> Algebra is the offer made by the devil to the mathematician. The devil says: "I will give you this powerful machine, and it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvellous machine." . . . the danger to our soul is there, because when you pass over into algebraic calculation, essentially you stop thinking: you stop thinking geometrically, you stop thinking about the meaning. (Sir Michael Atiyah)

1 Introduction

It is with this provocative quote that we begin our discussion: indeed, algebra provides a powerful tool by which we can study, well, geometry. In particular, our goal here will be to furnish a proof of Hilbert's Nullstellensatz, which essentially states that there is a one-to-one correspondence between geometric objects (varieties) to ideals of polynomial rings. Thus if we want to study geometry, we turn to this powerful machine that is algebra. . . . Some of the following material is based on [Artin, 2011], but the primary references were [Reid, 2013] and [Smith et al., 2000], with [Aluffi, 2009] as well. But first, we'll discuss a baby version of our end goal.

Proposition 1.1. *Let F be a field. The maximal ideals of $F[x]$ are the principal ideals generated by the monic irreducible polynomials.*

Proof. Hey, we proved this in February 17, 2022 lecture! (in particular, $F[x]$ is a PID). ■

Corollary 1.2. *There is a bijective correspondence between the maximal ideals of $\mathbb{C}[x]$ and points in $\mathbb{C}$. The maximal ideal M_a that corresponds to a point $a \in \mathbb{C}$ is the kernel of the substitution homomorphism which sends x to a. Indeed, $M_a = \langle x - a \rangle$.*

Proof. The kernel of the substitution homomorphism is all polynomials which have a as a root. So, they must be divisible by $x - a$, and $M_a = \langle x - a \rangle$. On the other hand, if M is a maximal ideal of $\mathbb{C}[x]$, then by Proposition 1.1 we know M is generated by the monic irreducible polynomials of $\mathbb{C}[x]$, which are simply $x - a$. ■

2 Affine Algebraic Sets

Definition 2.1. Suppose $\{f_i\}_{i \in I}$ is an indexed collection, not necessarily finite or countable, of polynomials. The common zero set

$$\mathbb{V}(\{f_i\}_{i \in I}) \coloneqq \{x \in \mathbb{C}^n \mid f_i(x) = 0 \text{ for all } i \in I\}$$

is called an **affine algebraic set**.

Example 2.2. By definition, a complex line in $\mathbb{C}^2$ is made of the solutions to the equation $ax + by + c = 0$, so it is an affine algebraic set. Similarly, the point (a, b) is an affine algebraic set since it is the common solution of the equations $x - a$ and $y - b$. The empty set is the solution of the constant function, $\varnothing = \mathbb{V}(1)$, and the whole space is the solution of the constant function $\mathbb{C}^2 = \mathbb{V}(0)$, and so are both affine algebraic sets.

Example 2.3. We can identify $\mathrm{Mat}_{n \times n}(\mathbb{C})$ with $\mathbb{C}^{n \times n}$. $\det : \mathrm{Mat}_{n \times n} \to \mathbb{C}$ is a polynomial function, and so

$$SL(n, \mathbb{C}) = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{C}) \mid \det A - 1 = 0\}$$

is an affine algebraic set.

Remark 2.4. Note that in the standard Euclidean topology for $\mathbb{C}^n$, every polynomial is continuous; hence for any polynomial p, $p^{-1}(\{0\})$ is closed since a singleton is closed in the standard topology. Then every affine algebraic set is an intersection of closed sets, and thus is closed. This discussion shows that $GL(n, \mathbb{C})$, which is not closed, is not an affine algebraic set for all n.

3 Hilbert's Basis Theorem

Definition 3.1 (Noetherian Ring)**.** We say that a ring R is **Noetherian** if every ideal $I \lhd R$ is finitely generated; that is, if $I \lhd R$, then there exists $f_1, \dots, f_k \in I$ such that $I = \langle f_1, \dots, f_k \rangle$.

Proposition 3.2. *Let R be a ring. The following are equivalent:*

(i) R *is Noetherian.*

(ii) R *satisfies the ascending chain condition (a.c.c): if $I_1 \subseteq I_2 \subseteq \cdots$ is an increasing chain of ideals, then the chain terminates; that is, there exists an n such that $I_{n-1} \subseteq I_n = I_{n+1} = \cdots$.*

(iii) Every nonempty collection of ideals of R has a maximal element ordered by inclusion.

