A canonical path to Hilbert's Nullstellensatz

Shintaro Fushida-Hardy
381B Sloan Hall, Stanford University, CA

This document contains results culminating in a proof of Hilbert's Nullstellensatz. The notes are mostly self-contained, relying only on basic algebra (integral domains, prime ideals, modules etc). However, some knowledge of localisations is assumed when developing some preliminary dimension theory results.

Contents

1 Introduction and outline

Hilbert's Nullstellensatz is the most fundamental theorem in algebraic geometry, establishing a rigorous correspondence between geometry and commutative algebra. In this document we prove Hilbert's Nullstellensatz assuming only basic definitions from a first course in ring theory. This is not the shortest route to the Nullstellensatz: the shortest proof I am familiar with is available on Daniel Allcock's website. However, I believe the route taken in these notes are canonical in the sense that the preliminary results focus on understanding the geometry of algebraic objects, hopefully giving some intuition as to why a correspondence between geometry (varieties) and algebra (ideals) is expected.

An overall outline of our proof of the Nullstellensatz is as follows:

1. An important idea in commutative algebra is that rings can be *extended*, and these extensions can satisfy certain "finiteness" properties (in the sense that the extension is only "finitely different" from the subobject). We first explore the properties of three such extensions, namely finite, finite-type, and integral extensions. In particular, we show that

$$\text{finite} \;\Leftrightarrow\; \text{integral} \;+\; \text{finite-type} \quad \text{(for ring extensions).}$$

2. The stronger the finiteness property, the more properties are preserved by the extension. We introduce a notion of dimension, and show that *integral extensions* are strong enough to ensure that dimensions are preserved.

3. We wish to use dimension arguments to prove the Nullstellensatz (or more precisely, Zariski's lemma). Therefore the next step is to:

    (a) show that the dimension of $k[x_1, \dots, x_n]$ is n,

(b) show that any integral domain R (which is finite-type over k) is a finite extension of some $k[x_1, \ldots, x_n]$.

Combining these two facts allows us to determine the dimensions of a general family of rings, since finite extensions preserve dimension. (b) is an important result on its own, called the *Noether normalisation lemma.* Both of the above facts are closely related, and follow from the *tilting of axes lemma* which is really a geometric result.

4. In particular, using these two facts above, we can prove *Zariski's lemma*:

$$\text{finite} \;\Leftrightarrow\; \text{finite-type} \quad \text{(for field extensions).}$$

This on its own is sometimes referred to as the weak Nullstellensatz, as the usual form of the weak Nullstellensatz follows almost immediately.

5. Finally we prove the general form of the Nullstellensatz from the weak form, using the Rabinowitsch trick.

2 Dimension theory

2.1 Integral, finite, and finite-type maps.

Recall from the introduction that our first local goal is to understand various notions for extensions of rings to be "finite".

Definition 2.1. A ring S is said to be *finite over R* if it is finitely generated as a module over R. That is, there is a ring homomorphism $f : R \to S$ (allowing S to be viewed as an R-module), and an R-linear surjection $R^n \to S$ for some n. S is a *finite extension* of R if f is injective.

Definition 2.2. A ring S is said to be *finite-type over R* if it is finitely generated as an algebra over R. That is, there is a ring homomorphism $f : R \to S$ (allowing S to be viewed as an R-module), and a surjective R-linear ring homomorphism $R[x_1, \ldots, x_n] \to S$. Equivalently, S is isomorphic to a quotient of $R[x_1, \ldots, x_n]$ as an R-algebra.

Definition 2.3. Let $f : R \to S$ be a ring homomorphism. An element $s \in S$ is *integral over R* if it is the root of a monic polynomial in $f(R)[X]$. S is *integral over R* if every element of S is integral over R, in which case f is said to be an integral homomorphism. If f is injective, it is an *integral extension.*

We later see that integral extensions preserve dimension, which is crucial in the development of our theory. It is not immediately clear that the above notions are related, but a characterisation of integrality in terms of submodule gives the following characterisation of finite morphisms:

Proposition 2.4. A ring is finite over R if and only if it is integral and finite-type over R.

This result depends on the following lemma:

Lemma 2.5. Let $f : R \to S$ be a ring homomorphism. $s \in S$ is integral over R if and only if it is contained in an R-subalgebra that is finite over R.

