Bridging Algebra and Geometry: Hilbert's Nullstellensatz

Timothy Cho

December 2023

Abstract

Hilbert's Nullstellensatz gives a bijection between a specific subset of polynomial ring ideals and geometric objects describable by algebraic equations. In this paper, we give intuition on this fundamental theorem through examples from both the algebraic and geometric viewpoints. We describe the concepts of *variety* and *ideal*, which are maps in opposing directions between the set of ideals in a polynomial ring over a field $k[x_1, \ldots, x_n]$ and the collection of subsets of k^n which are solutions to systems of polynomial equations. In this paper, we prove that the variety and ideal maps are invertible in one direction but not the other. However, we will state and prove Hilbert's Nullstellensatz, which shows that while this second direction is not fully invertible, we are, in an algebraically closed field k, able to restrict the domain of ideals in $k[x_1, \ldots, x_n]$ we discuss in order to get a useful bijection.

1. Introduction

Algebra arose from people finding ways to solve polynomial equations. Linear and quadratic polynomials were well-understood since antiquity, and polynomials of degrees 3 and 4 were the topic of intense study in 16th-century Europe [7]. In the same vein, the work of Niels Henrik Abel (1802-1829) and his contemporaries showed that there was no general solution in radicals to polynomial equations of degree at least 5. While it seemed as if this branch of algebra was "closed off" to further mathematical exploration, this work led to the development of rigorous abstract algebra.

We can continue to chase abstraction by considering *systems* of polynomial equations instead: given a set $S \subseteq k[x_1, \ldots, x_n]$, where k is a field, what is the common set of roots to every polynomial in S? The case that every $f \in S$ had degree 1 led to the modernization of linear algebra, from which arose our definitions of *vector spaces* and *subspaces*, which abstracted and generalized the visual notions of lines and planes that we are accustomed to in two- and three-dimensional Euclidean space.

This type of generalization is the heart of algebraic geometry: we ask for the common set of roots V given a set $S \subseteq k[x_1, \ldots, x_n]$, except now each $f \in S$ can take any degree. Moreover, we pose an inverse question: given a set of "solutions" $V \subseteq k^n$ (n-dimensional space over a field k), what are all of the polynomials that vanish on V? That is, we would like to encode spatial, geometric information as algebraic information (a set of polynomials), and vice versa. Algebraic geometry is the study of this "translation manual" between algebra and geometry; however, as with language, translation manuals could never produce a bijective correspondence. In many cases, two distinct sets of polynomials $S, T \subseteq k[x_1, \ldots, x_n]$ can share a vanishing set V. This is potentially disastrous; however, in 1893, David Hilbert (1862-1943) proved the Nullstellensatz in a paper on invariant theory, an area of mathematics closely related to modern algebraic geometry. The Nullstellensatz states that, in an algebraically closed field, the way objects are "lost in translation" is quite predictable: S and T as above are always essentially "synonymous" with each other, so that we can safely disregard a large portion of subsets of $k[x_1, \ldots, x_n]$ to get a useful bijection.

As such, algebraic geometry exploded over the 20th century — instead of a weak link between shapes and polynomials, the modernization of algebra along with the bridge of Hilbert's Nullstellensatz allowed mathematicians to express shapes through rigorously-defined rings and ideals. This partially allows us to do away with the need of visuals, in favor of abstraction and generalization. Thus, objects which may seem nonsensical, like a "curve" in $\mathbb{F}_9^2$ (2-dimensional space over the field of 9 elements), suddenly become meaningful, and even relevant. As a result, modern algebraic geometry continues to reveal previously-unseen connections between areas of mathematics, and today, algebraic geometry intersects with almost every branch of mathematics that is studied [6].

To give an example of a problem solved by algebraic geometry, one need not consider further than Fermat's Last Theorem, which states that there do not exist positive integers a, b, c such that $a^n + b^n = c^n$, where $n \geq 3$. This conjecture is ostensibly not very geometric. However, by building off of work in algebraic geometry and number theory, Andrew Wiles (1953-) converted the problem into a statement about curves and successfully proved the conjecture in 1994. More generally, ideas in number theory are usually represented algebraically, but algebraic geometry provides useful alternative viewpoints.

In Section 2, we provide the ring theoretic background needed for the proof of the Nullstellensatz. In Section 3, we introduce the *variety* and *ideal*, the two main objects of study in algebraic geometry, and we provide examples and graphs for certain varieties (Example 3.3). We also note a few basic propositions about varieties and ideals, and suggest that they are nearly mutually inverse. Finally, in Section 4, we build towards a proof of Hilbert's Nullstellensatz (Theorem 4.11) via Noether's Normalization Lemma (Theorem 4.8) and applying Rabinowitsch's Trick from the so-called "weak" form of the Nullstellensatz (Theorem 4.10).

2. Algebraic Preliminaries

All rings in this paper are unital and commutative, so all ideals are automatically two-sided. Also, if R is a ring and $I \subseteq R$ is an ideal, for clarity we will write $I \trianglelefteq R$ in lieu of $I \subseteq R$. Finally, whenever we have an inclusion of rings $R \leq S$, we will assume $1_R = 1_S$.

We start by generalizing the familiar concept of roots of polynomials.

Definition 2.1. Let R be a ring, and let $f \in R[x_1, \ldots, x_n]$. A *root* of f is an n-tuple $a = (a_1, \ldots, a_n) \in R^n$ such that $f(a) = f(a_1, \ldots, a_n) = 0$.

If $R = k$ is a field, then any $f \in k[x]$ has at most $\deg f$ distinct roots, so the set of roots of f is finite. However, our next example demonstrates that root-finding is far more interesting in multiple variables.