Proof. ((i) $\Rightarrow$ (ii)) Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and set $I \coloneqq \bigcup_{j \in \mathbb{N}} I_j$. This is an ideal by Homework 1, and so it is finitely generated, say $I = \langle f_1, \dots, f_k \rangle$. Then each f_i must be in some I_{m_i} for some m_i, and take $m \coloneqq \max\{m_i \mid 1 \leqslant i \leqslant k\}$, we have that $I = I_m$, and so the chain terminates after m.

((ii) $\Rightarrow$ (iii)) For the contrapositive, suppose that R has a family $\mathcal{F}$ of ideals without a maximal element. Then pick $I_1 \in \mathcal{F}$; since this is not a maximal element, then there exists an $I_2 \in \mathcal{F}$ such that $I_1 \subset I_2$ a proper inclusion. Now inductively we may define, for $I_n \in \mathcal{F}$, an $I_{n+1} \in \mathcal{F}$ such that $I_n \subset I_{n+1}$ since I_n is not maximal in $\mathcal{F}$; then we have an ascending chain $I_1 \subset I_2 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots$ that does not terminate.

((iii) $\Rightarrow$ (i)) Let $I \lhd R$ be an ideal, and let $\mathcal{F} = \{J \subseteq I \mid J \text{ is a finitely generated ideal}\}$. Then certainly $\{0\} \in \mathcal{F}$ so $\mathcal{F} \neq \varnothing$. Thus $\mathcal{F}$ must have a maximal element by inclusion, call it M. Then $M = I$, since if not, there is an element $f \in I \setminus M$, and $M + Rf$ must be another finitely generated element which strictly contains M, a contradiction. ∎

Example 3.3. Every field is a Noetherian ring, since it only has two ideals, namely the trivial ideal and the whole field.

Example 3.4. Every PID is a Noetherian ring since every ideal is generated by a single element. In particular, $F[x]$ is a Noetherian ring if F is a field.

Now we are ready to prove the main theorem of this section.

Theorem 3.5 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then $R[x]$ is also Noetherian.*

Proof. Let $J \lhd R[x]$ be an ideal. Our aim will be to show that J is finitely generated. Define $J_n \subseteq R$ to be the set of leading coefficients of polynomials in J of degree n:

$$J_n \coloneqq \{a_n \in R \mid \text{ there exists } f \in J \text{ such that } f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0\}.$$

Then J_n inherits its ideal property from J, and moreover for each n, $J_n \subseteq J_{n+1}$ since if $a \in J$, then there exists an $f \in J$ such that a is the leading coefficient of f. Taking $xf(x)$, we see that a can also be the leading coefficient of a polynomial of degree $n+1$. Now since R is Noetherian, it satisfies a.c.c, and so there exists some N such that $J_N = J_{N+1} = \cdots$. Now each J_i, $i \leqslant N$, is finitely generated since R is Noetherian, say $a_{i_1}, \dots, a_{i_{m_1}}$ be the generators of J_i. Then associated to each a_{i_k} is a function $f_{i_k} \in J$ with degree i and leading coefficient a_{i_k}. Then we claim that $\{f_{i_k}\}$ generates J. Let $g \in J$, and let $\deg g = m$. Write the leading coefficient of g as b, and then $b \in J_m$. Now take the generators in J_m to write

$$b = \sum c_{m'_k} a_{m'_k},$$

where $m' = m$ if $m \leqslant N$, and $m' = N$ if $m > N$. Now define

$$g_1 \coloneqq g - x^{m-m'} \cdot \sum c_{m'_k} f_{m'_k}.$$

This subtraction "deletes" the leading coefficient of g, and so $\deg g_1 \leqslant \deg g - 1$. Now by induction, we can write g as a combination of f_{i_k}, which implies that they generate j. ■

Corollary 3.6. *If R is a Noetherian ring, then $R[x_1, \dots, x_n]$ is also Noetherian. In particular, $\mathbb{C}[x_1, \dots, x_n]$ is Noetherian for all n.*

Proof. Take the above and throw induction at it. ■

4 The Correspondences $\mathbb{V}$ and $\mathbb{I}$

Now with similar notation as in Section 2, we may refine our notion of what $\mathbb{V}$ is: it is a function that takes sets of polynomials and maps it to subsets of $\mathbb{C}^n$. On the other hand, we define the "inverse map" $\mathbb{I}$, if V is a subset of $\mathbb{C}^n$, not necessarily an affine algebraic set,

$$\mathbb{I}(V) \coloneqq \{f \in \mathbb{C}[x_1, \dots, x_n] \mid f(x) = 0 \text{ for all } x \in V\}.$$

Clearly $\mathbb{I}(V)$ is an ideal.