Proof. ($\Rightarrow$) Suppose $s \in S$ is integral over R. Then there is a monic polynomial p with coefficients in R with s as a root. The R-module generated by $1, s, \ldots, s^{\deg p - 1}$ is then closed under multiplication (since $s^{\deg p}$ can be expressed in terms of lower powers using p). Therefore this finitely generated R-submodule is in fact an R-subalgebra.

($\Leftarrow$) We employ the well-known trick used to prove Nakayama's lemma. Suppose s is contained in an R-algebra A which is finite over R. Let $a_1, \ldots, a_n \in A$ generate A as an R-module. Since A is closed under multiplication, there exists c_{ij} in $f(R)$ such that $sa_i = \sum c_{ij} a_j$ for each i. Let M denote the matrix representing s in the basis $\{a_i\}$. Then

$$(sI - M)(a_1, \ldots, a_n) = 0,$$

so in particular

$$\chi_M(s)(a_1, \ldots, a_n) = \det(sI - M)(a_1, \ldots, a_n) = \operatorname{adj}(sI - M)(sI - M)(a_1, \ldots, a_n) = 0.$$

This shows that $\chi_M(s)$ annihilates A, so in particular it kills 1. This shows that s is a root of χ_M, which is a monic polynomial with coefficients in $f(R)$. Therefore s is integral over R. □

We are now ready to prove the following proposition:

Proposition 2.6. Let $f : R \to S$ be a ring homomorphism. Then S is finite over R if and only if S is integral and finite-type over R.

Proof. ($\Rightarrow$) Suppose S is finite over R. S is then a finite R-subalgebra of itself, so S is integral over R by lemma 2.5. Next it is immediate that S is finite-type over R, since a finite set generating S as a module also generates S as an algebra.

($\Leftarrow$) Suppose S is integral and finite-type over R. Let $s_1, \ldots, s_n \in S$ generate S as an R-algebra. Since they are integral, consider the R-submodule of S generated by $\{s_i^{j_i}\}$, where the j_i vary between 1 and $\deg s_i - 1$. This is an R-algebra which is finite over R, and contains each s_i, so it contains S. Therefore by lemma 2.5 S is finite over R. □

Proposition 2.7. Suppose $f : R \to S$ is an integral homomorphism. Then integrality is preserved by localisations of R and quotients of S. Precisely,

1. If $D \subset R$ is multiplicative, the induced map $f : D^{-1}R \to f(D)^{-1}S$ is an integral homomorphism. (In fact, if $f : R \to S$ is an integral *extension*, so is the induced map on localisations).

2. If $I \subset S$ is an ideal, the induced map $f : R/f^{-1}(I) \to S/I$ is an integral homomorphism.

Proof. 1. Let $s/f(d) \in f(D)^{-1}S$. Choose a monic polynomial p with coefficients in R such that s is a root of p. Explicitly, there exists $r_i \in R$ such that

$$p(X) = X^n + r_1 X^{n-1} + \cdots + r_n.$$

Replacing each coefficient r_i with $r_i/d^i \in D^{-1}R$ gives a monic polynomial with coefficients in $D^{-1}R$ which has $s/f(d)$ as a root.

Now suppose moreover that $f : R \to S$ is an extension, i.e. injective. Suppose $f(r/d) = f(r)/f(d) = 0$. Then $f(d')f(r) = 0$ for some $d' \in D$. This requires $d'r = 0$, so r/d is zero in $D^{-1}R$. Therefore the induced map on localisations is also injective, hence an integral extension.

2. Let $\overline{s} = s + I \in S/I$. Choose a monic polynomial p with coefficients in R such that s is a root of p. The reduction of the coefficients of p modulo $f^{-1}(I)$ gives a monic polynomial with $\overline{s}$ as a root. □

2.2 The lying over and going up theorems

In the previous subsection we defined some notions for comparing rings. We now develop some results allowing us to compare the *dimensions* of rings. In particular, we show that dimension is preserved by integral extensions.

Definition 2.8. Let R be a ring. The *dimension* of R is the supremum of lengths of ascending chains of prime ideals $P_0 \subset P_2 \subset \cdots \subset P_n$ of R. Note that each P_i must be properly contained in P_{i+1}, and the *length* of the chain $P_0 \subset P_2 \subset \cdots \subset P_n$ is n.

