Hilbert's Nullstellensatz and Syzygy Theorems

Nicholas Biglin

October 25, 2024

1 Introduction

1.1 Motivation

Hilbert's Nullstellensatz is very important for many reasons, but chief among them are the following 2:

1. It provides a vast generalization of the fundamental theorem of algebra and the theorem on consistency of linear systems

2. It provides a concrete connection between geometric objects (affine varieties) and algebraic objects (ideals in rings). This is a very important basis for algebraic geometry

1.2 History

- David Hilbert was one of the most important and influential mathematicians of the twentieth century

- In many ways he set the course of mathematics for the twentieth century (axiomatization of geometry, embracing Cantor's set theory, etc.)

- He was considered a "universalist" in that he contributed widely to most areas of mathematics at the time

- This presentation will pick up where the last one left off and consider some of his other important results related to invariant theory and algebraic geometry

[6]

1.3 Mathematical Preliminaries: Definitions

- Affine Space: K^n with no structure for some field K (i.e. just points in K with n coordinates)

- Zero Set: For an ideal of polynomials $J \in K[x_1, ..., x-n]$, $V(J) := \{(a_1, ..., a_n) \in K^n | f(a) = 0 \forall f \in J\}$
- Ideal of subset of Affine Space: For $X \subseteq K^n, I(X) := \{f \in K[x_1, ..., x_n] | f(x) = 0 \forall x \in X\}$
- Noetherian Ring: A ring such that every ascending chain of ideals eventually stabilizes (there is a maximal ideal in the chain)
- Algebra: A vectorspace with (bilinear) multiplication defined between vectors

Note that Algebraic Varieties are "essentially" zero sets, though their modern definition has been generalized. However, we will use them as zero sets.

Example of Zero Set: For $x^2 + 1 \in \mathbb{C}[x], \pm i$ is its zero set

Example of Ideal: For $i \in \mathbb{C}, I(i) = (x - i)$ (the ideal generated by (x-i)).

1.4 Mathematical Preliminaries: Results

Definition: Maximal Ideal: In a ring R an ideal m is maximal if $\nexists m'$ such that m' is a proper ideal containing m (i.e. $\nexists m'$ st $m \subsetneq m' \subsetneq R$)

Theorem: For a ring R and an ideal m, m is maximal if and only if R/m is a field

2 Nullstellensatz

Noether Normalization is an important algebraic result en route to the Nullstellensatz. In addition to that, it has important geometric consequences in its own right.

2.1 Introductory Concepts for Noether Normalization

Finitely generated Algebra vs Finite Algebra:

Suppose A is an algebra over B. Then A is

finitely generated over B if $\exists a_1, ..., a_n \in A$ st $A = B[a_1, ..., a_n]$

a finite algebra over B if $\exists a_1, ..., a_n \in A$ st $A = a_1 B + ... + a_n B$

Example of finitely generated but not finite algebra:

For a ring R consider R[x]. This is a finitely generated algebra (we just append x), but it is not a finite algebra, as suppose we could write it finitely: $y_1 R + ... + y_m R$. Choose $N = \max \deg(y_i)$. Then consider $x^{N+1} \notin y_1 R + ... + y_m R$. So we cannot have $R[x] = y_1 R + ... + y_m R$

2.2 Statement of Noether Normalization

Theorem: Suppose K is a field. Let $A = K[a_1, ..., a_n]$ be a finitely generated K-algebra. Then $\exists y_1, ..., y_m \in A, m \leq n$ st:

1. $y_1, ..., y_m$ are algebraically independent over K ($\nexists 0 \not\equiv f \in K[x_1, ..., x_n]$ st $f(y_1, ..., y_m) = 0$)

2. A is a finite $K[y_1, ..., y_m]$ algebra

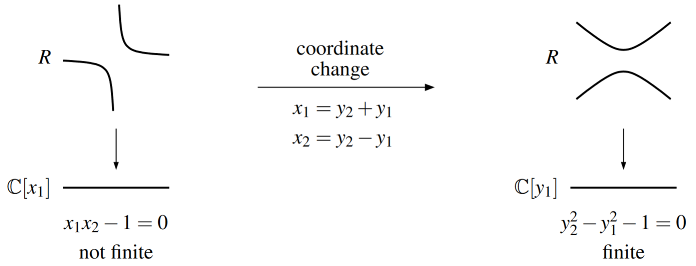
   i.e. If $B = K[y_1, ..., y_m]$ then $A = c_1B + ... + c_lB$ for some $c_i \in A$

Essentially this theorem tells us ”finite extensions of polynomial rings are relatively easy to deal with.”

