Nullstellensatz

Joseph Sullivan

July 2022

1 Introduction

These notes are a paraphrase/clarification/obfuscation of Gathmann's notes on Commutative Algebra, covering most of the essentials to proving Hilbert's Nullstellensatz.

Definition 1.1. Let K be a field. We define

- $\mathbb{A}^n_K = \mathbb{A}^n = K^n$.
- $I(a) = (x_1 - a_1, \ldots, x_n - a_n) \trianglelefteq K[x_1, \ldots, x_n]$,
- For $S \subseteq K[x_1, \ldots, x_n]$, $V(S) = \{a \in \mathbb{A}^n \mid f(a) = 0 \text{ for all } f \in S\}$
- For $X \subseteq K^n$, $I(X) = \{f \in K[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in X\}$

In words, $V(S)$ is the set of points where all of S is zero, and $I(X)$ are the functions that are zero on at least X.

2 Cayley-Hamilton

Theorem 2.1 (Cayley-Hamilton)**.** Let M be a finitely generated R-module, I an ideal of R, and $\varphi : M \to M$ an R-module homomorphism with $\varphi(M) \subseteq IM$. Then there is a monic polynomial

$$\chi = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$$

with $a_0, \ldots, a_{n-1} \in I$ and

$$\chi(\varphi) := \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 \mathrm{id} = 0 \quad \in \mathrm{Hom}_R(M, M)$$

where φ^i denotes the i-fold composition of φ with itself.

Proof. Let $m_1, \ldots, m_n$ be generators of M. We can then represent φ in this generating set, i.e., write

$$\varphi(m_i) = \sum_{j=1}^{n} a_{i,j} m_i$$

for some $a_{i,j} \in I$, so we can write

$$\begin{bmatrix} \varphi(m_1) \\ \vdots \\ \varphi(m_n) \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix}.$$

We denote this matrix by $A \in M_n(R)$, and we denote our column of m_i by $\mathbf{m} \in M^n$. Upgrading our module M to an $R[x]$-module by defining $x \cdot m = \varphi(m)$, we also get

$$\begin{bmatrix} \varphi(m_1) \\ \vdots \\ \varphi(m_n) \end{bmatrix} = \begin{bmatrix} x & & 0 \\ & \ddots & \\ 0 & & x \end{bmatrix} \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = xI_n\mathbf{m}$$

Thus, we have

$$(xI_n - A)\mathbf{m} = 0.$$

Multiplying by the adjugate matrix in $M_n(R[x])$, we get

$$\det(xI_n - A)\mathbf{m} = 0.$$

Expanding the determinant, we get that $\det(xI_n - A)$ is a monic polynomial in $R[x]$ with non-leading coefficients in $\langle a_{i,j} \rangle \subseteq I$. Then, since it annihilates $m_1, \ldots, m_n$ which are generators for M, so it annihilates all of M. Thus, $\chi := \det(xI_n - A)$ is the zero homomorphism in $\mathrm{Hom}_R(M, M)$. $\square$

Remark 2.2. If we take $R = K$ a field and $I = K$, $M = V$ a finite dimensional K vector space, and $m_i = e_i$ a K-basis for V—then we get the classical Cayley-Hamilton with $\chi = p_\varphi(\lambda) = \det(\lambda I - \varphi)$.

3 Localization

Proposition 3.1. Let S be a multiplicative subset in a ring R, and let $I \trianglelefteq R$ be an ideal with $I \cap S = \emptyset$. Then, there exists a prime ideal P of R containing I with $P \cap S = \emptyset$ and $S^{-1}P$ is a maximal ideal in $S^{-1}R$.

When we take $S = \{1, f, f^2, \ldots\}$, we can interpret this theorem geometrically in scheme language. It tells us in particular that $D(f) \cap V(I)$ is nonempty.

Proof. The ideal $S^{-1}I \trianglelefteq S^{-1}R$ is proper because $I \cap S = \emptyset$. In more detail, otherwise we would have $1 \in S^{-1}I$, so there exists $a \in I, s \in S$ so that $\frac{a}{s} = 1$. Then, this implies there exists $v \in S$ such that $va = vs$. However, this element would be in $I \cap S$.