Next, we ask the question if $\mathbb{I}$ and $\mathbb{V}$ are inverses; note that clearly $V \subseteq \mathbb{V}(\mathbb{I}(V))$ since $\mathbb{I}$ contains all functions vanishing on V, and $\mathbb{V}(\mathbb{I}(V))$ is the vanishing set of $\mathbb{I}(V)$. However, the reverse inclusion may not hold, and this brings us to the next proposition:

Proposition 4.1. *If $V \subseteq \mathbb{C}$, then $V = \mathbb{V}(\mathbb{I}(V))$ if and only if V is an affine algebraic set.*

Proof. Suppose $V = \mathbb{V}(\mathbb{I}(V))$. Then V is the image of some ideal under $\mathbb{V}$, which is by definition an affine algebraic set. Conversely, suppose V is an algebraic variety. We have shown one inclusion always holds; we need to show the reverse inclusion. If $x \in \mathbb{V}(\mathbb{I}(V))$, then $f(x) = 0$ for all $f \in \mathbb{I}(V)$, but V is the vanishing set of all $\{f_i\}_{i \in I}$, and so each $f_i \in \mathbb{I}(V)$ and it follows that $x \in V$, and so $\mathbb{V}(\mathbb{I}(V)) \subseteq V$, and the equality follows. ■

Now, from Corollary 3.6 we have that $\mathbb{C}[x_1, \dots, x_n]$ is a Noetherian ring, and so if V is an affine algebraic set in $\mathbb{C}^n$, $\mathbb{I}(V)$ is an ideal and so it is *finitely generated*. Therefore we have that every affine algebraic set is the zero set of finitely many polynomials. Thus every affine algebraic set can be described by finitely many polynomials, a rather surprising and powerful fact.

Our discussion above gives us a set to which the restriction of $\mathbb{V} \circ \mathbb{I}$ is the identity map: namely, the collection of all affine algebraic sets. Now we consider the natural follow-up question: are there necessary and sufficient conditions for which $\mathbb{I} \circ \mathbb{V}$ is the identity map? Certainly for any ideal I, one has $I \subseteq \mathbb{I}(\mathbb{V}(I))$, but this inclusion may be a strict one. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and consider f^a for $a \geqslant 2$. Then one has $f(x) = 0$ if and only if $f(x)^a = 0$, which implies $\mathbb{V}(f) = \mathbb{V}(f^a)$, which would imply that $f \in \mathbb{I}(\mathbb{V}(f^a))$, but in general $f \notin \langle f^a \rangle$. Our hopes are now dashed, and this motivates the need for Hilbert's Nullstellensatz.

5 Hilbert's Nullstellensatz

The proof of Hilbert's Nullstellensatz is a bit long, so one would naturally ponder if its inclusion is necessary especially since the soft page count limit of 2–3 has already been violated. But for the sake of completeness the authors feel compelled to discuss it, and to do that a definition is necessary.

Definition 5.1. Let $I \lhd R$. Then the **radical** of I is defined as

$$\operatorname{rad} I \coloneqq \{f \in R \mid \text{there exists some } n \text{ such that } f^n \in I\}.$$

An ideal I is called a **radical ideal** if $\operatorname{rad} I = I$.