Example 2.2. Let $f(x) := (x^2+4y^2-4)^2 \in \mathbb{R}[x, y]$, and let V be the set of roots of f. If $a := (x, y) \in V \subseteq \mathbb{R}^2$, then $f(a) = 0$ if and only if $x^2 + 4y^2 = 4$. Hence, $V = \{(x, y) \in \mathbb{R}^2 : x^2 + 4y^2 = 4\}$. To gain a geometric perspective, we divide by 4 go obtain $(x/2)^2 + y^2 = 1$. Hence, we can visualize V is an ellipse centered at the origin, with semimajor axis 2 and semiminor axis 1:

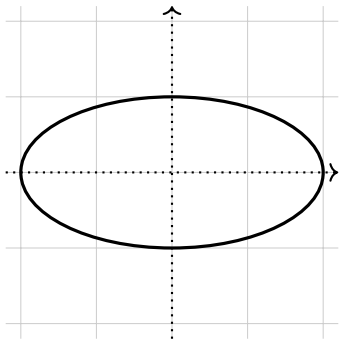


Figure 1: $V = \{(x, y) : x^2 + 4y^2 = 4\}$.

From the previous example, we expect that it is usually the case that multivariate polynomials have infinite sets of roots. Now, we pose an related question central to algebraic geometry: given a polynomial ring $k[x_1, \ldots, x_n]$ and a set $V \subseteq k^n$, how do we easily describe the set of polynomials that share V as a common set of roots? The language of rings and ideals will do nicely here. However, to understand an ideal, we should understand its generating set. Hence, we introduce the definition below.

Definition 2.3. A ring R is *Noetherian* if every ideal $I \trianglelefteq R$ is finitely generated.

Example 2.4. The ring $\mathbb{Z}$ is a PID. Hence, $\mathbb{Z}$ is Noetherian, as every ideal $I \trianglelefteq \mathbb{Z}$ is generated by one element.

The next result, proved by Hilbert in 1890, allows us to quickly see if a polynomial ring is Noetherian.

Theorem 2.5 (Hilbert Basis Theorem)**.** *Let R be a ring. If R is Noetherian, so is $R[x]$.*

See [3, Theorem 3.11] for a proof in full detail; we provide a sketch below.

Proof Sketch. Suppose R is Noetherian. If $I \trianglelefteq R[x]$ is an ideal, we find that J, the set of all leading coefficients of polynomials in I, is an ideal of R. Let $J = \langle A \rangle$, where $|A| < \infty$. Now, for each $a \in A$, select a polynomial $g \in I$ with leading coefficient a, and let $G \subseteq R[x]$ be the set of all such g's chosen. By finiteness, G has a polynomial of maximal degree k.

Now, for each degree $i \leq k$, let $J_i \trianglelefteq R$ be the ideal consisting of the leading coefficients of polynomials in I with degree at most i. Hence for each $i \leq k$, pick a finite generating set A_i with $J_i = \langle A_i \rangle$, and pick G_i similar to above. Define $I_0 := \langle G, G_0, G_1, \ldots, G_k \rangle \trianglelefteq R[x]$. By construction, I_0 is finitely generated, and $I_0 \subseteq I$. To show that $I \subseteq I_0$, suppose for contradiction that there exists some $f \in I \setminus I_0$ of minimal degree. From here, casework on the degree of f shows a contradiction, so $I = I_0$; hence $R[x]$ is Noetherian. •

By induction, we have the following corollary.

Corollary 2.6. *Let R be a ring. If R is Noetherian, so is $R[x_1, \ldots, x_n]$.*

Hence, all of the rings we will encounter in this paper will be Noetherian. An important example of a non-Noetherian ring would be a polynomial ring $R[x_1, x_2, \ldots]$, with infinitely many indeterminates x_i, but we will not consider it in this paper except in this short comment.

Our next definition will occur frequently in the examples of Section 3, and it is used in the statement of Hilbert's Nullstellensatz (Theorem 4.11).

Definition 2.7. Let R be a ring and $I \trianglelefteq R$. The *radical of I* is the set

$$\sqrt{I} := \left\{ r \in R : r^n \in I \text{ for some } n \in \mathbb{Z}^+ \right\}.$$

Similarly, $I \trianglelefteq R$ *is radical* if $I = \sqrt{I}$.

Informally, $\sqrt{I}$ is the set of all "nth roots" of elements of $I \trianglelefteq R$. It is readily checked that $I \subseteq \sqrt{I}$, and with some work one can show $\sqrt{I} \trianglelefteq R$. Although computing radicals given an arbitrary I is usually not an easy task, it is manageable if I is principal. We give two examples.

Example 2.8. Let $I := \left\langle (x^2 + 4y^2 - 4)^2 \right\rangle \trianglelefteq \mathbb{Z}[x, y]$. If $f \in \sqrt{I}$, then $f^n \in \left\langle (x^2 + 4y^2 - 4)^2 \right\rangle$ for some $n \in \mathbb{Z}^+$. Observe that $x^2 + 4y^2 - 4 \in \sqrt{I}$. Moreover, we can check that $x^2 + 4y^2 - 4$ is irreducible, so we claim that $\sqrt{I} = \left\langle x^2 + 4y^2 - 4 \right\rangle$. Indeed, if $f \in \left\langle x^2 + 4y^2 - 4 \right\rangle$, then $f = g(x, y)(x^2 + 4y^2 - 4)$ for some $g(x, y) \in \mathbb{Z}[x, y]$, so that $f^2 = g(x, y)^2 (x^2 + 4y^2 - 4)^2 \in I$. Hence $f \in \sqrt{I}$ and $\left\langle x^2 + 4y^2 - 4 \right\rangle \subseteq \sqrt{I}$.

For the reverse inclusion, fix $f \in \sqrt{I}$, so there exists some $n \in \mathbb{Z}^+$ such that $f^n \in I$. Taking V as defined in Example 2.2, we see that f^n vanishes on V. But this is only possible if $x^2 + 4y^2 = 4$, so that f has an irreducible factor of $x^2 + 4y^2 - 4$. Hence $f \in \left\langle x^2 + 4y^2 - 4 \right\rangle$, so $\sqrt{I} = \left\langle x^2 + 4y^2 - 4 \right\rangle$.