Then, since $S^{-1}I$ is proper, it can be extended to a maximal ideal in $S^{-1}R$. The contraction P will then be a prime (not necessarily maximal) ideal disjoint from S. $\square$

4 Integrality

Definition 4.1 (Integral and finite ring extensions)**.**

- If $R \subseteq R'$, we call R' an **extension ring** of R, and we call $R \subseteq R'$ a ring extension.
- An element $a \in R' \supseteq R$ is called **integral** over R if there is a monic polynomial $f \in R[x]$ with $f(a) = 0$. We say R' is **integral** over R if every elements of R' is integral over R.
- A ring extension $R \subseteq R'$ is called **finite** if R' is finitely generated as an R-module.

Remark 4.2. For integrality, we require the existence of a *monic* polynomial because for purposes of finite generation we want to be able to write a^n in terms of lower powers of a for sufficiently large n. In a field, we can always make polynomials monic to accomplish this, but for rings we need the monic condition.

Proposition 4.3. An extension ring R' is finite over R if and only if $R' = R[a_1, \dots, a_n]$ for integral elements $a_1, \dots, a_n \in R'$ over R.

Moreover, in this case the whole ring extension $R \subseteq R'$ is integral.

Proof. Assume $R' = \langle a_1, \dots, a_n \rangle$ (is finitely generated) as an R-module. In particular, $R' = R[a_1, \dots, a_n]$. We now just need to show that R' is integral over R to get the "moreover" and that $a_1, \dots, a_n$ are integral over R. Let $a \in R'$. Applying Cayley-Hamltion theorem 2.1 to the R-module homomorphism

$$\begin{aligned} m_a : R' &\longrightarrow R' \\ x &\longmapsto ax \end{aligned}$$

to get a monic polynomial equation

$$m_a^k + c_{k-1} m_a^{k-1} + \cdots + c_0 = 0,$$

for some $c_0, \dots, c_{k-1} \in R$, which applied to $1 \in R$ gives us

$$a^k + c_{k-1} a^{k-1} + \cdots + c_0 = 0.$$

Thus, a is integral over R.

Now, assume $R' = R[a_1, \dots, a_n]$ with $a_1, \dots, a_n$ integral over R. Thus, each a_i satisfies a monic relation of degree d_i. Therefore, we can write every element of R' as a sum

$$\sum_{0 \le k_i \le d_i} c_{k_1, \dots, k_n} a_1^{k_1} \cdots a_n^{k_n}$$

since the homomorphism $R[x_1, \dots, x_n] \to R[a_1, \dots, a_n]$ is surjective and we can rewrite any higher degree terms in terms of lower degrees using our monic relation. Thus, $R' = \left\langle a_1^{k_1} \cdots a_n^{k_n} \right\rangle$ for $k_i = 0, \dots, n$ as an R-module. Therefore, R' is a finitely generated module over R. $\square$

Lemma 4.4. Let $R \subseteq R' \subseteq R''$ be ring extensions.

(a) If $R \subseteq R'$ and $R' \subseteq R''$ are finite, then so is $R \subseteq R''$.

(b) If $R \subseteq R'$ and $R' \subseteq R''$ are integral, then so is $R \subseteq R''$.

Proof of (a). By proposition 4.3, we can write $R' = R[a_1, \ldots, a_n]$ and $R'' = R'[b_1, \ldots, b_m]$. Then, we can write $R'' = R[a_i b_j \mid i = 1, \ldots, n, j = 1, \ldots, m]$, so R'' is finite over R. □

Proof of (b). Let $a \in R''$. Since R'' is integral over R', there exists monic polynomial

$$a^n + c_{n-1}a^{n-1} + \cdots + c_1 a^1 + c_0 = 0,$$

for $c_0, \ldots, c_{n-1} \in R'$, so

$$a \in R[c_0, \ldots, c_{n-1}].$$

Since R' is integral over R, each of $c_0, \ldots, c_{n-1}$ are integral over R. Therefore, $R[c_0, \ldots, c_{n-1}]$ is a finite extension of R, so $a \in R[c_0, \ldots, c_{n-1}]$ is integral over R. Thus, R'' is integral over R. □

Lemma 4.5. Let $R \subseteq R'$ be an integral ring extension. If $I \trianglelefteq R'$, then R'/I is an integral ring extension of R/I.

