BASIC THEORY OF ALGEBRAIC GEOMETRY

SAMUEL BLOOM

Abstract. In this paper, we discuss the basic theory of algebraic geometry, and in doing so begin to develop an intimate relationship between algebraic and geometric objects and concepts.

Contents

1. Introduction and Preliminaries: The zero-set of an ideal; the ideal of a set of points.

In this paper, we begin a discussion of algebraic geometry: specifically, we will develop a correspondence between ideals in a polynomial ring and subsets of n-dimensional space, which will suggest an analogy between algebraic and geometric objects and concepts. Throughout the paper, we will attempt to emphasize this analogy.

In this first section, we give the basic definitions that are essential to the theory of algebraic geometry: the zero-set of an ideal in a polynomial ring over a field, the ideal of a set of points in affine space, algebraic sets, and the like. In the second section, we prove the Hilbert Basis Theorem and apply it to a finiteness property of algebraic sets. In the third section, we consider specific types of algebraic sets: first, *irreducible* algebraic sets, or *affine varieties*, which serve as a sort of basis for algebraic sets, and second, algebraic sets in the affine plane, which are more familiar. In the fourth section, we prove the Nullstellensatz, and with it solidify the correspondence which we will develop throughout the paper between algebraic and geometric objects. In the fifth section, we consider maps from and between irreducible algebraic sets.

We give the preliminary definitions and properties as indicated above. Knowledge of basic commutative algebra is assumed in this paper, including concepts and

Date: August 21, 2010.

basic results about rings and homomorphisms of rings, polynomial rings, prime ideals of rings, and fields. Let k be a field.

Definition 1.1. Denote by $\mathbb{A}^n(k)$ the n-fold Cartesian product of k with itself, which we will call *n-dimensional affine space* over k. If the field k is understood by context, we will simply write $\mathbb{A}^n$. We will call an element $x = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ a *point* in affine space. We will call $\mathbb{A}^1(k)$ the *affine line* and $\mathbb{A}^2(k)$ the *affine plane*.

Definition 1.2. For a polynomial $F \in k[X_1, X_2, \ldots, X_n]$, a point $P = (a_1, \ldots, a_n)$ is a *zero* of F if $F(a_1, \ldots, a_n) = 0$. If F is not a constant polynomial, then the set of zeros of F is called the *hypersurface* in $\mathbb{A}^n$ defined by F, and this will be denoted by $V(F)$. We may also denote $V(F)$ as the *zero-set* of the polynomial F. If the degree of F is one, we will call $V(F)$ a *hyperplane* in $\mathbb{A}^n$.

Definition 1.3. Generally, if $S \subseteq k[X_1, X_2, \ldots, X_n]$, the *zero-set* of S will be $V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\}$. Note that $V(S) = \bigcap_{F \in S} V(F)$. If $S = \{F_1, F_2, \ldots, F_m\}$, we will write $V(F_1, F_2, \ldots, F_m)$ instead of $V(\{F_1, F_2, \ldots, F_m\})$.

Definition 1.4. A subset $V \subseteq \mathbb{A}^n$ is an *affine algebraic set*, or more simply an *algebraic set*, if $V = V(S)$ for some $S \subseteq k[X_1, X_2, \ldots, X_n]$.

Examples 1.5. Any conic section $\mathbb{R}^2$ is an algebraic set. The unit sphere $S^n \subset \mathbb{A}^{n+1}(\mathbb{R})$ is an algebraic set. The set $\{(x, y) \mid y = \sin(x)\} \subset \mathbb{A}^2(\mathbb{R})$ is not algebraic.

The following are the first basic properties of these objects. These properties are easy to verify.