Example 2.9. We give a example of a radical $I \trianglelefteq \mathbb{Z}[x]$. Let $I := \left\langle x^2 - 2x + 2 \right\rangle \trianglelefteq \mathbb{Z}[x]$. If $f \in \sqrt{I}$, then $f^n \in \left\langle x^2 - 2x + 2 \right\rangle$ for some $n \in \mathbb{Z}^+$. However, $x^2 - 2x + 2$ is quadratic and has no integer roots, so it is irreducible. Thus, we claim $\sqrt{I} = \left\langle x^2 - 2x + 2 \right\rangle = I$, and the proof of this is similar to the argument in the previous example.

From above, notice that since the polynomial $x^2 - 2x + 2$ is irreducible, $\left\langle x^2 - 2x + 2 \right\rangle$ is a prime ideal. However, we also saw that the ideal was radical, and this is in fact true in general: when $I \trianglelefteq R$ is prime, no work is needed to assert $\sqrt{I} = I$.

Proposition 2.10. *Prime ideals are radical.*

Proof. Let R be a ring and $I \trianglelefteq R$ be prime. We know $I \subseteq \sqrt{I}$, so fix $r \in \sqrt{I}$. By well-ordering, there exists some *minimal* $n \in \mathbb{Z}^+$ such that $r^n \in I$. If $n = 1$, we are done, so suppose $n \geq 2$. Write $r^n = r r^{n-1}$, but because I is prime, $r \in I$ or $r^{n-1} \in I$. Assume $r \notin I$. Then $r^{n-1} \in I$, but this violates the minimality of n, a contradiction. Hence $r \in I$, so $\sqrt{I} \subseteq I$ and thus $I = \sqrt{I}$. □

Finally, we review two basic definitions from ring theory. The first of these is related to the various notions of *integrality* we will see in Definition 4.3, which we will use to prove the Nullstellensatz.

Definition 2.11. Let $R \leq S$ be an inclusion of rings. An element $s \in S$ is *algebraic* over R if s is the root of some $f(x) \in R[x]$. If $s \in S$ is not algebraic, then s is *transcendental* over R.

Although we give a generalized definition here, we will be purely discussing algebraicity over integral domains, rather than arbitrary rings.

Our final definition is a critical assumption needed for Hilbert's Nullstellensatz to hold.

Definition 2.12. A field k is *algebraically closed* if every non-constant polynomial $f \in k[x]$ has a root in k.

3. A Geometric Perspective

With our algebraic tools in place, we return to our main discussion on polynomial roots. Recall the set V from Example 2.2, which described an ellipse in $\mathbb{R}^2$. Before we give a general definition, we first examine a simpler example: visualizing the roots of a polynomial in one variable.

Example 3.1. The set of roots V of $x^4 - 5x^2 + 4 \in \mathbb{R}[x]$ is $\{\pm 1, \pm 2\}$. On the real number line, we visualize V as follows:

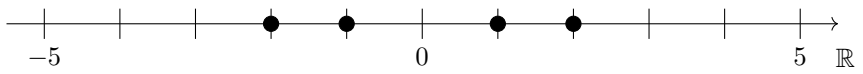


Figure 2: A one-dimensional algebraic variety.

Figure 2 above is a very simple example of an *algebraic variety*, which, informally, is the "visualization" of the roots of a polynomial, or of a set of polynomials. Varieties are profoundly boring in one dimension: given any $f \in k[x]$ (where k is a field), the variety of f has at most $\deg f < \infty$ points. However, our discussion will focus on polynomials in multiple variables; hence, we give our main, general definition below.

Definition 3.2. Let k be a field and $S \subseteq k[x_1, \ldots, x_n]$. The *affine algebraic variety of* S is the set of common roots of all of the polynomials in S:

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

Similarly, $V \subseteq k^n$ is an *algebraic set* if $V = \mathbb{V}(S)$ for some $S \subseteq k[x_1, \ldots, x_n]$.

We note that there are other types of varieties beyond affine varieties; see [6]. However, in the scope of this paper, all varieties will be affine, so we write "variety" when we mean "affine algebraic variety."

Example 3.3. The following are examples of varieties.

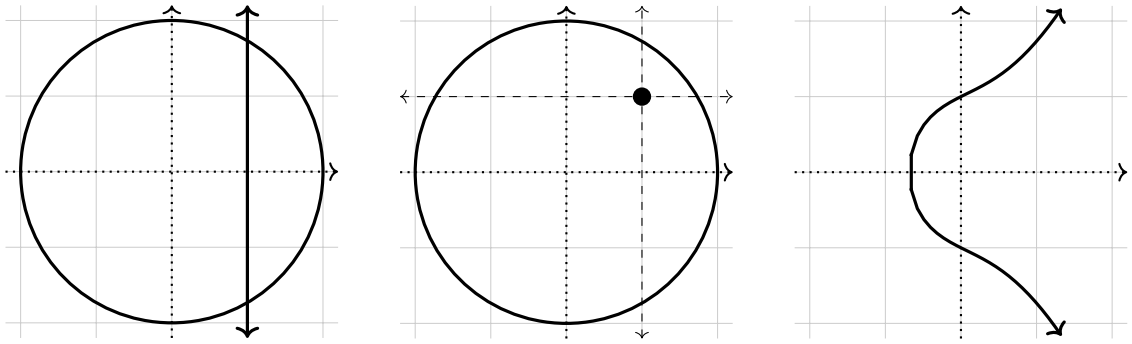
1. In Example 2.2, we found that in $\mathbb{R}^2$, $\mathbb{V}\left((x^2 + 4y^2 - 4)^2\right)$ is an ellipse.[1]
2. Let $f(x, y) := x^2 + y^2 - 4$ and $g(x, y) := x - 1$, where both polynomials are viewed as being in $\mathbb{R}[x, y]$. Then $\mathbb{V}(fg)$ is the set $\{(x, y) : (x^2 + y^2 - 4)(x - 1) = 0\}$, which consists of the circle centered at the origin of radius 2 and the vertical line $x = 1$. We also see that $\mathbb{V}(fg) = \mathbb{V}(f) \cup \mathbb{V}(g)$: the visualization for this is found in Figure 3a.
3. Let f, g be as above, and let $h(x, y) := y - 1$. Then $\mathbb{V}(fg, fh)$ is the set of points in $\mathbb{R}^2$ that vanish on both fg and fh; which, by solving a system of equations, we see that $\mathbb{V}(fg, fh)$ consists of the point $(1, 1)$ and the circle centered at the origin of radius 2. Notice that this is precisely the intersection $\mathbb{V}(fg, fh) = \mathbb{V}(fg) \cap \mathbb{V}(fh)$: see Figure 3b.