Proof. Let $\overline{a} \in R'$. Then, $a \in R'$ satisfies some monic relation

$$a^n + c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 = 0$$

for $c_0, \ldots, c_{n-1} \in R$, so $\overline{a}$ satisfies the relation

$$\overline{a}^n + \overline{c_{n-1}a}^{n-1} + \cdots + \overline{c_1 a} + \overline{c_0} = 0$$

for $\overline{c_0}, \ldots, \overline{c_{n-1}} \in R/(I \cap R)$ (identified with subring of R'/I), so $\overline{a}$ is integral over $R/(I \cap R)$. □

Proposition 4.6 (Lying Over)**.** Let $R \subseteq R'$ be a ring extension, and $P \trianglelefteq R$ prime.

(a) There is a prime ideal $P' \trianglelefteq R'$ with $P' \cap R = P$ if and only if $PR' \cap R \subseteq P$.

(b) If $R \subseteq R'$ is integral, then this is always the case.

We say in this case that P' is lying over P.

The condition in (a) is saying that the extension P^e isn't too large, i.e., that when we contract to get P^{ec} we are bounded by P. Geometrically, (b) says that the map $\operatorname{Spec} R' \to \operatorname{Spec} R$ is surjective when $R \subseteq R'$ is integral.

Proof of (a). Assume there exists $P' \trianglelefteq R'$ such that $P' \cap R = P$. Then,

$$PR' \cap R = (P' \cap R)R' \cap R \subseteq P'R' \cap RR' \cap R = P' \cap R \cap R = P$$

(watch out that product and intersection need not commute exactly).

Now, assume that $PR' \cap R \subseteq P$. We are looking for a prime ideal $P' \trianglelefteq R$ containing PR' and not much more. By proposition 3.1, since for $S = R \setminus P$, we have

$$PR' \cap S = PR' \cap R \setminus P = \emptyset,$$

there exists a prime ideal $P' \trianglelefteq R'$ containing $PR' \supseteq P$ with $P' \cap S = \emptyset$. This means $P' \cap (R \setminus P) = \emptyset$, and since $P \subseteq P'$, this means $P' \cap R = P$. □

Proof of (b). We show that $PR' \cap R \subseteq P$. Let $a \in PR' \cap R$. In particular, $a \in PR'$, so we have R-module homomoprhism

$$\begin{aligned} m_a : R' &\longrightarrow PR' \\ x &\longmapsto ax. \end{aligned}$$

By Cayley Hamilton theorem 2.1, there exist $c_0, \dots, c_{n-1} \in P$ such that

$$\begin{aligned} m_a^n + c_{n-1}m_a^{n-1} + \cdots + c_1 m_a + c_0 = 0 \\ a^n = -(c_{n-1}a^{n-1} + \cdots + c_1 a + c_0). \end{aligned}$$

Since $a \in R$, the left hand expression is in $RP = P$, so $a^n \in P$. Since P is prime, $a^n \in P$ implies $a \in P$. Thus, $PR' \cap R \subseteq P$. □

Proposition 4.7 (Incomparability)**.** Let $R \subseteq R'$ be an integral ring extension. If P' and Q' are distinct prime ideals in R' with $P' \cap R = Q' \cap R$ then $P' \not\subseteq Q'$ and $Q' \not\subseteq P'$.

Geometrically, we are saying that for the map $\operatorname{Spec} R' \to \operatorname{Spec} R$, if points P', Q' are mapped to the same point, then neither is contained in each other—i.e., P' doesn't correspond to an irreducible closed subscheme containing Q' and vice versa. In particular, the fiber of a closed point does not contain a closed subscheme, so we have some sort of finite fiber condition here.

Proof. Assume $P' \cap R = Q' \cap R$ and $P' \subseteq Q'$. We prove that $Q' \subseteq P'$ so that $P' = Q'$.

Suppose, to the contrary, that there exists $a \in Q' \setminus P'$. Then, we consider $\overline{a} \in R'/P'$, which is integral over $R/(P' \cap R)$ by lemma 4.5. Our strategy is to show that this relation on $\overline{a}$ has to be trivial, so $\overline{a} = 0$ and $a \in P'$.

Take a relation of minimal degree, and since $a \notin P'$ the degree is at least 2. We have

$$\begin{aligned} \overline{a}^n + \overline{c_{n-1}a}^{n-1} + \cdots + \overline{c_1 a} + \overline{c_0} = 0 \\ \overline{a}^n + \overline{c_{n-1}a}^{n-1} + \cdots + \overline{c_1 a} = -\overline{c_0} \end{aligned}$$

for some $c_0, \dots, c_{n-1} \in R$. Since $a \in Q'$, the left hand side is in Q'/P', so $\overline{c_0} \in Q'/P'$. Since $c_0 \in R$, we get

$$c_0 \in (R \cap Q')/(R \cap P') = 0$$

(by our original assumption). Thus, we have no constant term in the relation, but since we are in an integral domain R'/P', we can cancel out a factor of $\overline{a}$ to get a monic relation of strictly smaller degree.