(1) If $I = (S) \subseteq k[X_1, X_2, \ldots, X_n]$ is the ideal generated by a subset S of the polynomial ring, then $V(I) = V(S)$. Thus, any algebraic set is equal to $V(I)$ for some ideal I. For this reason, we will almost exclusively talk about ideals of the polynomial ring.
(2) If $\{I_\alpha\}_\alpha$ is a collection of ideals in $k[X_1, X_2, \ldots, X_n]$, then $V\left(\sum_\alpha I_\alpha\right) = \bigcap_\alpha V(I_\alpha)$. Thus, the arbitrary intersection of algebraic sets in $\mathbb{A}^n$ is itself an algebraic set.
(3) If $I \subset J$, then $V(I) \supset V(J)$, so this correspondence is inclusion-reversing.
(4) For any polynomials F, $G \in k[X_1, X_2, \ldots, X_n]$, we have $V(FG) = V(F) \cup V(G)$. For any two ideals I, $J \subset k[X_1, X_2, \ldots, X_n]$, we have $V(I) \cup V(J) = V(I \cap J)$, so that a finite union of algebraic sets is itself an algebraic set.
(5) $V(0) = \mathbb{A}^n$. $V(k[X_1, X_2, \ldots, X_n]) = \emptyset$. In $\mathbb{A}^n$, we have $V(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) = \{(a_1, a_2, \ldots, a_n)\}$ for all $a_i \in k$. Thus, any finite set in $\mathbb{A}^n$ is an algebraic set.

The size of these algebraic sets is another basic property to consider. We have the following results:

Proposition 1.6. *Any proper algebraic subset of $\mathbb{A}^1(k)$ is finite.*

Proof. If k is a field, then $k[X]$ is a PID. Any algebraic set in $\mathbb{A}^1(k)$ has the form $X = V(I)$ for an ideal $I \subseteq k[X]$; if $I = k[X]$, then $X = \emptyset$; otherwise, $I = (F)$ for some polynomial F. But F has finite degree, so F has finitely many roots (if any). □

Proposition 1.7. *Let k be algebraically closed, and $F \in k[X_1, X_2, \ldots, X_n]$ be irreducible. Then, $\mathbb{A}^n(k) \setminus V(F)$ is infinite, and for $n \geq 2$, $V(F)$ is infinite as well.*

Proof. Since k is algebraically closed, the polynomial $F(1, 1, \ldots, X_n)$ has only finitely many roots in X_N, so the subset

$$\{(1, 1, \ldots, a_n) \mid a_n \text{ is not a root of } F(1, 1, \ldots, X_n)\} \subset \mathbb{A}^n(k) \setminus V(F)$$

is infinite. The first statement of the proposition follows.

For $n \geq 2$, for each $a_1, a_2, \ldots a_{n-1} \in k$, the polynomial $F(a_1, a_2, \ldots, a_{n-1}, X_n)$ has at least one root, since k is algebraically closed. Thus, since k is infinite, $V(F)$ is infinite. □

We have considered a correspondence from ideals in the a polynomial ring to subsets of $\mathbb{A}^n$; we now develop the correspondence in the opposite direction.

Definition 1.8. For a subset $X \subset \mathbb{A}^n(k)$, we consider the set of polynomials that vanish on the set X, and denote this by

$$I(X) = \{F \in k[X_1, X_2, \ldots, X_n] \mid F(P) = 0 \ \forall P \in X\}.$$

Clearly, $I(X)$ is an ideal for any $X \subseteq \mathbb{A}^n$; we will call it the *ideal* of the set X.

The following are the first basic properties of these objects, and these properties are easy to verify.

(1) If $X \subset Y$, then $I(X) \supset I(Y)$, so this correspondence is inclusion-reversing. Moreover, $I(X) = I(Y) \iff X = Y$.
(2) $I(\emptyset) = k[X_1, X_2, \ldots, X_n]$. If k is infinite, $I(\mathbb{A}^n(k)) = (0)$. For $a_1, \ldots, a_n \in k$, $I((a_1, \ldots, a_n)) = (X_1 - a_1, \ldots, X_n - a_n)$.
(3) $I(V(S)) \supseteq S$ for any set S of polynomials.
(4) If V is an algebraic set in $\mathbb{A}^n$, then $V = V(I(V))$.
(5) For any $X \subseteq \mathbb{A}^n$, $I(X)$ is a radical ideal. That is, if a polynomial F has a power F^N vanishing on X, then F must as well vanish on X. Moreover, for any ideal $I \subset k[X_1, X_2, \ldots, X_n]$, $\mathrm{Rad}(I) \subseteq I(V(I))$.