2.3 Geometric Interpretation of Noether Normalization

Noether normalization considers algebraic sets as (finite) covers of Affine Space

Example:



[4]

”Algebraic sets are covers of Affine Space.” We can get an includsion (via a finite extension) of $K[x_1, ..., x_m]$ into an Algebraic Set A, and the variety associated with A projects surjectively onto the linear space associated with $K[x_1, ..., x_m]$

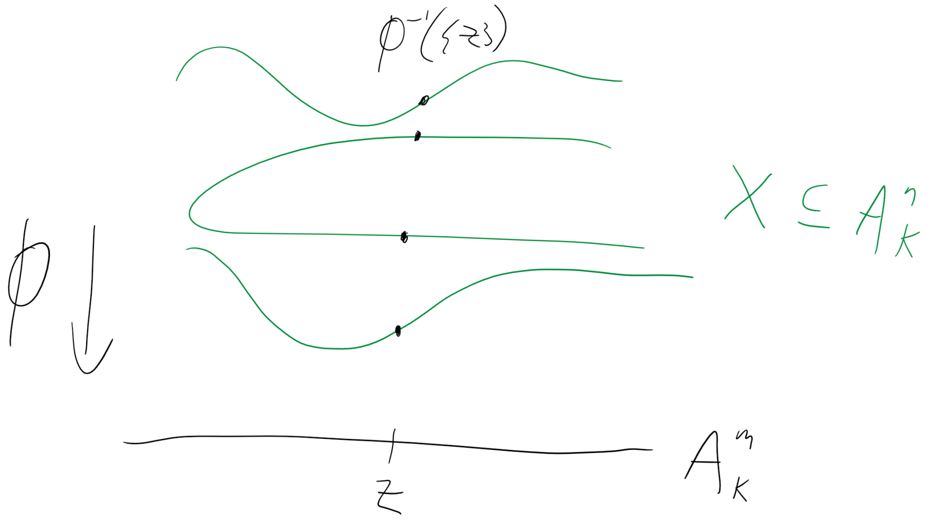
More formally, let X be a variety in K^n, and assume X is irreducible.

Consider $A = K[a_1, ..., a_n] = K[x_1, ..., x_n]/I(X)$ $(a_i = x_i \mod I)$.

Then $\exists$ algebraically independent $y_1, ..., y_m$ st A is a finite $K[y_1, ..., y_m]$ algebra.

Then we can define a projection (i.e. surjective map) $\phi : X \to K^m$ st $\forall z \in K^m, \phi^{-1}(\{z\})$ is finite

Pictorally (simple model):



2.4 The Nullstellensatz Formally Stated

Theorem: Let K be algebraically closed, $A = K[x_1, ..., x_n]$. Then:

1. Every maximal ideal m in A is of the form $m = (x_1 - a_1, ..., x_n - a_n) = I(P), P \in K^n$

2. If $J \subsetneq A$ is a proper ideal, then V(J)=0

   Equivalently, any set of polynomials $f_1, ..., f_m \in K[x_1, ..., x_n]$ has a common zero unless $\exists g_1, ..., g_m \in K[x_1, ..., x_n]$ st $g_1 f_1 + ... + g_m f_m = 1$

3. For every ideal $J \subseteq A, I(V(J)) = \sqrt{J}$

   That is, $f(x_1, ..., x_n) = 0 \forall (x_1, ..., x_n) \in V(J) \subseteq K^n \iff f^r \in J$ for some $r \in \mathbb{N}$

(3) can be phrased of as: "The set of all polynomials that vanish on the points that vanish on all polynomials in J is the radical of J, that is, all the polynomials that, when raised to some power, are in J"

Significance:

Condition (2) is a vast generalization of the Fundamental Theorem of Algebra and the theorem on consistency of linear systems

Condition (1) is an explicit connection between Algebra and Geometry: Maximal ideals in polynomial rings (Algebra) are in correspondence with points in Affine Space (geometry)

(In general, ideals correspond to subsets of Affine Space, which is a corollary)

This Theorem forms the backbone for much of modern algebraic geometry, and has a great many consequences.