Thus, we have a contradiction, so $a \in P'$ and $P' = Q'$. □

Corollary 4.8. Let $R \subseteq R'$ be an integral ring extension of integral domains. Then, R is a field if and only if R' is a field.

Proof. Assume that R is a field. Let $P' \trianglelefteq R'$ be a maximal ideal. Then, P' must contract to the 0 ideal, since the contraction is a prime ideal. Therefore,

$$0 \cap R = P' \cap R,$$

so by incomparability, $P' = 0$. Thus, R' has only maximal ideal 0, so it is a field.

Now, assume that R is not a field, so there exists a non-zero maximal ideal $\mathfrak{m} \trianglelefteq R$. By Lying Over proposition 4.6, there exists a prime ideal $P' \trianglelefteq R'$ with $P' \cap R = \mathfrak{m}$. In particular, $P' \neq 0$, so R' has a nontrivial proper ideal and is not a field. $\square$

5 Normalization

Remark 5.1. The idea of Noether Normalization is very nice. In one sentence, for any affine variety, we can pick coordinates $z_1, \ldots, z_r$ such that projection is a finite morphism. See Gathmann's Example 10.1.

Proposition 5.2 (Noether Normalization)**.** Let R be a finitely generated algebra over a field K with generators $x_1, \ldots, x_n \in R$. Then there is an injective K-algebra homomorphisms $K[z_1, \ldots, z_r] \to R$ from a polynomial ring over K to R that makes R into a finite extension ring of $K[z_1, \ldots, z_r]$.

Moreover, if K is an infinite field the images of $z_1, \ldots, z_r$ in R can be chosen to be K-linear combinations of $x_1, \ldots, x_n$.

We first give the proof idea, before going to some necessary lemmas and the actual detailed proof. The idea is as follows: Pick generators $x_1, \ldots, x_n$. Check if there is an algebraic relation among $x_1, \ldots, x_n$, i.e., a nonzero polynomial f in $x_1, \ldots, x_n$ over K with $f(x_1, \ldots, x_n) = 0$. If there is no algebraic relation, then R is isomorphic the polynomial ring $K[z_1, \ldots, z_n]$. Otherwise, we use some lemmas to choose new coordinates $y_1, \ldots, y_n$ such that y_n is redundant, in the sense that y_n is integral over $K[y_1, \ldots, y_{n-1}] \subseteq R$. We keep adjusting our coordinates until $y_1, \ldots, y_r$ have no algebraic relations, in which case we have found our copy of the polynomial ring $K[z_1, \ldots, z_r]$ inside R.

We give two lemmas to showcase two strategies for picking new coordinates—one that is linear but only works for infinite fields, and one that works in general.

Lemma 5.3 (Linear Coordinate Change for Infinite Fields)**.** Let $f \in K[x_1, \ldots, x_n]$ be a nonzero polynomial over an infinite field K. Then there exists $\lambda \in K$ (to get rid of scalar) and $a_1, \ldots, a_{n-1} \in K$ such that

$$\lambda f(y_1 + a_1 y_n, y_2 + a_2 y_n, \ldots, y_{n-1} + a_{n-1} y_n, y_n) \quad \in K[y_1, \ldots, y_n]$$

is monic in y_n (i.e., as an element of $(K[y_1, \ldots, y_{n-1}])[y_n]$).

Proof. Let $\lambda, a_1, \ldots, a_n \in K$ be arbitrary. We compute f written in our new coordinates, and then we determine how to choose our parameters. Writing

$$f = \sum_{k_1,\ldots,k_n} c_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n},$$

we get

$$\begin{aligned}
&\lambda f(y_1 + a_1 y_n, y_2 + a_2 y_n, \ldots, y_{n-1} + a_{n-1} y_n, y_n) \\
&\qquad = \lambda \sum_{k_1,\ldots,k_n} c_{k_1,\ldots,k_n} (y_1 + a_1 y_n)^{k_1} \cdots (y_{n-1} + a_{n-1} y_n)^{k_{n-1}} y_n^{k_n}.
\end{aligned}$$