Theorem 2.9 (Lying over theorem)**.** *Let $f : R \to S$ be an integral extension of rings. A prime ideal Q of S is said to* lie over *a prime P in R if $P = f^{-1}(Q)$.*

1. *If R and S are integral domains, R is a field if and only if S is a field.*
2. *A prime $Q \lhd S$ is maximal if and only if $f^{-1}(S)$ is maximal.*
3. *The primes of S lying over a prime of R have no non-trivial inclusions. That is, if $P \lhd R$ is prime, and $Q_1 \subset Q_2 \lhd S$ are primes lying over P, then $Q_1 = Q_2$.*
4. *Every prime of R has a prime lying over it.*

Note that the proofs of (3) and (4) use the machinery of localisations.

Proof. 1. Suppose R is a field. Let $s \in S$ be non-zero. There is a monic polynomial $f \in R[x]$ such that $f(s) = 0$. Explicitly, for some r_i, we have

$$s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0.$$

Without loss of generality, $r_0 \neq 0$. (If it were, the relation $s^{n-1} + \cdots + r_1 = 0$ would hold. At least one r_i must be non-zero, since s is non-zero and S is a domain.) But now since R is a field,

$$s(-s^{n-1}/r_0 - \cdots - r_1/r_0) = 1,$$

so s is a unit. Therefore S is a field.

Conversely, suppose S is a field. Let $r \in R$ be non-zero. Then $s = f(r)^{-1} \in S$. Since S is integral over R, for some r_i, we have

$$s^n + r_{n-1}s^{n-1} + \cdots + r_0 = f(r)^{-n} + r_{n-1}f(r)^{1-n} + \cdots + r_0 = 0.$$

Multiplying through by $f(r)^n$ gives

$$1 = f(r)(-r_{n-1} - \cdots - r_0 f(r)^{n-1}).$$

Therefore $-r_{n-1} - r_{n-2}r - \cdots - r_0 r^{n-1} \in R$ is the inverse of r, showing that R is a field as required.

2. Suppose $Q \subset S$ is a prime ideal. Then $f^{-1}(Q)$ is a prime ideal. The induced map $R/f^{-1}(Q) \to S/Q$ is an integral extension between domains. Therefore by 1, $f^{-1}(Q)$ is maximal if and only if Q is maximal.

3. Let $P \subset R$ be prime, and suppose $Q_1 \subset Q_2 \subset S$ are primes such that $f^{-1}(Q_1) = f^{-1}(Q_2) = P$. There is an induced integral extension $R_P \to S_{f(P)}$ by proposition 2.7. Each Q_i is disjoint from $f(R \setminus P)$, and hence descends to a prime ideal in $S_{f(P)}$. This is necessarily maximal by 2 since P is maximal in R_P. In particular, since $Q_1 \subset Q_2$, each Q_i descends to the same maximal ideal $Q_{1f(P)} = Q_{2f(P)}$. Since prime ideals of $S_{f(P)}$ are in bijective correspondence with prime ideals of S that are disjoint from $f(R \setminus P)$, $Q_1 = Q_2$.

4. This is similar to the previous proof. Let $P \subset R$ be prime, and consider the induced integral extension $R_P \to S_{f(P)}$ by 2.7. Let $Q_{f(P)}$ be a maximal ideal in $S_{f(P)}$. By 2, the preimage of $Q_{f(P)}$ is maximal in R_P, so it is necessarily P_P. $Q_{f(P)}$ lifts to a prime ideal Q in S, and P_P lifts to $P \subset R$.

To see that Q is lying over P, observe that $R \to R_P \to S_{f(P)}$ and $R \to S \to S_{f(P)}$ commute, so the preimages along either composition are equal. The first gives P and the second gives $f^{-1}(Q)$. □

Theorem 2.10 (Going up theorem). *If $f : R \to S$ is an integral homomorphism, $P_1 \subset \cdots \subset P_n$ is a chain of primes in R, and $Q_1 \subset \cdots \subset Q_m$ is a chain of primes lying over P_i with $m < n$, then Q_i can be extended to $Q_1 \subset \cdots \subset Q_n$, with each Q_i lying over P_i.*

Proof. By induction, it suffices to consider the case where $P_1 \subset P_2 \subset R$ are prime, and $Q_1 \subset S$ is a prime lying over P_1. Since Q_1 is lying over P_1, f descends to an integral extension $R/P_1 \to S/Q_1$ by proposition 2.7, so the lying over theorem applies. That is, there exists $\overline{Q}_2$ prime in S/Q_1 lying over the prime $\overline{P}_2$ in R/P_1. This lifts to a unique prime Q_2 in S.