2.5 Nullstellensatz Proof Ingredients

Theorem: Let K be an infinite field and $A = K[a_1, ..., a_n]$ a finitely generated K-Algebra. If A is also a field, then A is algebraic over K (any element in A is a root of polynomials over K).

This theorem given follows from Noether Normalization. It requires some other algebraic results, so we shall not prove it.

Recall: R/m is a field if and only if m is a maximal ideal.

Recall: Every proper ideal in a Noetherian ring is contained in some maximal ideal.

2.6 Proof of the Nullstellensatz

1.

i. We begin by proving $(x_1 - a_1, ..., x_n - a_n)$ is maximal

Consider the evaluation map $\phi_P : K[x_1, ..., x_n] \to K, f \mapsto f(P), P \in K^n$

By a simple coordinate change we take $a_1 = a_2 = ... = a_n = 0$

Then we get that $K[x_1,...,x_n]/(x_1,...,x_n) \cong K$

This is intuitive (we are just removing all the nonconstant terms) but also we can see this through an application of the first isomorphism theorem: $f \in \ker\phi \iff f(0,...,0) = 0 \iff c_f = 0$ where c_f is the constant term in f. So The kernel is all polynomials without constant terms. Then we also note that we can get any element in K by choosing c_f appropriately for some f (e.g. just consider all the constant functions for each element in K). Then by the first isomorphism theorem we get $K[x_1,...,x_n]/(x_1,...,x_n) \cong K$.

ii. Now we will prove that any maximal ideal is of the form $(x_1 - a_1,...,x_n - a_n)$.

Assume m is a maximal ideal in $K[x_1,...,x_n]$. Then $\tilde{K} = K[x_1,...,x_n]/m$ is a field. We also have that $\tilde{K}$ is a finitely generated K algebra, as it can be realized as $\tilde{K} = K[[x_1],...,[x_n]]$ where each $[x_i] = x_i \mod m$. So (by the theorem given to us by Noether Normalization) $\tilde{K}$ is algebraic over K. But K is algebraically closed, so $\tilde{K} = K$.

Then consider the isomorphism $\phi : K \hookrightarrow K[x_1,...,x_n] \xrightarrow{\pi} K[x_1,...,x_n]/m = \tilde{K}$

Consider $a_i = \phi^{-1}([x_i])$. We note that $\pi(x_i - a_i) = [x_i] - [x_i] = 0 \implies x_i - a_i \in \ker\pi \ \forall i \in \{1,...,n\}$.But note also $\ker\pi = m$

So we must have that $(x_1 - a_1,...,x_n - a_n) \subseteq m$. But the first term is maximal (by part i) hence we must get that $(x_1 - a_1,...,x_n - a_n) = m$

2. 1 $\implies$ 2

Suppose $J \subsetneq A = K[x_1,...,x_n]$ is a proper ideal. Then $K[x_1,...,x_n]$ is Noetherian $\implies \exists$ a maximal ideal m st $J \subseteq m$

By 1, we have $m = I(P)$ for some $P \in K^n$

Then $\{P\} = V(I(P)) \subseteq V(J) \implies V(J) \neq \emptyset$

Note V(I(P)) is "all points that vanish on the ideal generated by polynomials that vanish at the point P," hence it is trivially P.

Since J is a subset of I(P), it has less polynomials in it. Think of this as having "less constraints." That is to say, at the very least all the polynomials in J vanish at P, but they could vanish at more points. Hence the subset in the above, and thus the nonemptyness of V(J).

3. 2 $\implies$ 3

This will be proved with something called the Rabinowitsch trick, whereby we will introduce an additional variable (thus meaning we work in a new polynomial ring) and do some algebraic trickery before eventually returning to our original polynomial ring.

If you don't like proofs that rely simply on algebraic dark magic, then I apologize, you will not enjoy this proof. Nevertheless, it is related to localization.

Let $J = (f_1,...,f_m) \subseteq K[x_1,...,x_n], f \in V(J)$

Consider the ideal $(f_1,...,f_m, 1 - tf) \in K[x_1,...,x_m,t]$ for t a new variable (thus we have moved into a new polynomial ring.

Since f vanishes at all the points where all the f_i simultaneously vanish, this new ideal has no zeros (because wherever the first m vanish, 1-tf becomes 1, not 0). Hence, by the above, it generates the unit ideal.