[1] We dropped the set brackets in the notation here for convenience — we do this whenever it does not cause confusion.

4. Any point in $\mathbb{R}^3$ can be viewed as an algebraic variety. Indeed, if $(a,b,c) \in \mathbb{R}^3$, then $\{(a,b,c)\} = \mathbb{V}(x-a, y-b, z-c)$. Generalizing this, if k is any field, then any point in k^n is viewable as an algebraic variety: if $(a_1,\ldots,a_n) \in k^n$, then $\{(a_1,\ldots,a_n)\} = \mathbb{V}\left(\{x_i - a_i\}_{i=1}^n\right)$.

5. Generalizing the previous point, if k is a field, we can show that any finite subset of k^n is an algebraic set. This is similar to the one-dimensional case we discussed in Example 3.1.

6. An *elliptic curve* in $\mathbb{R}^2$ is a set of points satisfying the equation $y^2 = x^3 + ax + b$ for some $a, b \in \mathbb{R}$, where $4a^3 + 27b^2 \neq 0$. It is easy to see that if C is an elliptic curve, then $C = \mathbb{V}(x^3 - y^2 + ax + b)$. Elliptic curves are important in number theory, cryptography, as well as many other branches of mathematics. Andrew Wiles applied the theory of elliptic curves, which rests on algebraic geometry, to prove Fermat's Last Theorem [6]. An example of an elliptic curve is given in Figure 3c.



(a) $\mathbb{V}\left[(x^2+y^2-4)(x-1)\right]$ (b) $\mathbb{V}(fg, fh) = \mathbb{V}(fg) \cap \mathbb{V}(fh)$ (c) $\mathbb{V}(x^3 - y^2 + x + 1)$

Figure 3: Various algebraic varieties as described in Examples 3.3(2), (3), and (6).

Our reasoning in Examples 3.3(2) and (3) can be generalized into the proof of the following proposition, which we exclude for brevity.

Proposition 3.4. *Let k be a field and $S, T \subseteq k[x_1,\ldots,x_n]$. Then $\mathbb{V}(S) \cup \mathbb{V}(T) = \mathbb{V}(ST)$, and $\mathbb{V}(S) \cap \mathbb{V}(T) = \mathbb{V}(S \cup T)$, where $ST := \{f \cdot g : f \in S, g \in T\}$.*

Remark 3.5. From Proposition 3.4, we should be quick to notice that the operation of "taking the variety" flips the inclusion: if $S \subseteq T$, then $\mathbb{V}(S \cup T) = \mathbb{V}(T) = \mathbb{V}(S) \cap \mathbb{V}(T)$, which implies $\mathbb{V}(T) \subseteq \mathbb{V}(S)$. This is consistent with our intuitions, as it should be more "difficult" for a point in k^n to be a common zero for a larger set of polynomials T compared to a smaller set S. As such, we mention here that unsurprisingly, we will see that the bijection of Hilbert's Nullstellensatz also flips the inclusion.

As we have seen, varieties convert lists of polynomials into subsets of k^n. However, it is natural to consider the dual notion: given a subset $V \subseteq k^n$, what is the *set of polynomials* that vanish on all of V?

Example 3.6. Refer back to Example 3.1, where we found the roots of $x^4 - 5x^2 + 4 \in \mathbb{R}[x]$. However, we now fix the set of roots $V = \{\pm 1, \pm 2\}$, and ask for the set of all polynomials that vanish on V. We know that $f(x) := x^4 - 5x^2 + 4$ vanishes on V, but more generally, if $g \in \mathbb{R}[x]$, then fg also vanishes on V, though it may vanish on more roots than just the four listed in V. However, it is clear that the polynomials in $\left\langle x^4 - 5x^2 + 4 \right\rangle \trianglelefteq \mathbb{R}[x]$ all vanish on *at least* V.

This motivates our next definition.

Definition 3.7. Let k be a field, and let $V \subseteq k^n$. The *ideal of V* is the set of all polynomials in $k[x_1,\ldots,x_n]$ that vanish on all of V:

$$\mathbb{I}(V) := \{f \in k[x_1,\ldots,x_n] : f(a) = 0 \text{ for all } a \in V\}.$$

Immediately, we should notice a similarity between Definitions 3.2 and 3.7: all we have done was switch the roles of $k[x_1, \ldots, x_n]$ and k^n, in a manner we will make precise with Proposition 4.2 and the Nullstellensatz (Theorem 4.11). For now, it is relatively safe to conjecture that due to this role exchange, the operations $\mathbb{V}$ and $\mathbb{I}$ are mutually inverse. We view a two-dimensional example of an ideal.