To see that Q_2 is lying over P_2, observe that $R \to R/P_1 \to S/Q_1$ and $R \to S \to S/Q_1$ commute, so the preimages along either composition are equal. The first gives P_2 and the second gives $f^{-1}(Q_2)$. □

Proposition 2.11. Integral extensions preserve dimensions. That is, if $R \subset S$ is an integral extension of rings, then $\dim R = \dim S$.

Proof. Suppose $R \to S$ is an integral extension. Let $P_0 \lhd \cdots \lhd P_n$ be a strictly increasing chain of prime ideals in R. By the lying over theorem, there is a prime Q_0 lying over P_0, and now by the going up theorem, there is a strictly increasing chain of prime ideals $Q_0 \lhd \cdots \lhd Q_n$ in S. This shows that $\dim S \geq \dim R$.

Conversely, suppose $Q_0 \lhd \cdots \lhd Q_n$ is a strictly increasing chain of prime ideals in S. Then there is an increasing chain of prime ideals $f^{-1}(Q_0) \lhd \cdots \lhd f^{-1}(Q_n)$ in R. In fact, this chain is also *strictly* increasing, since in part 3 of the *lying over theorem* we showed that primes lying over a given prime in R have no non-trivial inclusions. □

2.3 The tilting of axes lemma

Suppose f is an irreducible polynomial in $k[x_1, \ldots, x_n][x_{n+1}]$. Then it is not true in general that the inclusion

$$k[x_1, \ldots, x_n] \to \frac{k[x_1, \ldots, x_n][x_{n+1}]}{(f)}$$

is finite. For example, consider $f(y) = xy - 1$ as a polynomial in $\mathbb{C}[x][y]$. However, finiteness is recovered if we perturb the basis, or "tilt the axes". In this example it corresponds to the observation that $\mathbb{C}[w] \to \mathbb{C}[w][z]/(g)$ is a finite extension, where $g(z) = w^2 - z^2 + 1$. Observe that g is really the same polynomial as f but with a tilted set of axes.

Proposition 2.12 (Tilting of axes lemma)**.** Let k be a field, and let $f \in B = k[x_1, \ldots, x_n]$ be non-constant. Then there exists a new set of coordinates $x'_1 \ldots x'_{n-1} \in B$ such that $f, x'_1, \ldots, x'_{n-1}$ are algebraically independent, and such that B is finite over $k[f, x'_1, \ldots, x'_{n-1}]$. In particular, $B/(f)$ is finite over $k[x'_1, \ldots, x'_{n-1}]$.

Proof. Let k be a field, and let $f \in B = k[x_1, \ldots, x_n]$ be non-constant. We prove that there exists a new set of coordinates $x'_1 \ldots x'_{n-1} \in B$ such that $f, x'_2, \ldots, x'_n$ are algebraically independent, and such that B is integral over $k[f, x'_2, \ldots, x'_n]$. Since integral finite-type extensions are finite by proposition 2.6, the first result will follow. (Note that the second result is then immediate.)

Let $f = \sum a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$ denote an element of B. For each monomial in f, there is a corresponding polynomial $p_j(t) = i_1 + i_2 t + \cdots i_n t^{n-1} \in \mathbb{Z}[t]$. For each distinct pair k, j, let $q_{kj}(t) = p_k(t) - p_j(t)$. Then there are finitely many polymonials q_{kj}, each of which has finitely many roots. Since the integers are infinite, there exists $d \in \mathbb{Z}$ such that $q_{kj}(d) \neq 0$ for any q_{kj}. That is, every $p_j(d)$ is distinct.