So this tells us $\exists g_1, ..., g_m, g \in K[x_1, ..., x_n, t]$ such that

$$g \cdot (1 - tf) + \sum_{i=1}^{m} g_i \cdot f_i = 1 \in K$$

Now t is just a variable, so equality will hold for all substitutions we make. So let us substitute $t = \frac{1}{f(x_1,...,x_n)}$. Note that when we make this substitution, we now move into the field of fractions (AKA field of rational functions) $K(x_1, ..., x_n)$, since we now have x_i terms in the denominator. Thus we get:

$$g \cdot (1 - \frac{1}{f} \cdot f) + \sum_{i=1}^{m} g_i(x_1, ..., x_n, \frac{1}{f(x_1, ..., x_n)}) \cdot f_i(x_1, ..., x_n, \frac{1}{f(x_1, ..., x_n)}))$$

$$= \sum_{i=1}^{m} g_i(x_1, ..., x_n, \frac{1}{f(x_1, ..., x_n)}) \cdot f_i(x_1, ..., x_n, \frac{1}{f(x_1, ..., x_n)})) = 1$$

Now note that the only expressions in the denominator of the terms in the bottom line are $f(x_1, ..., x_n)^{l_i}$ for some exponent l_i, so we can rewrite these all as polynomials using some common denominator $r = \text{lcm}(l_i)$. Hence we get

$$1 = \sum_{i=1}^{m} \frac{h_i(x_1, ..., x_n) \cdot f_i(x_1, ..., x_n)}{f(x_1, ..., x_n)^r}$$

Then by simply multiplying out the denominator we get $f^r = \sum_{i=1}^{m} h_i \cdot f_i$ where now all of terms are back in $K[x_1, ..., x_n]$.

Note now that $\sum_{i=1}^{m} h_i \cdot f_i \in J \implies f^r \in J$.

But this tells us that any polynomial that vanishes on the points on which all the polynomials in J vanish is in the radical of J. That is $V(J) = \sqrt{J}$. So we're done!

2.7 Immediate Corollaries of Nullstellensatz

Corollary 1.17. *For $A = k[x_1, \dots, x_n]$, the maps V and I*

$$\{\textit{ideals of } A\} \xleftrightarrow{V,I} \{\textit{subsets of } \mathbb{A}_k^n\}$$

induce the following bijections:

$$\begin{array}{ccc}
\{\textit{radical ideals of } A\} & \xleftrightarrow{1:1} & \{\textit{subvarieties of } \mathbb{A}_k^n\} \\
\cup & & \cup \\
\{\textit{prime ideals of } A\} & \xleftrightarrow{1:1} & \{\textit{irreducible subvarieties of } \mathbb{A}_k^n\} \\
\cup & & \cup \\
\{\textit{maximal ideals of } A\} & \xleftrightarrow{1:1} & \{\textit{points of } \mathbb{A}_k^n\}.
\end{array}$$

[5]

2.8 Nullstellensatz Example

Consider $f(x,y) = 8x+5y-3, g(x,y) = 2xy+5+4x, h(x,y) = 4xy-5y+14$. We can see that f-2g+h=1. Therefore the ideal generated by these polynomials has an empty zero set.

2.9 A Note on Philosophy of Proof

It's interesting to note that Hilbert's original proof was controversial and not immediately widely accepted due to the fact that it was nonconstructive; it didn't tell you how to find the zero set of the ideal.

This is a good reminder that mathematical proofs are fundamentally sociological constructions, they depend on the shared agreement of the mathematical community. We like to think of mathematical proofs as expressing a form of ultimate truth, that once we deriving something from the axioms it's immutably true, but this isn't an accurate description of reality.

This isn't just a problem fo the past. For a modern incarnation of this same problem, consider Mochizuki's claimed proof of the abc conjecture.

3 The Syzygy Theorem

3.1 Pre-Syzygy: Modules

The Syzygy theorem primarily concerns modules and their generators.

Think of modules as generalizations of vector spaces, but instead of being over fields they're over rings.

Vector spaces have bases, modules have generators which may not be independent.

Free module: A module with a basis (i.e. linearly independent generators).

We will mostly work with the free module $R^n = R \times ... \times R$ for some ring R, which is analogous to the vectorspace K^n for some field K.