Example 3.8. With respect to Example 2.2, let $V = \{(x, y) : x^2 + 4y^2 = 4\} \subseteq \mathbb{R}^2$. Then $\mathbb{I}(V)$ is the set of polynomials in $\mathbb{R}[x, y]$ that vanish on V. Clearly, $x^2 + 4y^2 - 4 \in \mathbb{I}(V)$, and if $f \in \mathbb{R}[x, y]$ is any polynomial, $f(x, y)(x^2 + 4y^2 - 4) \in \mathbb{I}(V)$. Hence, given this "absorption property," we claim that $\mathbb{I}(V) = \langle x^2 + 4y^2 - 4 \rangle$. We have demonstrated the inclusion $\mathbb{I}(V) \supseteq \langle x^2 + 4y^2 - 4 \rangle$ above. If $\mathbb{I}(V) \not\subseteq \langle x^2 + 4y^2 - 4 \rangle$, there exists a polynomial $f \in \mathbb{I}(V) \setminus \langle x^2 + 4y^2 - 4 \rangle$. Now, f vanishes on V, so $f(x, y)$ must satisfy $x^2 + 4y^2 = 4$. If $(x^2 + 4y^2 - 4) \mid f$, this shows $f \in \langle x^2 + 4y^2 - 4 \rangle$, so we assume $f \mid (x^2 + 4y^2 - 4)$, so $\deg f = 1$. However, we can check that $x^2 + 4y^2 - 4$ is irreducible, so such an f cannot exist. Hence $\mathbb{I}(V) = \langle x^2 + 4y^2 - 4 \rangle$.

In the example above, $\mathbb{I}(V)$ was actually an ideal in the ring-theoretic sense. Indeed, it is for this reason that mathematicians chose the name "ideal" for this subset:

Proposition 3.9. *Let k be a field and $V \subseteq k^n$. Then $\mathbb{I}(V) \trianglelefteq k[x_1, \ldots, x_n]$.*

Proof. By definition, $\mathbb{I}(V) \subseteq k[x_1, \ldots, x_n]$. Take $f, g \in \mathbb{I}(V)$, and fix $a \in V$. Then $f(a) = g(a) = 0$, so $(f - g)(a) = f(a) - g(a) = 0$, so $f - g \in \mathbb{I}(V)$. Hence, $(\mathbb{I}(V), +) \leq (k[x_1, \ldots, x_n], +)$. Now, we check the absorption property. Take $f \in \mathbb{I}(V)$, $r \in k[x_1, \ldots, x_n]$, and fix $a \in V$. Since $f(a) = 0$, it follows that $rf(a) = r(a) \cdot f(a) = r(a) \cdot 0 = 0$, so $rf \in \mathbb{I}(V)$. Hence $\mathbb{I}(V)$ is an ideal. □

Though we did not see an example of this, we have the following analogue to Proposition 3.4 and Remark 3.5 for ideals, with a very similar proof.

Proposition 3.10. *Let k be a field and $V, W \subseteq k^n$. Then $\mathbb{I}(V) \cap \mathbb{I}(W) = \mathbb{I}(V \cup W)$. Moreover, if $V \subseteq W$, then $\mathbb{I}(W) \subseteq \mathbb{I}(V)$.*

Proof. That $\mathbb{I}(V) \cap \mathbb{I}(W) = \mathbb{I}(V \cup W)$ follows from the definition of $\mathbb{I}$. Now, suppose $V \subseteq W$. Then $\mathbb{I}(W) = \mathbb{I}(V \cup W) = \mathbb{I}(V) \cap \mathbb{I}(W)$, which implies $\mathbb{I}(W) \subseteq \mathbb{I}(V)$. □

The above proposition shows that "taking the ideal" also reverses the inclusion, giving us more justification into believing that $\mathbb{V}$ and $\mathbb{I}$ are mutually inverse. If indeed this is true, then $\mathbb{V}$ and $\mathbb{I}$ will define a bijection from the set of ideals in $k[x_1, \ldots, x_n]$ to algebraic subsets of k^n.

4. Proof of the Nullstellensatz

In the previous section, we expected the operations $\mathbb{V}$ and $\mathbb{I}$ to be inverses of each other. More formally, for any $I \trianglelefteq k[x_1, \ldots, x_n]$ and $V \subseteq k^n$, we conjectured $\mathbb{I}(\mathbb{V}(I)) = I$ and $\mathbb{V}(\mathbb{I}(V)) = V$. However, our next example demonstrates that this is *nearly* the case: $\mathbb{I}(\mathbb{V}(I)) \neq I$ but $\mathbb{V}(\mathbb{I}(V)) = V$. Then, we will build to a proof of the Nullstellensatz, which gives as a "restriction" in which $\mathbb{I}$ and $\mathbb{V}$ are truly inverses. The sequence of propositions in this section is given in [2], and we refer the reader to [1] for an alternate path.

Example 4.1. Combining Examples 2.2, 2.8, and 3.8, we see that if $V = \{(x, y) : x^2 + 4y^2 = 4\}$ and $I = \langle (x^2 + 4y^2 - 4)^2 \rangle$, then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I} \neq I$. But $\mathbb{I}(V) = \langle x^2 + 4y^2 - 4 \rangle$, and since $x^2 + 4y^2 - 4$ is irreducible, we see that $\mathbb{V}(\mathbb{I}(V)) = \mathbb{V}\left(\langle x^2 + 4y^2 - 4 \rangle\right) = V$.

There are two important equalities in the preceding example. The first is $\mathbb{V}(\mathbb{I}(V)) = V$, which holds for any *algebraic set* V, as we will show in the next proposition. The other is $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$: this is Hilbert's Nullstellensatz, *as long as* we consider I to be an ideal in $\mathbb{C}[x, y]$.

Proposition 4.2 (Backward Nullstellensatz)**.** *Let k be a field, and let $V \subseteq k^n$ be an algebraic set. Then $\mathbb{V}(\mathbb{I}(V)) = V$.*

Proof. Take $a \in V$. Then $\mathbb{I}(V)$ is the set of polynomials that vanish on all of V, and thus a. Now, take any $f \in \mathbb{I}(V)$. Then $f(a) = 0$, so this implies $a \in \mathbb{V}(\mathbb{I}(V))$, so that $V \subseteq \mathbb{V}(\mathbb{I}(V))$.