We give a construction which will be useful later:

Proposition 1.9. *Let $P_1, P_2, \ldots, P_n$ be distinct points in $\mathbb{A}^n$. Then, there exist polynomials $F_i \in k[X_1, X_2, \ldots, X_n]$ such that $F_i(P_j) = \delta_{ij} = \begin{cases} 0 \text{ if } i \neq j \\ 1 \text{ if } i = j. \end{cases}$*

Proof. For each i, let $V_i = \{P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n\}$. Then, from the first property above, $V_i \subsetneq V_i \cup \{P_i\}$ implies $I(V_i) \supsetneq I(V_i \cup \{P_i\})$. Pick $G_i \in I(V_i \cup \{P_i\}) \setminus I(V_i)$. G_i is zero on V_i, but is non-zero on P_i. Thus, our desired polynomials are $F_i = \left(\frac{1}{G_i(P_i)}\right) G_i$. □

2. Hilbert Basis Theorem and its application.

We defined algebraic sets in terms of an arbitrary set of polynomials, and although we can clearly restrict our attention to ideals of polynomials, we will see that the situation is even simpler. In other terms, an algebraic set can be thought of as the intersection of an arbitrary collection of hypersurfaces, since $V(S) = \bigcap_{F \in S} V(F)$. However, we will see that even just finite intersections of hypersurfaces will be enough:

Theorem 2.1. *Any algebraic set in $\mathbb{A}^n$ is a finite intersection of hypersurfaces.*

For the proof of this theorem, we will need the following lemma:

Lemma 2.2 (Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then $R[X_1, X_2, \ldots, X_n]$ is a Noetherian ring as well.*

Proof. We will induct. The inductive step is clear, since $R[X_1, X_2, \ldots, X_i] \cong \big(R[X_1, X_2, \ldots, X_{i-1}]\,\big)[X_i]$.

So, assume R is Noetherian; we will show that $R[X]$ is Noetherian by showing that any proper ideal $I \subset R[X]$ is finitely generated.

Let J be the set of leading coefficients of elements in I. Clearly, J is an ideal of R, so J is finitely generated. Let $F_1, \ldots, F_r \in I$ be polynomails whose leading coefficients generate J. Take $N > \max\{\deg(F_i)\}$.

For each $m \leq N$, let J_m be the ideal in R consisting of all leading coefficients of all polynomials in I of degree less than or equal to m. Let $\{F_{mj}\}_j$ be a finite set of polynomials of degree less than or equal to m whose leading coefficients generate J_m. Let $I' = \Big(\{F_i\}_i, \{F_{mj}\}_{m,j}\Big)$. We wish to show that $I' = I$.

Suppose $I' \subsetneq I$. Let $G \in I \setminus I'$ be an element of *lowest* degree in $I \setminus I'$.

If $\deg(G) > N$, we can find polynomials $Q_i \in R[X]$ such that $\sum_i Q_i F_i$ and G have the same leading term, since $\{F_i\}$ generates J and the leading coefficient of G is in J. Then, subtracting off, $\deg(G - \sum_i Q_i F_i) < \deg(G)$. Since G is of minimal degree, $G - \sum_i Q_i F_i \in I'$. But this implies $G \in I'$, a contradiction.

Similarly, if $\deg(G) = m \leq N$, we can lower the degree of G by subtracting $\sum_j Q_j F_{mj}$ for some polynomials $Q_j \in R[X]$, again contradicting minimality of degree.