Proposition 5.2. *For* $I \lhd R$, $\operatorname{rad} I$ *is an ideal.*

Proof. First let $f \in \operatorname{rad} I$, and say $f^n \in I$. Then if $h \in R$, $(fh)^n = h^n f^n \in I$ and so $fh \in \operatorname{rad} I$. If $f, g \in \operatorname{rad} I$, say $f^n, g^m \in I$, then by the binomial theorem

$$(f+g)^r = \sum_{a=0}^{r} \binom{r}{a} f^a g^{r-a},$$

and from here it is clear that for sufficiently large r one has $(f+g)^r \in \operatorname{rad} I$. ∎

Example 5.3. Every prime ideal is a radical ideal. Obviously $I \subseteq \operatorname{rad} I$, and conversely suppose $f \in \operatorname{rad} I$. Then there exists an n such that $f^n \in I$, and since $f^n = ff^{n-1}$, either $f \in I$ or $f^{n-1} \in I$, and proceed inductively.

Example 5.4. If V is an affine algebraic set, then $\mathbb{I}(V)$ is a radical ideal, since if $(f(x))^n = 0$ then $f(x) = 0$. So given any f^n which vanishes, we know f vanishes as well.

Now we are ready to state and prove the main theorem.

Theorem 5.5 (Hilbert's Nullstellensatz)**.**

(i) Every maximal ideal of the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ *is of the form* $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ *for some* $a = (a_1, \ldots, a_n) \in \mathbb{C}^n$. *Thus there is a one-to-one correspondence*

$$\{\textit{maximal ideals of } \mathbb{C}[x_1, \ldots, x_n]\} \longleftrightarrow \{\textit{points of } \mathbb{C}^n\}.$$

(ii) If $I \lhd \mathbb{C}[x_1, \ldots, x_n]$ *is an ideal, then* $\mathbb{V}(I) = \varnothing$ *if and only if* $I = \langle 1 \rangle$.

(iii) For any $I \lhd \mathbb{C}[x_1, \ldots, x_n]$,

$$\mathbb{I}(\mathbb{V}(I)) = \operatorname{rad} I.$$

Remark 5.6. The word "Nullstellensatz" is German for "theorem of zeros." Item (ii) is sometimes referred to as the weak Nullstellensatz, and item (iii) is sometimes referred to as the strong Nullstellensatz. However, *"stick to the German if you don't want to be considered an ignorant peasant"* [Reid, 2013].

We can also replace $\mathbb{C}$ with any algebraically closed field k, but for our sakes we will just consider $\mathbb{C}$.

We will first state a lemma which will be crucial in our proof of (i), but in the interest of brevity and clarity we will not prove it.

Lemma 5.7 (Zariski)**.**

(i) Let R be a ring that has $\mathbb{C}$ as a subring. The laws of composition on R can be used to make R into a complex vector space.

(ii) As a vector space, the field $\mathcal{F} = \mathbb{C}[x_1, \dots, x_n]/M$ is spanned by a countable set of elements.

(iii) Let V be a vector space spanned by a countable set of vectors. Then every independent subset of V is either finite or countably infinite.

(iv) Taking $\mathbb{C}(x)$ as a vector space over $\mathbb{C}$, the uncountable set of rational functions $(x-\alpha)^{-1}$ with α in $\mathbb{C}$ is independent.

Now assuming the lemma, we will furnish a proof for Theorem 5.5.

Proof. We first prove (i). Let $s_a : \mathbb{C}[x_1, \dots, x_n] \to \mathbb{C}$ be the substitution homomorphism of a, and M_a be the kernel of s_a. We know that s_a is surjective, so since $\mathbb{C}$ is a field M_a must be a maximal ideal. To verify that every maximal ideal is of the form in (a), we can see that if $a = (0, 0, \dots, 0)$ then every monomial that appears in $f \in s_0$ must be divisible by at least one of the variables, so f can be written as a linear combination of the variables with polynomial coefficients. For the general case we can simply make the variable substitution $x_i = x_i' + a_i$ to move a to the origin.

The harder part is showing that all maximal ideals have the form described in M_a. Let M be a maximal ideal, and $\mathcal{F} = \mathbb{C}[x_1, \dots, x_n]/M$. If we restrict the canonical map $\pi : \mathbb{C}[x_1, \dots, x_n] \to \mathcal{F}$ to the subring $\mathbb{C}[x_1]$, then we get a homomorphism $\phi_1 : \mathbb{C}[x_1] \to \mathcal{F}$. Then the kernel of ϕ_1 is either the zero ideal or one of the maximal ideals $\langle x_1 - a_1 \rangle$ of $\mathbb{C}[x_1]$. (Note that we could've easily swapped out x_1 for any such x_i.) This will mean that M contains some M_a, and since M_a is maximal then $M = M_a$. Seeking a contradiction, suppose $\ker \phi = \langle 0 \rangle$. Then we can show $\mathcal{F}$ contains a field isomorphic to $\mathbb{C}(x)$.