Now define $x_i' = x_i - x_1^{d^{i-1}}$ for $2 \leq i \leq n$. Then

$$f(x_1, x_2' + x_1^d, \ldots, x_n' + x_1^{d^{n-1}}) = f(x_1, \ldots, x_n) = f.$$

Expanding the expression on the left gives

$$f(x_1, x_2' + x_1^d, \ldots, x_n' + x_1^{d^{n-1}}) = \sum a_{i_1 \cdots i_n} x_1^{i_1 + \cdots + i_n d^{n-1}} + g(x_1, x_2', \ldots, x_n'),$$

where g has degree strictly less than the first term. This is because every coefficient in the expression in the sum is distinct by the choice of d, so no two terms in the sum have the same multi-degree, meaning each non-zero $a_{i_1 \cdots i_n}$ contributes a distinct non-zero term in the last expression. (This means the characteristic of k is irrelevant.) Viewing $f(x_1)$ as a polynomial in $k[x_2', \ldots, x_n'][x_1]$, it follows that $\alpha f(x_1)$ is monic for an appropriate $\alpha \neq 0$ in k. But now $\alpha f(x_1) - \alpha f = 0$ is an integral relation showing that x_1 is integral over $k[f, x_2', \ldots, x_n']$. Since $k[x_1, x_2', \ldots, x_n'] = k[x_1, \ldots, x_n]$, it follows that $k[x_1, \ldots, x_n]$ is integral over $k[f, x_2', \ldots, x_n']$ as required. □

2.4 The dimension of $k[x_1, \ldots, x_n]$

We are now ready to prove that $k[x_1, \ldots, x_n]$ has dimension n. This is a proof by induction, using the tilting of axes lemma and the result that integral extensions preserve dimension (proposition 2.11).

Theorem 2.13. *The dimension of $k[x_1, \ldots, x_n]$ is n.*

Proof. It's clear that $\dim k[x_1, \ldots, x_n] \geq n$ by considering the chain of prime ideas

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n).$$

Therefore we proceed by induction on n to show that $\dim k[x_1, \ldots, x_n] \leq n$. The base case is trivial, since k is a field. Now fix m, and suppose $\dim k[x_1, \ldots, x_m] = m$. Suppose for a contradiction that $\dim k[x_1, \ldots, x_{m+1}] > m + 1$, and let $P_0 \subset \cdots \subset P_s$ be a strictly increasing chain of prime ideals in $k[x_1, \ldots, x_{m+1}]$ with $s > m + 1$. Assume without loss of generality that $P_0 = 0$. Choose any non-zero element of P_1, and decompose it into irreducible factors. Since P_1 is prime, at least one of these factors f lies in P_1, so now consider the strictly increasing chain of primes

$$0 \subset (f) \subset \cdots \subset P_s.$$

Since f has degree at least 1, the *tilting of axes lemma* applies: there exists $x_1', \ldots, x_m'$ algebraically independent such that there is a finite (and hence integral) extension

$$k[x_1', \ldots, x_m'] \to \frac{k[x_1, \ldots, x_{m+1}]}{(f)}.$$

By the proposition that integral extensions preserve dimension and the inductive hypothesis, the right side has dimension m. But this is a contradiction, since the chain of primes $(f) \subset \cdots \subset P_s$ descends to a strictly increasing chain of prime ideals in $\frac{k[x_1, \ldots, x_m][x_{m+1}]}{(f)}$, of length $s > m + 1$. Therefore $\dim k[x_1, \ldots, x_n] \leq n$ for any n, as required. □

3 Various forms of the Nullstellensatz

3.1 Noether normalisation and Zariski's lemma

We are almost ready to prove the Nullstellensatz. In the previous section we showed that every integral finite-type ring homomorphism is finite. In the case of field extensions, it turns out that finite-type is equivalent to finite without even requiring integrality! This is *Zariski's lemma*, which is often simply referred to as Hilbert's weak Nullstellensatz.

To prove Zariski's lemma, we use the *Noether normalisation lemma* (which is another corollary of the tilting of axes lemma), and the fact that $\dim k[x_1, \ldots, x_n] = n$.

Theorem 3.1 (Noether normalisation lemma). *Let R be an integral domain, finite-type over a field k. Let $d = trdeg(K(R)/k)$. (Here $K(R)$ denotes the field of fractions of k.) Then there exists $x_1, \ldots, x_d$ algebraically independent in R such that $k[x_1, \ldots, x_d] \to R$ is a finite extension.*

Before proceeding with the proof, we describe the *transcendence degree* of a field extension. Let K/k be a field extension, i.e. suppose there is a ring homomorphism $f : k \to K$. Then the transcendence degree of K is the supremum of cardinalities of algebraically independent subsets of K over k. In particular, the transcendence degree of $k(a_1, \ldots, a_n)$ is at most n, and equal to n if and only if the a_i are algebraically independent over k.