Thus, $I = I' = \Big(\{F_i\}_i, \{F_{mj}\}_{m,j}\Big)$, so I is finitely generated. □

Proof. (of 2.1): We are to show that any algebraic set is the finite intersection of hypersurfaces. Let $V = V(I)$ be an algebraic set in $\mathbb{A}^n(k)$. k is a field, and is thus a Noetherian ring, so by Lemma (2.2), $k[X_1, X_2, \ldots, X_n]$ is a Noetherian ring as well. Thus, $I \subseteq k[X_1, X_2, \ldots, X_n]$ is finitely generated; say $I = (F_1, \ldots, F_m)$. If $I = k[X_1, X_2, \ldots, X_n]$, then $V(I) = \emptyset = V(1)$. Otherwise,

$$V = V(I) = V\big((F_1, \ldots, F_m)\big) = V(F_1) \cap \cdots \cap V(F_m).$$

□

3. Irreducible algebraic sets, and properties of the affine plane.

We now restrict our attention to two particulars: a certain type of algebraic set, and $\mathbb{A}^2(k)$, the affine plane.

Definition 3.1. An algebraic set $V \subseteq \mathbb{A}^n$ is *reducible* if $V = V_1 \cup V_2$ for some non-trivial (i.e. non-empty) algebraic sets $V_1, V_2 \subset \mathbb{A}^n$, with $V \neq V_1$ and $V \neq V_2$. Otherwise, V is *irreducible*.

Ireducible algebraic sets will play a major role in the basic theory we are developing. Following are a few important theorems.

Theorem 3.2. *An algebraic set V is irreducible if and only if $I(V)$ is a prime ideal.*

Proof. ($\Longrightarrow$): If $I(V)$ is not prime, suppose $F_1 F_2 \in I(V)$ but $F_i \notin I(V)$ for each i. Then,

$$V = \big(V \cap V(F_1)\big) \bigcup \big(V \cap V(F_2)\big)$$

since for all $P \in V$, if $F_1(P)F_2(P) = 0$, then either $F_1(P) = 0$ or $F_2(P) = 0$, so either $P \in V(F_1)$ or $P \in V(F_2)$. But clearly, $F_i \notin I(V)$ implies $V(F_i) \neq V$ for each i.

($\Longleftarrow$): Suppose $V = V_1 \cup V_2$ is reducible. Then, $V_i \subsetneq V$ implies $I(V_i) \supsetneq I(V)$ for each i. Let $F_i \in I(V_i) \setminus I(V)$. Then, $F_i \notin I(V)$ for each i, but $F_1F_2 \in I(V)$ since for all $P \in V$, either $F_1(P) = 0$ or $F_2(P) = 0$. Thus, $I(V)$ is not prime. □

Theorem 3.3. *Let V be an algebraic set in $\mathbb{A}^n(k)$. Then, there exist unique irreducible algebraic sets $V_1, \ldots, V_m$ such that $V = V_1 \cup \cdots \cup V_m$ and $V_i \nsubseteq V_j$.*

We first need the following lemma:

Lemma 3.4. *Let $\boldsymbol{D}$ be a non-empty collection of ideals of a Noetherian ring R. Then, $\boldsymbol{D}$ has a maximal member.*

Proof. Suppose we have a infinite chain of ideals in $\mathbf{D}$:

$$I_0 \subset I_1 \subset I_2 \subset \ldots$$

Then, $\bigcup_{i=0}^{\infty} I_i$ is an ideal of R, so it generated by $a_1, \ldots, a_n$. Then, $a_i \in I_{f(i)}$ for some $f(i) \in \mathbb{N}$. Take $N = \max\{f(i)\}$. Then, $a_i \in I_N$ for all i. Thus, $\bigcup_{i=0}^{\infty} I_i = I_N$, so the chain has an upper bound. Thus, by Zorn's Lemma, $\mathbf{D}$ has a maximal member. □

Proof. (of 3.3): Define the set

$$\mathbf{D} = \{\text{algebraic sets } V \subseteq \mathbb{A}^n \mid V \text{ is not the union of a finite number of irreducible algebraic sets in } \mathbb{A}^n\}.$$