Conversely, take $a \in \mathbb{V}(\mathbb{I}(V))$. Then for every $f \in \mathbb{I}(V)$, we have $f(a) = 0$. However, V is an algebraic set, so $V = \mathbb{V}(S)$ for some $S \in k[x_1, \ldots, x_n]$. If $S \subseteq \mathbb{I}(V)$, then we are done, as $\mathbb{V}(\mathbb{I}(V)) \subseteq \mathbb{V}(S) = V$ by Remark 3.5. Hence, assume for contradiction that $S \not\subseteq \mathbb{I}(V)$, so we can take some $f \in S \setminus \mathbb{I}(V)$. Then $f(a) = 0$, but both f and a were arbitrary, so that $f \in \mathbb{I}(V)$: f vanishes at every $a \in V$. This is a contradiction, so we must have $S \subseteq \mathbb{I}(V)$, so we are done. □

Now, we build the proof for the "forward" Nullstellensatz. The proof is far more involved than that of Proposition 4.2, so we need a few more definitions to assist us.

Definition 4.3. Let $R \leq S$ be an extension of rings. An element $s \in S$ is *integral over* R if s is the a root of a monic polynomial in $R[x]$. The set of elements of S that are integral over R is the *integral closure of* R, and if S is the integral closure over R, then S is an *integral extension of* R. In particular, if R is an integral domain, the *normalization* of R is the integral closure of R inside its field of fractions.

Of course, if $s \in S$ is integral over R, then s is algebraic over R. We view some examples.

Example 4.4. Consider the extension of integral domains $\mathbb{Z} \leq \mathbb{Q}$. The following are true:

1. The rational number $\frac{5}{2}$ is *not* integral over $\mathbb{Z}$, as there does not exist a monic polynomial $f \in \mathbb{Z}[x]$ such that $f\left(\frac{5}{2}\right) = 0$. However, we see that $\frac{5}{2}$ *is* integral over $\mathbb{Q}$ itself, as it is the root of $x - \frac{5}{2} \in \mathbb{Q}[x]$.
2. Generalizing (1), we see that the integral closure in $\mathbb{Q}$ of $\mathbb{Z}$ is just $\mathbb{Z}$ itself. Phrased differently, the normalization of $\mathbb{Z}$ is $\mathbb{Z}$ itself.
3. However, $\sqrt{3} \in \mathbb{R}$ is integral over both $\mathbb{Z}$ and $\mathbb{Q}$, as it is a root of $x^2 - 3 \in \mathbb{Z}[x] \leq \mathbb{Q}[x]$.

We will be dealing with fields and field extensions in the proof of the Nullstellensatz, so we hope that integrality "plays nicely" with field extensions. Luckily, the following proposition guarantees this.

Proposition 4.5. *Let $R \leq S$ be an integral extension. If S is an integral domain, then R is a field if and only if S is a field.*

Proof. Let $R \leq S$ be an integral extension, where S is an integral domain.

Suppose R is a field, and fix $s \in S$. We show that s has an inverse. Since s is integral over R, let $p(x) := a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in R[x]$ be the minimal polynomial for s, so $a_0 \in R \setminus \{0\}$ and $p(a) = 0$. Rearranging, we see that $s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1) = -a_0$, and since R is a field, we divide by $-a_0$ to obtain

$$\frac{s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1}{-a_0} \cdot s = 1,$$

so we have found an inverse for s. Hence S is a field.

Conversely, suppose S is a field, and let $r \in R \setminus \{0\} \subseteq S$. We know $r^{-1} \in S$, so it suffices to show $r^{-1} \in R$. By assumption, $s := r^{-1} \in S$ is integral over R, so there exist $a_0, \ldots, a_{n-1} \in R$ such that $s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0$. But multiplying through by r^{n-1} and noting $s = r^{-1}$, we observe that $r^{-1} + a_{n-1}r^0 + \cdots + a_0 r^{n-1} = 0$, so $r^{-1} = -(a_{n-1} + \cdots + a_0 r^{n-1}) \in R$ by closure. Hence R is a field. □

Next, we generalize the notion of polynomial rings. We first state what it means for R to be *generated* by a field k and some elements $r_1, \ldots r_n$, even if the r_i are not necessarily indeterminates.

Definition 4.6. Let R be a ring and k be a field. If $k \leq R$, then R is a *k-algebra.* Furthermore, R is a *finitely generated k-algebra* if R is generated by k, together with some finite set $\{r_1, \ldots, r_n\} \subseteq R$.

If k is a field, then the polynomial ring $R := k[x_1, \ldots, x_n]$ is a finitely generated k-algebra: indeed, $k \leq k[x_1, \ldots, x_n]$, and R is generated by k and the elements $\{x_1, \ldots, x_n\}$. It is also the "freest" possible k-algebra, in that a finitely generated k-algebra $k[r_1, \ldots, r_n]$ is similar[2] to a polynomial ring in n variables, but the "pseudo-indeterminates" r_i may or may not satisfy non-trivial polynomial relations with each other. That is, there may or may not be some $f \in k[x_1, \ldots, x_n]$ such that $f(r_1, \ldots, r_n) = 0$, so that we may "solve for" one of the r_i in terms of the others (even if implicitly). Our next definition, along with Theorem 4.8, makes this idea precise.

[2]More precisely, there is a canonical homomorphism $\varphi : k[x_1, \ldots, x_n] \to k[r_1, \ldots, r_n]$ by $x_i \mapsto r_i$.

Definition 4.7. Let k be a field and R be a k-algebra. The elements $y_1, \ldots, y_q \in R$ are *algebraically independent over* k if there is no nonzero polynomial $f \in k[x_1, \ldots, x_q]$ such that $f(y_1, \ldots, y_q) = 0$. Equivalently, $y_1, \ldots, y_q$ are algebraically independent if $k[y_1, \ldots, y_q]$ is isomorphic to the polynomial ring $k[x_1, \ldots, x_q]$.

The next theorem tells us that, given a finitely generated k-algebra $R = k[r_1, \ldots, r_n]$, we can view R as an integral extension of a polynomial ring in $q \leq n$ variables. In other words, R can be viewed as a normalization of a polynomial ring, hence the name of the theorem below.