Let $d = \deg f$. Then, the maximum y_n degree is d. Compute an expression for the y_n degree d part, we get

$$\lambda \sum_{\substack{k_1,\ldots,k_n \\ k_1+\cdots+k_n=d}} c_{k_1,\ldots,k_n} a_1^{k_1} \cdots a_{n-1}^{k_{n-1}} y_n^{k_1+\cdots+k_n} = \lambda f_d(a_1, \ldots, a_{n-1}, 1) y^d,$$

where f_d is the degree d part of f. We can therefore guarantee f in the new coordinates to be monic, as long as we can choose $f_d(a_1, \ldots, a_{n-1}, 1) \in K$ nonzero and λ to be the inverse. The next lemma guarantees such a choice of $a_1, \ldots, a_{n-1}$ is possible. □

Lemma 5.4. Let $f \in K[x_1, \ldots, x_n]$ be a nonzero homogeneous polynomial over an infinite field K. Then, there are $a_1, \ldots, a_{n-1} \in K$ such that $f(a_1, \ldots, a_{n-1}, 1) \neq 0$.

Proof. We prove the lemma by induction on n. If $n = 1$, then $f = cx$ for $c \in K$ nonzero, so $f(1) = c$. Now, assume $n > 1$. We can view f as a polynomial in $(K[x_2, \ldots, x_n])[x_1]$ and write

$$f = \sum_{i=0}^{d} f_i x_1^i,$$

where d is the degree of f, and the (potentially zero) f_i are homogeneous degree $d - i$ polynomials in $K[x_2, \ldots, x_n]$. At least one f_i is nonzero because f is nonzero. Then, by induction we can choose $a_2, \ldots, a_{n-1} \in K$ such that for this i,

$$f_i(a_2, \ldots, a_{n-1}, 1) \neq 0.$$

Fixing these $a_2, \ldots, a_{n-1} \in K$, we get

$$f(x_1, a_2, \ldots, a_{n-1}, 1) \in K[x_1]$$

a nonzero polynomial. It has at most finitely many roots (i.e., bounded by degree), and since K is infinite, we can choose $x_1 = a_1$ to not be a root. □

Lemma 5.5 (Coordinate Change for Arbitrary Fields)**.** Let $f \in K[x_1, \ldots, x_n]$ be a nonzero polynomial over an arbitrary field K. Then there exists $\lambda \in K$ and $a_1, \ldots, a_{n-1} \in \mathbb{N}$ such that

$$\lambda f(y_1 + y_n^{a_1}, y_2 + y_n^{a_2}, \ldots, y_{n-1} + y_n^{a_{n-1}}, y_n) \quad \in K[y_1, \ldots, y_n]$$

is monic in y_n (i.e., as an element of $(K[y_1, \ldots, y_{n-1}])[y_n]$).

Proof. We prove the claim by induction on n. For $n = 1$, $f = c_n x^n + \cdots + c_1 x + c_0$. We can then choose $\lambda = \frac{1}{c_n}$.

Now, assume that $\deg f > 1$. Let $d = \deg_{x_1} f$. Then, we can write

$$f = g x_1^d + h,$$

where $g \in K[x_2, \ldots, x_n]$ and $h \in K[x_1, \ldots, x_n]$ with $\deg_{x_1} h \leq d - 1$. By our induction hypothesis, we can choose $\lambda \in K$ and $a_2, \ldots, a_{n-1} \in \mathbb{N}$ such that

$$\lambda g(y_2 + y_n^{a_2}, \ldots, y_{n-1} + y_n^{a_n}, y_n)$$

is monic in y_n. Denote its leading y_n term by y_n^k. Fix a_1, we will see how to choose it later. We write $\widetilde{f}$ to denote the evaluation of f at our new coordinates, i.e., the image of f under the homomorphism

$$\begin{aligned} \varphi : K[x_1, \ldots, x_n] &\longrightarrow K[y_1, \ldots, y_n] \\ x_i &\longmapsto y_i + y_n^{a_i} \qquad i \neq n \\ x_n &\longmapsto y_n. \end{aligned}$$

Then, we have

$$\widetilde{f} = \widetilde{g}(y_1 + y_n^{a_1})^d + \widetilde{h}.$$

The leading y_n term of $\widetilde{g}(y_1 + y_n^{a_1})$ is just $\frac{1}{\lambda} y_n^{k + a_1 d}$. On the other hand, writing the y_n degree of $\widetilde{h}$ is bounded a function of $a_2, \ldots, a_{n-1}$ plus a term $a_1(d-1)$. Therefore, we can choose a_1 sufficiently large so $\frac{1}{\lambda} y_n^{k+a_1 d}$ dominates $\widetilde{h}$ in y_n degree (e.g., choose $a_1 > a_2 \cdots a_{n-1} \deg f$), giving us a choice of $a_1, \ldots, a_{n-1} \in \mathbb{N}$ and $\lambda \in K$. $\square$

Finally, with our two strategies for picking coordinates, we are in a position to prove Noether Normalization.