We want to show $\mathbf{D}$ is empty. Suppose not. Let V be a minimal member of $\mathbf{D}$. (This exists by a similar argument as in the proof of the above lemma.) Since $V \in \mathbf{D}$, V is not irreducible, so let $V = V_1 \cup V_2$ for some $V_i \subsetneq V$. Then, $V_i \notin \mathbf{D}$ by minimality. Thus, V_1 and V_2 are finite unions of irreducible algebraic sets, so $V = \big(V_{1,1} \cup \cdots \cup V_{1,r}\big) \bigcup \big(V_{2,1} \cup \cdots \cup V_{2,s}\big)$, and thus $V \notin \mathbf{D}$, contradiction.

Thus, any algebraic set can be written as $V = V_1 \cup \cdots \cup V_m$ for some irreducibles V_i. The second condition ($V_i \nsubseteq V_j$) can be obtains by simply throwing away any such V_i contained in another irreducible algebraic set in the list.

For uniqueness, suppose

$$V = V_1 \cup \cdots \cup V_m = W_1 \cup \cdots \cup W_m$$

is two distinct unions of irreducible algebraic sets with the given conditions. Then, for each i, we have $V_i = \bigcup_i (V_i \cap W_j)$. But each V_i is irreducible, so only one of the terms of the union can be non-empty, i.e. there exists a function σ on the subscripts such that $V_i \subseteq W_{\sigma(i)}$. Similarly, there exists a function τ such that $W_{\sigma(i)} \subseteq V_{\tau(\sigma(i))}$. Then, $V_i \subseteq V_{\tau(\sigma(i))}$ implies $V_i = V_{\tau(\sigma(i))}$ implies $V_i = W_{\sigma(i)}$. Similarly, $W_j = V_{\tau(j)}$. Thus, the decompositions are the same. □

This leads us to the following general definition, which simplifies algebraic sets and allows us to talk about different "parts" of an algebraic set:

Definition 3.5. If V is an affine algebraic set, and $V = V_1 \cup \cdots \cup V_m$ as above, each V_i is called an *irreducible component* of V, and the expression of the union is the *decomposition* of V into irreducible components.

We now study a particular affine space and its corresponding polynomial ring: the affine plane $\mathbb{A}^2(k)$, and the polnomial ring $k[X,Y]$. Examples of familiar hypersurfaces in $\mathbb{A}^2(\mathbb{R})$ are the parabola $Y - X^2$, which we will sometimes write $Y = X^2$, and the unit circle $X^2 + Y^2 - 1$.

We give a few properties of affine algebraic sets in the plane, and then classify all the irreducible algebraic sets in the plane.

Proposition 3.6. *Let $F, G \in k[X,Y]$ have no common factors. Then, $V(F,G) = V(F) \cap V(G)$ is a finite set of points.*

Proof. The polynomials F and G have no common factors in $k[X][Y]$, so neither do they have common factors in $k(X)[Y]$. Since $k(X)$ is a field, $k(X)[Y]$ is a PID, and so $(F,G) = (1)$ in $k(X)[Y]$, so there exist polynomials $R, S \in k(X)[Y]$ such that $FR + GS = 1$.

Then, there exists a non-zero $D \in k[X]$ such that $RD, SD \in k[X][Y]$. (Clear denominators.) Then, $F \cdot RD + G \cdot SD = D$. Then, for $P \in V(F) \cap V(G)$, we have $F(P) = G(P) = 0$, so $D(P_x) = 0$, where P_x is the X-coordinate of P. Thus, there are only finitely many choices of X-coordinate for P. Similarly for the Y-coordinate. Thus, we must have that $V(F) \cap V(G)$ is finite. □

Corollary 3.7. *If $F \in k[X,Y]$ is irreducible and $V(F)$ is infinite, then $I(V(F)) = (F)$, and $V(F)$ is irreducible.*

Proof. If $G \in I(V(F))$, then $G(P) = 0$ for all $P \in V(F)$, so $V(F) \cap V(G)$ is infinite. Thus, by Proposition (3.6), F and G have common factors. But F is irreducible, so $F|G$ implies $G \in (F)$ implies $I(V(F)) \subseteq (F)$. But clearly, $(F) \subseteq I(V(F))$, so indeed $I(V(F)) = (F)$.