Theorem 4.8 (Noether's Normalization Lemma)**.** *Let k be a field. If $R = k[r_1, \ldots, r_n]$ is a finitely generated k-algebra, then for some $q \leq n$, there exist algebraically independent elements $y_1, \ldots, y_q \in R$ such that R is integral over $k[y_1, \ldots, y_q]$.*

The following proof sketch is adopted from [2] and [4], which the reader can consult for the details we excluded for brevity.

Proof Sketch. We induct on n, and note that the case $n = 0$ is trivial. Assume the induction hypothesis, pick $R := k[r_1, \ldots, r_n]$, and assume that the r_i are not algebraically independent. Then, pick a nonzero polynomial $f \in k[x_1, \ldots, x_n]$ such that $f(r_1, \ldots, r_n) = 0$. By defining integers α_i and new indeterminates $X_i := x_i - x_n^{\alpha_i}$, we view f as a polynomial in the ring $k[X_1, \ldots, X_{n-1}, x_n]$. By tediously comparing f and its representation in the new ring (call it g) term by term, we establish that, via an appropriate choice of the α_i, that g has a leading term cx_n^N, where $N := \deg g$. Then $\frac{1}{c}g$ is a monic polynomial, and by defining $s_i = r_i - r_n^{\alpha_i}$ (thus applying the same shift to the indeterminates x_i to the elements r_i), we see

$$\frac{1}{c}g(s_1, \ldots, s_{n-1}, r_n) = \frac{1}{c}f(r_1, \ldots, r_n) = 0,$$

so r_n is integral over $S := k[s_1, \ldots, s_{n-1}]$. Now, we can show that each r_i, $i \leq n-1$, is integral over $S[r_n]$, so by transitivity of integrality,[3] we apply our inductive hypothesis and finish the proof. •

We immediately have a nice corollary.

Corollary 4.9 (Zariski's Lemma)**.** *Let $k \leq K$ be an extension of fields. If K is a finitely-generated k-algebra, then K is algebraic over k; that is, every element $\alpha \in K$ is algebraic over k.*

Proof. Let $K = k[r_1, \ldots, r_n]$. By Theorem 4.8, we see that K is integral over some $k[y_1, \ldots, y_q]$, for $0 \leq q \leq n$, where the y_i are algebraically independent. However, since the y_i are algebraically independent, $k[y_1, \ldots, y_q] \cong k[x_1, \ldots, x_q]$, where the x_i are indeterminates. By Proposition 4.5, $k[y_1, \ldots, y_q]$ and $k[x_1, \ldots, x_q]$ are fields, but this is impossible unless $q = 0$. Hence K is integral, thus algebraic, over k. □

We remark that although the next theorem is canonically labeled "weak," it and Theorem 4.11 imply each other; see [6]. Note the *algebraically closed* condition: this is crucial for the theorem to hold!

Theorem 4.10 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. Then $M \trianglelefteq k[x_1, \ldots, x_n]$ is maximal if and only if $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for $a_i \in K$. This defines a bijection between the sets*

$$k^n \longleftrightarrow \{\underline{\textit{maximal}} \textit{ ideals in } k[x_1, \ldots, x_n]\},$$

where the left-to-right direction is given by $\mathbb{I}$, and the right-to-left direction is given by $\mathbb{V}$.

Proof. Notice that $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is certainly a maximal ideal in $k[x_1, \ldots, x_n]$, as we see $k[x_1, \ldots, x_n]/M \cong k(a_1, \ldots, a_n) = k$, which by assumption is a field.

Now, let k be algebraically closed and $M \trianglelefteq k[x_1, \ldots, x_n]$ be maximal. Then $E := k[x_1, \ldots, x_n]/M$ is (isomorphic to) a field extension of k, and notice that E is generated by the cosets $x_i + M$, for $i = 1, 2, \ldots n$. Hence E is a finitely generated k-algebra, so Corollary 4.9 applies and E is *algebraic* over k. However, k is algebraically closed, so $E \cong k$. It follows that each coset $x_i + M$ corresponds to some $a_i \in k$, so $x_i - a_i \in M$. Hence $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq M$, but the first of these ideals is maximal, so $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

[3] We take this for granted, but readers with basic experience in module theory should check [2, p. 692-693].

We now accomplish our goal of stating and proving Hilbert's Nullstellensatz. The proof we present below is adopted from mathematician J.L. Rabinowitsch's[4] one-page paper [5], which contains a trick that shortens the proof substantially: introducing a new variable. It has been said that no one else can improve upon the "Rabinowitsch trick" [1], due to its relative simplicity.

Theorem 4.11 (Hilbert's Nullstellensatz)**.** *If k is an algebraically closed field and $I \trianglelefteq k[x_1, \ldots, x_n]$, then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$. Equivalently, there is a bijection between the sets*

$$\Big\{\textit{algebraic subsets of } k^n\Big\} \longleftrightarrow \Big\{\underline{\textit{radical}} \textit{ ideals in } k[x_, \ldots, x_n]\Big\},$$

where the left-to-right direction is given by $\mathbb{I}$, and the right-to-left direction is given by $\mathbb{V}$.

Proof. Let $f \in \sqrt{I}$. Then there exists some $n \in \mathbb{Z}^+$ such that $f^n \in I$, so we know that f^n vanishes on $\mathbb{V}(I)$. But this is only possible if f vanishes on $\mathbb{V}(I)$, which implies $f \in \mathbb{I}(\mathbb{V}(I))$, so $\sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(I))$.