Proof of Noether normalisation. Since R is finite-type over k, write $R = k[s_1, \ldots, s_n]$, where the s_i are not necessarily algebraically independent. Then $d = \mathrm{trdeg}(K(R)/k) \leq n$. We proceed by induction on n. If $d = n$, the result is immediate, since the s_i must be algebraically independent.

For the inductive step, suppose $d < n$, and suppose the result is true for all integral domains over k with generating sets of size less than n. For some prime ideal P, $R = k[y_1, \ldots, y_n]/P$. We use the tilting of axes lemma to express R as an integral extension of some $k[z_1, \ldots, z_{n-1}]/Q$, which is automatically finite over some $k[x_1, \ldots, x_d]$ by the inductive hypothesis.

Let f be any non-constant polynomial in P (which exists since the $s_1, \ldots, s_n$ are algebraically dependent). By the tilting of axes lemma, there exists $z_1, \ldots, z_{n-1} \in k[y_1, \ldots, y_n] = k[\overline{y}]$ such that f, z_i are algebraically independent, and $k[\overline{y}]/(f)$ is finite over $k[z_1, \ldots, z_{n-1}] = k[\overline{z}]$. In particular $k[\overline{y}]/P$ is finite over $k[\overline{z}]$. The kernel of the map $k[\overline{z}] \to k[\overline{y}]/P$ is a prime ideal Q, so there is a finite extension $k[\overline{z}]/Q \to k[\overline{y}]/P$. Since $k[\overline{z}]/Q$ is finite over $k[x_1, \ldots, x_d]$ by the inductive hypothesis, by transitivity it follows that $k[y_1, \ldots, y_n]/P$ is finite over $k[x_1, \ldots, x_d]$ as required. □

Theorem 3.2 (Zariski's lemma). *Suppose K is a field extension of k. If K is finite-type over k, then K is finite over k.*

Proof. Let K be a finite-type field extension of k. Then by the Noether normalisation lemma there exists $x_1, \ldots, x_d \in K$ such that $k[x_1, \ldots, x_d] \to K$ is a finite extension, and

$x_1, \dots, x_d$ are algebraically independent. If we can show that $d = 0$, (equivalently, if we show that K is algebraic over k), it follows that $k \to K$ is finite (which is Zariski's lemma).

To see this, recall from proposition 2.11 that integral extensions preserve dimensions, and observe that $k[x_1, \dots, x_d]$ has dimension d while K has dimension 0. This forces $d = 0$ as required. □

3.2 Hilbert's weak Nullstellensatz

Hilbert's weak Nullstellensatz states that maximal ideals in polynomial rings of dimension n correspond bijectively with points in n-dimensional affine space. Since quotients by maximal ideals give fields, this translates to a statement about field extensions, and in fact follows from Zariski's lemma.

Theorem 3.3 (Hilbert's weak Nullstellensatz, version 1)**.** *Let k be a field, and $M \subset k[x_1, \dots, x_n]$ a maximal ideal. Then $k[x_1, \dots, x_n]/M$ is a finite field extension of k. In particular, if k is algebraically closed, $k[x_1, \dots, x_n]/M \cong k$.*

Proof. The first part follows immediately from Zariski's lemma. The canonical map $k \to k[x_1, \dots, x_n]/M$ is not the zero map, since 1 cannot map into M. Therefore it must be injective. But $k \to k[x_1, \dots, x_n]/M$ is now a finite-type field extension, so by Zariski's lemma, it is a finite field extension.

Next suppose k is algebraically closed. Since every element of $k[x_1, \dots, x_n]/M$ is algebraic over k, it must be isomorphic to k. □

Theorem 3.4 (Hilbert's weak Nullstellensatz, version 2)**.** *Let k be an algebraically closed field. Then the maximal ideals of $k[x_1, \dots, x_n]$ are exactly of the form $(x_1 - a_1, \dots, x_n - a_n)$, for $a_i \in k$.*

Proof. First we observe that ideals of the form $(x_1 - a_1, \dots, x_n - a_n)$ are indeed maximal, since the quotients of $k[x_1, \dots, x_n]$ by such ideals gives k.