Now, since F is irreducible, (F) is prime. By Proposition (3.2), $V(F)$ is thus irreducible. □

Corollary 3.8. *Suppose k is infinite. Then, the irreducible algebraic subsets of $\mathbb{A}^2(k)$ are the following: $\mathbb{A}^2(k)$, $\emptyset$, points, and irreducible plane curves $V(F)$ for $F \in k[X,Y]$ irreducible and $V(F)$ infinite.*

Proof. Let $V \subseteq \mathbb{A}^2(k)$ be an irreducible algebraic set.

If V is finite, then V must clearly be a single point. If $I(V) = 0$, then $V = \mathbb{A}^2(k)$. If $I(V) = k[X,Y]$, then $V = \emptyset$.

Otherwise, $I(V)$ contains a non-constant polynomial F. Since $I(V)$ is prime, one of the irreducible factors of F is in $I(V)$; so, we can assume F is irreducible. Then, $I(V) = (F)$ by Cor. (3.7), since $V(F)$ is infinite. Thus, since V is algebraic, $V = V(I(V)) = V(F)$, as desired. □

With this classification, we can now decompose hypersurfaces in the affine plane into their irreducible components. We assume that k is algebraically closed, which will mean that k is infinite. This is a stronger assumption, which we will continue to use in the paper, for reasons which will be clear in the next section.

Corollary 3.9. *Assume k is algebraically closed and $F \in k[X,Y]$ is a non-constant polynomial. Let $F = F_1^{n_1} F_2^{n_2} \cdots F_r^{n_r}$ be the decomposition of F into irreducible factors. Then, $V(F) = V(F_1) \cup V(F_2) \cup \cdots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components, and $I(V(F)) = (F_1 F_2 \cdots F_r)$.*

Proof. Since $\gcd(F_i, F_j) = 1$ for all $i \neq j$, we have $V(F_i) \nsubseteq V(F_j)$ for $i \neq j$.

Then, since each F_i is irreducible,

$$I\big(\bigcup_{i=1}^{r} V(F_i)\big) = \bigcap_i I(V(F_i)) = \bigcap_i (F_i).$$

Since the F_i's share no common factors, any polynomial divisible by each F_i is divisible by $F_1F_2\cdots F_r$, so $\bigcap_i (F_i) = (F_1F_2\cdots F_r)$. Clearly, then,

$$V(F) = V(F_1^{n_1}F_2^{n_2}\cdots F_r^{n_r}) = V(F_1F_2\cdots F_r) = \bigcup_i V(F_i),$$

so $I(V(F)) = (F_1F_2\cdots F_r)$, and

$$V(I(V(F))) = V(F) = V(F_1F_2\cdots F_r) = V(F_1)\cup V(F_2)\cup\cdots\cup V(F_r).$$

□

4. Hilbert's Nullstellensatz

From the above discussion of algebraic sets in the plane, the following question arises: generally, what is $I(V(I))$ for an ideal $I \subset k[X_1, X_2, \ldots, X_n]$? For irreducible polynomials F, we have that $I(V(F^m)) = (F)$, and for polynomials in $k[X, Y]$, we have $I(V(F_1^{n_1}F_2^{n_2}\cdots F_r^{n_r})) = (F_1F_2\cdots F_r)$. These suggest that what we are looking at is the radical of the original ideal I. Hilbert's Nullstellensatz Theorem will confirm this.

Since the scope of this paper is mostly to show the connection that algebraic geometry makes between the two areas, we will omit the proof of the following lemma which will be necessary to prove Hilbert's Nullstellensatz.