Now, we show $\mathbb{I}(\mathbb{V}(I)) \subseteq \sqrt{I}$. Since $I \trianglelefteq k[x_1, \ldots, x_n]$, Corollary 2.6 applies and $I = \langle f_1, \ldots, f_m \rangle$ for some $m \in \mathbb{Z}^+$ and appropriate f_i. Now, pick some $g \in \mathbb{I}(\mathbb{V}(I))$, and introduce the *new* indeterminate x_0. Consider the new ideal $I' := \langle f_1, \ldots, f_m, x_0 g - 1\rangle \trianglelefteq k[x_0, x_1, \ldots, x_n]$. If $f_1, \ldots, f_m$ vanish at a point $a := (a_0, a_1, \ldots, a_n) \in k^{n+1}$, then so must g, as $a \in \mathbb{V}(I)$, and we picked $g \in \mathbb{I}(\mathbb{V}(I))$. This implies that $x_0 g - 1$ is nonzero at a, so we have forced $\mathbb{V}(I') = \varnothing$: none of the generators of I' are zero simultaneously. Because k is algebraically closed, we can invoke Theorem 4.10 to see that I' is certainly not maximal, but in view of Proposition 3.4 and Remark 3.5, I' is improper: $I' = k^{n+1}$. This implies $1 \in I'$, so by definition of I' there exist polynomials $p_i \in k[x_0, x_1, \ldots, x_n]$, $i = 0, 1, \ldots, m$, such that

$$1 = p_0 \cdot (x_0 g - 1) + \sum_{i=1}^{m} p_i \cdot f_i. \tag{1}$$

At this point, we reveal Rabinowitsch's swindle: since x_0 is an indeterminate, (1) holds even if x_0 were replaced.[5] We take $x_0 := 1/g$. Writing $p_i = p_i(x_0, x_1, \ldots, x_n) \in k[x_0, x_1, \ldots, x_n]$, we observe

$$1 = p_0 \cdot \left(\frac{1}{g} g - 1\right) + \sum_{i=1}^{m} p_i\left(\frac{1}{g}, x_1, \ldots, x_n\right) \cdot f_i = \sum_{i=1}^{m} p_i\left(\frac{1}{g}, x_1, \ldots, x_n\right) \cdot f_i. \tag{2}$$

Now by construction, each $p_i(1/g, x_1, \ldots, x_n)$ can be written in the form $p_i = a_i / g^{\ell_i}$, where $a_i \in k[x_1, \ldots, x_n]$ and $\ell_i \in \mathbb{Z}^+$. Take $M := \max\{\ell_1, \ldots, \ell_m\}$ to clear denominators: multiplying both sides of (2) by g^M gives $g^M = \sum_{i=1}^{m} b_i f_i \in I$, where $b_i := g^M a_i$. But this means $g \in \sqrt{I}$, so $\sqrt{I} \supseteq \mathbb{I}(\mathbb{V}(I))$, so we are done. □

In service of the fact that the *algebraically closed* condition played a critical role in the proof of the Nullstellensatz, our final example presents a failure of the theorem over the real numbers, which are not algebraically closed.

Example 4.12. The ideal of the empty set in $\mathbb{R}[x]$ is $\mathbb{I}(\varnothing) = \mathbb{R}[x]$, as every $f \in \mathbb{R}[x]$ vacuously shares $\varnothing$ as a set of common roots. But $\varnothing$ is an algebraic set, satisfying $\varnothing = \mathbb{V}(x^2 + k) \in \mathbb{R}[x]$ for any $k > 0$. If we define $I_k := \langle x^2 + k \rangle \trianglelefteq \mathbb{R}[x]$ for each $k > 0$, then each I_k is a distinct prime ideal, so Proposition 2.10 tells us that $I_k = \sqrt{I_k}$. Now $\mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\varnothing) = \mathbb{R}[x] \neq \sqrt{I_k}$, and there are uncountably many such ideals I_k. Hence, Hilbert's Nullstellensatz fails over $\mathbb{R}$.

In view of our final example, most algebraic geometers work over $\mathbb{C}$, which is in contrast to this paper, where we built intuition by working over $\mathbb{R}$. To gain a "feel" for some variety $\mathbb{V}(S) \subseteq \mathbb{C}^2$, for example, many authors draw $\mathbb{V}(S) \cap \mathbb{R}^2$ for obvious reasons (see [6]), but it is understood that the vast majority of varieties reside within an algebraically closed field. Algebraic geometry is still possible over non-algebraically closed fields, but the problem of non-invertibility leads to complications due to the lack of an efficient Nullstellensatz.

[4] *Rabinowitsch* was likely a pseudonym of mathematical physicist G.Y. Rainich (1886-1968), but this claim is disputed.

[5] Formally, we are using are "outsourcing" everything via an evaluation homomorphism.

References

[1] Daniel Allcock. "Hilbert's Nullstellensatz". Expository notes on webpage at `https://web.ma.utexas.edu/users/allcock/expos/nullstellensatz3.pdf`. Jan. 2005.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.

[3] Marc Maliar. *A Bottom-up Approach to Hilbert's Basis Theorem*. 2021. arXiv: `2110.08958 [math.AG]`.

[4] David Mumford. *The Red Book of Varieties and Schemes*. expanded. Vol. 1358. Lecture Notes in Mathematics. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello. Springer-Verlag, Berlin, 1999, pp. x+306. ISBN: 3-540-63293-X. DOI: `10.1007/b62130`. URL: `https://doi.org/10.1007/b62130`.

[5] J. L. Rabinowitsch. "Zum Hilbertschen Nullstellensatz". German. In: *Math. Ann.* 102.1 (1930), p. 520. ISSN: 0025-5831. DOI: `10.1007/BF01782361`. URL: `https://doi.org/10.1007/BF01782361`.

[6] Karen E. Smith et al. *An Invitation to Algebraic Geometry*. Universitext. Springer-Verlag, New York, 2000, pp. xii+155. ISBN: 0-387-98980-3. DOI: `10.1007/978-1-4757-4497-2`. URL: `https://doi.org/10.1007/978-1-4757-4497-2`.

[7] Bartel L. Waerden. *A History of Algebra*. Springer-Verlag, Berlin, 1985, pp. xi+274. ISBN: 978-3-642-51599-6. DOI: `10.1007/978-3-642-51599-6`. URL: `https://doi.org/10.1007/978-3-642-51599-6`.