Now we use Lemma 5.7. Parts (ii) and (iii) of Lemma 5.7 show every independent set of $\mathcal{F}$ is finite or countably infinite. But we showed $\mathcal{F}$ contains a subfield isomorphic to $\mathbb{C}(x)$, so by (iv) $\mathcal{F}$ contains an uncountable independent set, a contradiction.

Now we will show that (i) implies (ii). We showed that $\mathbb{V}(1) = \varnothing$ earlier. For the other direction, assume $I \neq \langle 1 \rangle$. Then there exists some maximal ideal m of $\mathbb{C}[x_1, \dots, x_n]$ such that $I \subset m$ from the a.c.c. From (a) we know that

$$m = \langle x_1 - a_1, \dots, x_n - a_n \rangle,$$

so clearly $f(a) = 0$ for all $f \in I$, and thus $a \in V(I)$.

Now we will finally show that (ii) implies (iii). Since we know by definition $I \subseteq \mathbb{I}(\mathbb{V}(I))$, by Example 5.4 we conclude $\operatorname{rad} I \subseteq \operatorname{rad} \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\mathbb{V}(I))$. To show the reverse direction, we use a "fiendishly clever" argument known as the Rabinowitsch trick, named after the original name of George Yuri Rainich. Take some $f \in \mathbb{I}(\mathbb{V}(I))$. Now, introduce another variable y and consider the ideal

$$I_1 = \langle I, fy - 1 \rangle \lhd \mathbb{C}[x_1, \dots, x_n, y].$$

We claim that $\mathbb{V}(I_1) = \varnothing$, since any point $q = (a_1, \ldots, a_n, b)$ in $\mathbb{V}(I_1)$ must have that $(a_1, \ldots, a_n) \in \mathbb{V}(I)$. But this means that $(fy-1)(q) = f(a_1, \ldots, a_n)b - 1 = -1$, which implies that $q \notin \mathbb{V}(I_1)$, a contradiction.

Then by (b), we know that $I_1 = \langle 1 \rangle$. So there exist $f_i \in I$, $g_0, g_1 \in \mathbb{C}[x_1, \ldots, x_n, y]$ such that

$$1 = \sum g_i f_i + g_0(fy-1).$$

Viewing this equality as an identity in the field of fractions $\mathbb{C}(x_1, \ldots, x_n, y)$, we can let $y = f^{-1}$ and see that

$$1 = \sum g_i(x_1, \ldots, x_n, f^{-1}) f_i(x_1, \ldots, x_n, f^{-1}).$$

But $g_i \in I \lhd \mathbb{C}[x_1, \ldots, x_n]$, so the extra y variable does not matter to them, and

$$f_i = \frac{\hat{f}_i}{f^m},$$

for some $\hat{f}_i \in \mathbb{C}[x_1, \ldots, x_n]$, for some sufficiently large integer m. Then we can multiply out by f^m to see that

$$f^m = \sum g_i \hat{f}_i \in I$$

meaning $f \in \operatorname{rad} I$, as desired. ■

> *"This requires a cunning trick" [Reid, 2013].*
>
> *"The argument is not difficult ... but it is fiendishly clever" [Aluffi, 2009].*

Corollary 5.8. *The correspondences $\mathbb{V}$ and $\mathbb{I}$ induce bijections*

$$\{\textit{radical ideals}\} \longleftrightarrow \{\textit{algebraic subsets}\}.$$

6 References

[Aluffi, 2009] Aluffi, P. (2009). *Algebra: Chapter 0*. American Mathematical Society, 1st edition.

[Artin, 2011] Artin, M. (2011). *Algebra*. Pearson, 2nd edition.

[Reid, 2013] Reid, M. (2013). *Undergraduate Algebraic Geometry*. Cambridge University Press, 2nd edition.

[Smith et al., 2000] Smith, K. E., Kahanpää, L., Kekäläinen, P., and Traves, W. (2000). *An Invitation to Algebraic Geometry*. Springer-Verlag.