Proof of Noether Normalization 5.2. By induction on the given number of generators, n. For $n = 0$, we get $R = K$ and we are done.

Otherwise, assume $n > 0$. Consider the map

$$\begin{aligned} K[z_1, \ldots, z_n] &\longrightarrow R \\ z_i &\longmapsto x_i \end{aligned}$$

from the polynomial ring to R. If the map is injective (i.e., no algebraic relations among the x_i), then $R \cong K[z_1, \ldots, z_r]$ for $r = n$, and we are done.

Otherwise, the map is not injective and there is a nonzero relation $f \in K[z_1, \ldots, z_n]$, i.e., $f(x_1, \ldots, x_n) = 0$. Using either lemma 5.3 or lemma 5.5 (depending on the size of K), pick new generators $y_1, \ldots, y_n$, i.e.,

- For lemma 5.3, choose $y_i := x_i - a_i x_n$ for $i \neq n$, and $y_n := x_n$.
- For lemma 5.5, choose $y_i := x_i - x_n^{a_i}$ for $i \neq n$, and $y_n := x_n$.

Now, these new generators satisfy the algebraic relation guaranteed by the lemmas, which is monic in y_n. This shows that y_n is integral over the subalgebra $K[y_1, \dots, y_{n-1}]$. Therefore, $R = K[y_1, \dots, y_{n-1}][y_n]$ is finite over the subalgebra $K[y_1, \dots, y_{n-1}]$. By induction, there exists $r \in \mathbb{N}$ and an injective homomorphism

$$K[z_1, \dots, z_r] \longrightarrow K[y_1, \dots, y_{n-1}]$$

such that $K[y_1, \dots, y_{n-1}]$ is finite over the image. Since finiteness is transitive by proposition 4.4, we get that R is finite over the image. This completes the induction.

If K is infinite, we will always do linear coordinate changes to get the images of $z_1, \dots, z_r$ to be K-linear combinations of $x_1, \dots, x_n$. $\square$

6 Nullstellensatz

Corollary 6.1 (Zariski's Lemma)**.** Let K be a field, and let R be a finitely generated K-algebra which is also a field. Then, $K \subseteq R$ is a finite field extension. In particular, if K is algebraically closed, then $R = K$.

Proof. By Noether Normalization in proposition 5.2, we know R is finite over a polynomial ring $K[z_1, \dots, z_n]$, so it is in particular integral over $K[z_1, \dots, z_n]$ by proposition 4.3. Since R is a field and the extension is integral, by corollary 4.8, $K[z_1, \dots, z_n]$ must be field. Thus, $r = 0$ for $K[z_1, \dots, z_r]$ to be a field (e.g., for z_1 to be invertible).

Thus, $K \subseteq R$ is a finite field extension, and if K is algebraically closed, this implies $R = K$. $\square$

Corollary 6.2 (Weak Nullstellensatz)**.** Let K be an algebraically closed field. Then all maximal ideals of the polynomial ring $K[x_1, \dots, x_n]$ are of the form

$$I(a) = (x_1 - a_1, \dots, x_n - a_n)$$

for some $a = (a_1, \dots, a_n) \in \mathbb{A}^n_K$.

Proof. Let $\mathfrak{m} \trianglelefteq K[x_1, \dots, x_n]$ be a maximal ideal. Then, $K[x_1, \dots, x_n]/\mathfrak{m}$ is a field as well as a finitely generated K-algebra (use cosets $x_1, \dots, x_n$). Thus, by Zariski's lemma 6.1, $K[x_1, \dots, x_n]/\mathfrak{m} = K$, i.e. identifying K with the image of $K \subseteq K[x_1, \dots, x_n]$ under the quotient map. Then, taking a_i to be the image of x_i under quotienting, we get

$$(x_1 - a_1, \dots, x_n - a_n) \subseteq \mathfrak{m},$$

and since the left hand ideal is already maximal, we must have

$$\mathfrak{m} = I(a) = (x_1 - a_1, \dots, x_n - a_n).$$

$\square$

Corollary 6.3. For every ideal I in a finitely generated algebra R over a field K, we have

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{m} \supseteq I}} \mathfrak{m}.$$

This is an upgraded version of a theorem about prime ideals instead of maximal ideals. In the language of schemes, we can now figure out if a function is nilpotent by only looking at closed points.

