\[ \square \]
3.2 Localization

In this subsection we define and study some basic properties of localization of a commutative ring at a prime ideal. Let $R$ be a commutative ring, and let $p$ be a prime ideal in $R$. Set $S = R - p$. Then $1 \in S$, and if $x, y \in S$ then since $p$ is prime, $xy \in S$. Hence, $S$ is a multiplicatively closed set. We want to define a new ring, denoted by $R_p$ which will contain $R$ and in which every element of $S$ will be invertible. We imitate the construction of the rational numbers from the integers: Define an equivalence relation on $R \times S$, by $(r_1, s_1) \sim (r_2, s_2)$ if there exist $t \in S$ such that $t(r_1s_2 - r_2s_1) = 0$. Setting $R_p = R \times S / \sim$ and under the natural operations, we obtain a ring, and under the identification $r = (r, 1) = \frac{r}{1}$, we see that $R$ is a sub-ring of $R_p$. Furthermore,

**Theorem 3.5** $R_p$ is a local ring with maximal ideal $pR_p$.

**Proof** Given an element $a/s \in R_p$, $a/s$ is invertible if and only if $s/a \in R_p$, if and only if $a \in S$, if and only if $a \notin p$. But $a \notin p$ if and only if $a/s \notin pR_p$, so that $R_p$ is a local ring with maximal ideal $pR_p$. □

4 Hilbert rings and the Nullstellensatz

**Definition** A commutative ring $R$ is called a Hilbert ring (or a Jacobson ring) if every prime ideal in $R$ is equal to the intersection of maximal ideals.

Note that if $R$ is a Hilbert ring and if $I$ is an ideal in $R$, then $R/I$ is also a Hilbert ring.

Our first goal is to show that a polynomial ring in $n$ variables over a field is a Hilbert ring.

**Lemma 4.1** Let $R \subseteq A$ be integral domains. Suppose that $A$ is a finitely generated $R$-algebra and that $\text{rad}R = 0$. Then $\text{Rad}A = 0$.

**Proof** By induction, we may assume that $A = R[a]$. We may also assume that every element in $A$ satisfy a polynomial with coefficients in $R$, since otherwise, $A$ contains a copy of $R[x]$ and we know by the a previous lemma that $\text{rad}R[x] = 0$. Suppose that $f(x) = \sum_{i=0}^{n} r_i x^i$ is a polynomial in $R[x]$ such that $f(a) = 0$ and $f$ is of a minimal degree. Suppose by contradiction that there exist $0 \neq b \in \text{rad}A$ and that $g(x) = \sum_{i=0}^{m} s_i x^i$ is a polynomial
in $R[x]$ such that $g(b) = 0$ and $g$ is of a minimal degree. Since $A$ is an integral domain, $s_0 = -\sum_{i=1}^{m} s_i b^i \in radA$ is not zero. Hence, $s_n s_0 \neq 0$.

Now, looking at $R_m$, we see that $r_n$ is a unit in $R_m$, so that $a \in R_m[a]$ satisfies a monic polynomial equation over $R_m$. Hence $R_m[a]$ is a finitely generated module over $R_m$, so by Nakayama’s lemma, $radR_m \cdot R_m[a] \subseteq R_m[a]$. But $radR_m = m$, so that $m \cdot R_m[a] \subseteq R_m[a]$. Hence, $mR[a] \neq R[a]$, so that $mA \subseteq R[a]$. Let $n$ be a maximal ideal of $A$ containing $mA$. Then $n \cap R = m$, and since $s_0 \notin m$, $s_0 \notin n$. This contradicts the assumption that $s_0 \in radA$.

**Theorem 4.2** Let $R \subseteq A$ be commutative rings, and suppose that $A$ is a finitely generated $R$-algebra, and that $R$ is a Hilbert ring. Then $A$ is also a Hilbert ring.

**Proof** Let $p \subseteq A$ be a prime ideal. Then $A/p$ is a finitely generated integral domain over $R/(p \cap R)$. Since $R/(p \cap R)$ is a Hilbert domain, $radR/(p \cap R) = nilR/(P \cap R) = 0$. Hence, by the previous lemma, $radA/p = 0$. The intersection of all maximal ideals in $A/p$ is the image in $A/p$ of the intersection of all maximal ideals in $A$ containing $p$, and since it is 0, $p$ is equal to the intersection of all maximal ideals containing it, so $A$ is a Hilbert ring.

**Corollary 4.3** Let $k$ be a field. Then the ring $k[x_1, \ldots, x_n]$ is an Hilbert ring.

**Corollary 4.4** Let $k$ be a field, and let $I$ be an ideal in $k[x_1, \ldots, x_n]$ then the radical of $I$, $\sqrt{I}$ is equal to the intersection of all maximal ideals containing $I$.

We need to prove just one more important lemma to obtain a full description of the ideals of algebraic sets:

**Lemma 4.5** Let $K$ be a field, $R \subseteq K$, such that $radR = 0$, and suppose that $K$ is a finitely generated $R$-algebra. Then $R$ is also a field, and $K$ is a finite algebraic field extension of $R$.