Conversely, suppose $M \subset k[x_1, \dots, x_n]$ is maximal. By the first form of the weak Nullstellensatz, $k[x_1, \dots, x_n]/M \cong k$. Each $x_i + M$ maps to some $a_i \in k$ under this isomorphism, so $x_i - a_i \in M$. But then $(x_1 - a_1, \dots, x_n - a_n) \subset M$ is a maximal ideal, so they must be equal. □

The second form of Hilbert's wek Nullstellensatz is a very geometric statement, as the ideal $(x_1 - a_1, \dots, x_n - a_n)$ consists of all polynomials which vanish at the point $(a_1, \dots, a_n) \in k^n$, so any point in k^n gives rise to a maximal ideal by considering the set of such polynomials.

3.3 Hilbert's strong Nullstellensatz

Hilbert's weak Nullstellensatz also implies what is often referred to as the strong Nullstellensatz, or just the Nullstellensatz. Rather than relating maximal ideals to geometry, this version of the Nullstellensatz relates all ideals to geometry.

Theorem 3.5 (Hilbert's strong Nullstellensatz)**.** *Let I be an ideal of $k[x_1, \ldots, x_n]$, where k is algebraically closed. Suppose $f \in k[x_1, \ldots, x_n]$ vanishes on the vanishing set of I. Then there exists $m \in \mathbb{N}$ such that $f^m \in I$.*

Proof. This follows from the *Rabinowitsch trick*. Let I be an ideal in $k[x_1, \ldots, x_n]$, and let $f \in k[x_1, \ldots, x_n]$. Since I is an ideal in a Noetherian ring, it is generated by $g_1, \ldots, g_m$. Suppose f vanishes on the vanishing set of I, which is equivalently the vanishing set of g. Consider the polynomial ring $k[x_1, \ldots, x_n, y]$, and define $f' \in k[x_1, \ldots, x_n, y]$ to be $f'(x_1, \ldots, y) = 1 - yf(x_1, \ldots, x_n)$. Then $\{f', g_1, \ldots, g_m\}$ has no common zeroes, since whenever all of $g_1, \ldots, g_m$ vanishes, f' takes the value 1. But by the weak Nullstellensatz, every maximal ideal vanishes at a point, so $(f', g_1, \ldots, g_m)$ generates the unit ideal.

Choose $h_0, \ldots, h_m \in k[x_1, \ldots, x_n, y]$ such that

$$1 = h_0 f' + \sum h_i g_i.$$

Since f is non-zero in $k[x_1, \ldots, x_n, y]$, $1/f \in k(x_1, \ldots, x_n)$. The evaluation $y \mapsto 1/f$ induces a homomorphism

$$k[x_1, \ldots, x_n, y] \to k(x_1, \ldots, x_n).$$

Under this map, the above expression maps to

$$\begin{aligned} 1 =& h_0(x_1, \ldots, x_n, 1/f)(1 - (1/f)f) + \sum h_i(x_1, \ldots, x_n, 1/f) g_i(x_1, \ldots, x_n) \\ =& \sum h_i(x_1, \ldots, x_n, 1/f) g_i(x_1, \ldots, x_n). \end{aligned}$$

Since each h_i is a polynomial, $1/f$ appears with finite degree finitely many times, so there exists $N \in \mathbb{N}$ such that f^N clears denominators. That is,

$$f^N = \sum f^N h_i(x_1, \ldots, x_n, 1/f) g_i(x_1, \ldots, x_n),$$

where the right side is a linear combination of $g_i(x_1, \ldots, x_n)$ with coefficients in $k[x_1, \ldots, x_n]$. This shows that $f^N \in I$ as required. □

The geometric content is that given an ideal J, it canonically carves out a geometric space in k^n, the *vanishing set of* J. This theorem states that this procedure is almost reversible: the collection of all polynomials vanishing on this space is itself an ideal of $k[x_1, \ldots, x_n]$, specifically the *radical of* J. Thus if $I(\Sigma)$ denotes the ideal of polynomials vanishing on $\Sigma \subset k^n$, and $V(J)$ denotes the set on which all polynomials in an ideal $J \lhd k[x_1, \ldots, x_n]$ vanish, the strong Nullstellensatz states that

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

In particular, a prime ideal is its own radical, so if P is prime then $I(V(P)) = P$.