3.2 Syzygys

Definition: A module M is said to be finitely generated over a ring R if $\exists z_1, ..., z_n \in M$ st $\forall x \in M, x = m_1r_1 + ... + m_nr_n,$ for $r_i \in R$

The z_i are the generators of M

Definition: A syzygy is a set of $(a_1, ..., a_n \in R^n$ st $a_1z_1 + ... + a_nz_n = 0$ for the z_i generators of a finitely generated module M over R.

Proposition: A syzygy is a submodule of R^n

We can encode syzygys as kernels of maps from free modules. This is best illustrated by example

Example of Syzygys as Kernels:[7]

Consider $I = (x^2, xy)$ as a module over $\mathbb{Z}/n[x,y] = R$ (ideals are modules over their rings).

Consider the map $\phi_0 : R^2 \to I, e_1 \mapsto x^2, e_2 \mapsto xy$. Here e_1, e_2 are analogous to their vectorspace counterparts (i.e. $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and vice versa for e_2).

Clearly ϕ_0 is surjective. Note however we have a nontrivial kernel. Indeed, $\ker \phi_0 = (\begin{bmatrix} -y \\ x \end{bmatrix})$ since $(-y)x^2 + x(xy) = 0$. Let us encode this within another map.

Consider $\phi_1 : R \to R^2, 1 \mapsto \begin{bmatrix} -y \\ x \end{bmatrix}$. Thus we have $\mathrm{im}\phi_1 = \ker \phi_0$.

Thus we have an exact sequence (called a free resolution):

$$0 \to R \xrightarrow{\phi_1} R^2 \xrightarrow{\phi_0} M \to 0$$

A natural question to ask is if this sequence always terminates, or is it possible to keep going to the left, keep getting more syzygys of syzygys of syzygys and so on.

3.3 Syzygy Theorem

Theorem: Let $R = K[x_1, ..., x_n]$. Then every finitely generated R module has a free resolution of length $\leq n$.

3.4 Example of Syzygys Applied

The Syzygy Theorem is an important theorem for solving problems in invariant theory. It is now considered an early result in homological algebra (the exact sequence given above may have caused you to recall the homology introduced by Tony in a previous week).

Here is an example, taken from Richard Borcherds (more examples in his video)[2]

Consider the group $A_n \subseteq S_n$ acting on $\mathbb{C}[x_1, ..., x_n]$, where every permutation acts by permuting the factors of x_i. We want to consider the polynomials invariant under all permutations.

Note that, by definition, all elementary symmetric polynomials are invariant. In addition, we get that $\Delta = \prod_{i<j}(x_i - x_j)$ is invariant under all elements in A_n. Then we have that Δ is not independent from the elementary symmetric functions e_i. In the case of n=2, this relationship can be displayed as follows:

$\Delta^2 = e_1^2 - 4e_2$. Hopefully this looks vaguely familiar from the discriminant of a quadratic: $\Delta^2 = b^2 - 4ac$.

Then we get that the ring of invariant polynomials under A_n is generated by $e_1, ..., e_n, \Delta$ with a syzygy as defined above.

4 References

References

[1] URL: wikipedia.org.

[2] Richard E. Borcherds. *Commutative algebra 3 (What is a syzygy?)* URL: https://www.youtube.com/watch?v=RYPt7kGdo7s.

[3] *Explain like I'm 5: Hilbert's Nullstellensatz.* URL: https://www.reddit.com/r/math/comments/pdfcl/explain_like_im_5_hilberts_nullstellensatz/.

[4] Andreas Gathman. *Commutative Algebra Class Notes.* URL: https://agag-gathmann.math.rptu.de/class/commalg-2013/commalg-2013.pdf.

[5] Klaus Hulek. *Elementary Algebraic Geometry.* American Mathematical Society, 2000.

[6] David Lewis. "David Hilbert and the Theory of Algebraic Invariants". In: *IMS Bulletin* (1994).

[7] Rodin Salman. "Hilbert's Syzygy Theorem". PhD thesis. Utrecht University, 2021.

[8] Unknown. *Hilbert.* URL: https://commons.wikimedia.org/w/index.php?curid=36302.

[9] *What does Noether's Normalization lemma even mean?* URL: https://math.stackexchange.com/questions/1472631/what-does-noethers-normalization-lemma-even-mean.

[10] Roger Wiegand. "What is... a Syzygy?" In: *Notices of AMS* (2006).