Proof. The inclusion $\subseteq$ is immediate because maximal ideals are prime, so they are radical, so $I \subseteq \mathfrak{m}$ implies $\sqrt{I} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$.

Now, we prove the $\supseteq$ inclusion. Let $f \notin \sqrt{I}$. We want to find $\mathfrak{m} \supseteq I$ (a closed point in $V(I)$) such that $f \notin \mathfrak{m}$ (f is nonzero at $\mathfrak{m}$). Thus, we want to find a closed point in $D(f) \cap V(I)$. Taking $S = \{1, f, f^2, \cdots\}$, equivalently we are looking for $\mathfrak{m}$ such that $\mathfrak{m} \cap S = \emptyset$ and $f \notin \mathfrak{m}$.

Since $f \notin \sqrt{I}$, we know $S \cap I = \emptyset$, so by proposition 3.1, we can at least find a prime ideal P with $P \cap S = \emptyset$, $f \notin P$, and P_f maximal. We now try to show P is in fact maximal anyways.

We consider the field extension which is the composition $K \to R/P \to (R/P)_f = R_f/P_f$. This is indeed a field extension (i.e., not the zero map) because the second map is injective, since R/P is an integral domain.

Then, by construction R_f/P_f is a field, and it is a finitely generated K-algebra because it has generators consisting of those of $R \hookrightarrow R_f$ together with $\frac{1}{f}$. Therefore, by Zariski's lemma 6.1, the extension is finite and in particular integral by proposition 4.3. Thus, $R/P \subseteq R_f/P_f$ is integral as well, so R/P is a field by corollary 4.8. Therefore, P is maximal. ☐

Theorem 6.4 (Hilbert's Nullstellensatz)**.** Let K be algebraically closed. Then for every ideal $I \trianglelefteq K[x_1, \ldots, x_n]$ we have $I(V(I)) = \sqrt{I}$.

In particular, there is a bijection

$$\begin{aligned} \{\text{affine varieties in } \mathbb{A}^n_K\} \quad &\longleftrightarrow \quad \{\text{radical ideals in } K[x_1, \ldots, x_n]\} \\ Y \quad &\longmapsto \quad I(Y) \\ V(I) \ &\longleftarrow\!\shortmid\ I. \end{aligned}$$

Proof. **Hard Part.** We prove $I(V(I)) \subseteq \sqrt{I}$. Assume that $f \notin \sqrt{I}$. We want to find a point $a \in V(I)$ such that $f(a) \neq 0$. By corollary 6.3,

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{m} \supseteq I}} \mathfrak{m},$$

so there exists $\mathfrak{m}$ maximal such that $f \notin \mathfrak{m}$. By corollary 6.2, this maximal ideal is $I(a)$ for some $a \in K^n$. Since $I \subseteq I(a)$, we have $a \in V(I)$. Since $f \notin I(a)$, we have $f(a) \neq 0$. Therefore, $f \notin \sqrt{I}$.

Easy Part. Let $f \in \sqrt{I}$, so $f^n \in I$. Let $a \in V(I)$. Since $f^n \in I$, we know $f^n(a) = 0$. Thus, $f(a) = 0$, so $f \in I(V(I))$.

This gives us $I(V(I)) = \sqrt{I}$. We also have $V(I(X)) = X$ for any affine variety in $\mathbb{A}^n_K$ because clearly $X \subseteq V(I(X))$. Then conversely, we know that since X is an affine variety, $X = V(J)$, so then we want to show $V(J) \supseteq V(I(V(J)))$. By our previous discussion, $J \subseteq \sqrt{J} \subseteq I(V(J))$, and applying V we get our desired subset relation.

Therefore, for radical ideals I and affine varieties X, we have $I(V(I)) = I$ and $V(I(X)) = X$. Therefore, $V(-), I(-)$ are inverse bijections. $\square$