**Proof** By induction we first assume that $K = R[a]$. Clearly, $a$ must satisfy a polynomial equation with coefficients in $R$. Suppose that $f(x) = \sum_{i=0}^{n} r_i x^i \in$
$R[x]$ has $f(a) = 0$. Let $m$ be a maximal ideal in $R$ such that $r_n \notin m$ (there exist such a $m$ because $\text{rad}R = 0$). As we saw in the proof of lemma (4.1), $mK \subsetneq K$. But $K$ is a field and $mK$ is an ideal in $K$. Hence, $mK = 0$. Hence $m = 0$, so that $R$ is a field, and since $K = R[a]$, $K$ is a finite algebraic extension of $R$. In the general case, suppose that $K = R[a_1, \ldots, a_m]$. Let $R' = R[a_1, \ldots, a_{m-1}]$. By a previous lemma, $\text{rad}R' = 0$, so by what we just proved, $R'$ is a field, and $K$ is a finite algebraic field extension of $R'$. By induction, we obtain that $R$ is a field and by the tower theorem of field extensions, $K$ is a finite algebraic field extension of $R$. \hfill \Box

**Corollary 4.6** Let $k$ be an algebraically closed field. Let $m$ be a maximal ideal in $k[x_1, \ldots, x_n]$. Then there exist a point $(a_1, \ldots, a_n) \in A^n$ such that $m = (x_1 - a_1, \ldots, x_n - a_n)$. Hence, $Z(m) = (a_1, \ldots, a_n)$.

**Proof** Let $A = k[x_1, \ldots, x_n]/m$. Then $A$ is a field, and since in the natural map $k[x_1, \ldots, x_n] \to A$, $k$ is mapped bijectively, we may view $k$ as a subring of $A$. Now, $A$ is clearly generated by $k$ and by the images of $x_i$ in $A$. Let $a_i = \overline{x_i}$. Hence, by the previous lemma, $A$ is a finitely algebraic field extension of $k$. But $k$ is algebraically closed, so we must have $A = k$. Hence $a_i \in k$. Now, given a polynomial $f(x_1, \ldots, x_n) \in m$. The image of $f(x_1, \ldots, x_n)$ in $A$ is zero, but it is also equal to the image of $f(a_1, \ldots, a_n)$ in $A$. But $f(a_1, \ldots, a_n) \in k$, and $k$ maps bijectively into $A$, so we must have $f(a_1, \ldots, a_n) = 0$.

Hence, $(a_1, \ldots, a_n) \in Z(m)$. Now, $I(Z(m))$ is a (proper) ideal in $k[x_1, \ldots, x_n]$ containing $m$, so it must be equal to $m$. Let $n = (x_1 - a_1, \ldots, x_n - a_n)$. Then $n$ is a maximal ideal, and $(a_1, \ldots, a_n) = Z(n)$. Hence, $I(\{(a_1, \ldots, a_n)\}) = I(Z(n)) = n$. Finally, Since $\{(a_1, \ldots, a_n)\} \subseteq Z(m)$, we have $m = I(Z(m)) \subseteq I(\{(a_1, \ldots, a_n)\}) = n$, so that $m = n$. \hfill \Box

The last corollary shows us that there is a bijection between maximal ideals in $k[x_1, \ldots, x_n]$ and points in $A^n$. Given a point $a \in A^n$, we denote by $m_a$ the maximal ideal of polynomials which annihilates $a$.

We may now formulate and prove the Hilbert Nullstellensatz:

**Theorem 4.7** Let $J \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then $I(Z(J)) = \sqrt{J}$.

**Proof** Suppose that $f \in \sqrt{J}$. Then there exist $n \geq 1$ such that $f^n \in J$. Given a point $a \in Z(J)$, we have $f^n(a) = 0$. Hence, since $k$ is a field, $f(a) = 0$. Since this holds for all $a \in Z(J)$, we have $f \in I(Z(J))$, so that
\( \sqrt{J} \subseteq I(Z(J)) \).

Conversely, let \( f \in I(Z(Z)) \). Then for every \( a \in Z(J) \), \( f(a) = 0 \). Hence, \( f \in m_a \). Hence, \( f \in \bigcap_{a \in Z(J)} m_a \).

Now, recall that \( \sqrt{J} \) is equal to the intersection of all prime ideals containing \( J \). But \( k[x_1, \ldots, x_n] \) is an Hilbert ring, so \( \sqrt{J} \) is equal to the intersection of all maximal ideals containing \( J \). Finally, if \( m \) is a maximal ideal containing \( J \), then \( Z(m) \subseteq Z(J) \). Hence, \( m = m_a \) for some \( a \in Z(J) \). Hence, there exist a subset \( V \subseteq Z(J) \) such that \( \sqrt{J} = \bigcap_{a \in V} m_a \). And finally, we obtain:

\[
f \in \bigcap_{a \in Z(J)} m_a \subseteq \bigcap_{a \in V} m_a = \sqrt{J}
\]

\[\square\]

**Corollary 4.8** There is a 1-1 correspondence between algebraic subsets of \( \mathbb{A}^n \) and radical ideals of \( k[x_1, \ldots, x_n] \).