Lemma 4.1. *Let k be an algebraically closed field k that is a subfield of a field L. Suppose there is a surjective ring homomorphism $k[X_1, X_2, \ldots, X_n] \overset{\phi}{\twoheadrightarrow} L$ such that ϕ is the identity on k. Then $k = L$.*

We now prove what is known as the "Weak Nullstellensatz", which will be a lemma for the Nullstellensatz.

Lemma 4.2 (Weak Nullstellensatz)**.** *Suppose k is an algebraically closed field. If $I \subset k[X_1, X_2, \ldots, X_n]$ is a proper ideal, then $V(I) \neq \emptyset$.*

Proof. By Zorn's Lemma, there exists a maximal ideal J containing I, so $V(J) \subseteq V(I)$. We will show $V(J)$ is non-empty.

The quotient $k[X_1, X_2, \ldots, X_n]/J = L$ is a field, since J is maximal, and k may be regarded as a subfield of L, since the composition $k \hookrightarrow k[X_1, X_2, \ldots, X_n] \twoheadrightarrow L$ is non-trivial ($1 \mapsto \overline{1}$), and is thus injective.

By Lemma (4.1), $k = L = k[X_1, X_2, \ldots, X_n]/J$. Then,

$$\begin{aligned}\overline{X_i} = a_i \in k &\implies \overline{X_i - a_i} = \overline{0} \implies X_i - a_i \in J \\ &\implies (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \subseteq J.\end{aligned}$$

But $\big(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n\big)$ is a maximal ideal of $k[X_1, X_2, \ldots, X_n]$. Thus, $J = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$. But $P = (a_1, a_2, \ldots, a_n) \in V(J) \subseteq V(I)$. □

We now proceed with the main theorem of this section:

Theorem 4.3 (Nullstellensatz)**.** *Let k be an algebraically closed field. Let I be an ideal of $k[X_1, X_2, \ldots, X_n]$. Then, $I(V(I)) = rad(I)$.*

Proof. ($\supseteq$): That $I(V(I)) \supseteq \operatorname{rad}(I)$ is easy: if $F_r \in I$, then $F^r(P) = \big(F(P)\big)^r = 0$ for all $P \in V(I)$. Since k is a field, $F(P) = 0$ for all $P \in V(I)$.

($\subseteq$): We show $I(V(I)) \subseteq \operatorname{rad}(I)$. Suppose $G \in I(V(F_1, \ldots, F_r))$, with $F_i \in k[X_1, X_2, \ldots, X_n]$. Let $J = (F_1, \ldots, F_r, X_{n+1}G - 1) \subseteq k[X_1, X_2, \ldots, X_{n+1}]$. Since G vanishes wherever all the F_i's vanish, $V(J) = \emptyset$. Thus, by Lemma (4.2), J is not a proper ideal, i.e. $J = k[X_1, X_2, \ldots, X_{n+1}]$. In particular, $1 \in J$. Then, there exist polynomials $A_i, B \in k[X_1, X_2, \ldots, X_{n+1}]$ such that

$$1 = \sum_i \big(A_i(X_1, \ldots, X_{n+1})F_i\big) + B(X_1, \ldots, X_{n+1})(X_{n+1}G - 1).$$

Formally, setting $X_{n+1} = \frac{1}{G}$, we have

$$1 = \sum_i \big(A_i(X_1, \ldots, \frac{1}{G})F_i\big) + B(X_1, \ldots, X_{n+1})(\frac{1}{G} \cdot G - 1) = \sum_i \big(A_i(X_1, \ldots, \frac{1}{G})F_i\big).$$

Then, each summand has a finite degree in $\frac{1}{G}$. Let N be the highest such degree. Then, setting $A_i' = G^N A_i \in k[X_1, X_2, \ldots, X_n]$ and multiplying through,

$$G^N = \sum_i A_i' F_i \in (F_1, F_2, \ldots, F_n) = I$$

so that $G \in \operatorname{rad}(I)$. □

With this powerful theorem, we are now able to solidify the correspondence we began to establish earlier:

Corollary 4.4. *Let k be an algebraically closed field. Then, there are natural correspondences as follows:*

$$\begin{aligned}
\{\textit{radical ideals in } k[X_1, X_2, \ldots, X_n]\} &\longleftrightarrow \{\textit{algebraic sets in } \mathbb{A}^n(k)\} \\
\{\textit{prime ideals in } k[X_1, X_2, \ldots, X_n]\} &\longleftrightarrow \{\textit{irreducible algebraic sets in } \mathbb{A}^n(k)\} \\
\{\textit{maximal ideals in } k[X_1, X_2, \ldots, X_n]\} &\longleftrightarrow \{\textit{points in } \mathbb{A}^n(k)\} \\
\{\textit{irreducible } F \in k[X_1, X_2, \ldots, X_n] & \\
\textit{up to associates}\} &\longleftrightarrow \{\textit{irreducible hypersurfaces in } \mathbb{A}^n(k)\}
\end{aligned}$$

We also have the following relationship between $V(I)$ and the quotient field modulo I:

Corollary 4.5. *Let I be an ideal in $k[X_1, X_2, \ldots, X_n]$. Then, $V(I)$ is finite if and only if $k[X_1, X_2, \ldots, X_n]/I$ is a finite-dimensional vector space over k. If this is true, then $|V(I)| \leq \dim_k (k[X_1, X_2, \ldots, X_n]/I)$.*

Proof. ($\Leftarrow$): Assume $k[X_1, X_2, \ldots, X_n]/I$ is finite-dimensional over k. Let $P_1, \ldots, P_r \in V(I)$. Choose $F_1, \ldots, F_r \in k[X_1, X_2, \ldots, X_n]$ such that

$$F_i(P_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

This is possible by Proposition (1.9). Let $\overline{F_i}$ be the residue modulo I of F_i. Then, if $\sum_i \lambda_i \overline{F_i} = 0$ for some $\lambda_i \in k$, then $\sum_i \lambda_i F_i \in I$, so for each j, $\left(\sum_i \lambda_i F_i\right)(P_j) = 0$. By the choice of F_i we made, $\lambda_j = \left(\sum_i \lambda_i F_i\right)(P_j) = 0$. Thus, all of the λ_js are zero, and thus $\left\{\overline{F_1}, \ldots, \overline{F_r}\right\}$ is linearly independent. But this means $r \leq \dim_k (k[X_1, X_2, \ldots, X_n]/I)$, so that $V(I)$ can contain at most

$\dim_k (k[X_1, X_2, \ldots, X_n]/I)$ many points.

($\Rightarrow$): Suppose $V(I) = \{P_1, \ldots, P_r\}$ is finite. Let each $P = (a_{i,1}, a_{i,2}, \ldots, a_{i,n})$. Define $F_j = \prod_{i=1}^{r}(X_j - a_{i,j})$ for $j = 1, \ldots, n$. Then, $F_j(P_i) = 0$ for each $P_i \in V(I)$, so that $F_j \in I(V(I))$ implies $F_j \in \text{rad}(I)$, and thus $F_j^{N_j} \in I$ for some $N_j > 0$. Take $N > \max N_j$.

Then, taking I-residues, $\overline{F_j^N} = 0$, so for each j, $\overline{X_j^{rN}}$ is a k-linear combination of elements in $\{\overline{1}, \overline{X_j}, \ldots, \overline{X_j^{rN-1}}\}$. By induction on the exponent, $\overline{X_j^s}$ is a k-linear combination of those same elements, for each j. Thus, $k[X_1, X_2, \ldots, X_n]/I$ is generated as a vector space by the set

$$\left\{ \prod_{j=1}^{n} X_j^{m_j} \;\middle|\; m_j < rN \text{ for each } j \right\},$$

which is finite. □

5. Affine varieties, coordinate rings, and polynomial maps.

We will now choose to work primarily on irreducible algebraic sets in $\mathbb{A}^n(k)$, where k is an algebraically closed field, since they are the "smallest" algebraic sets, as it were, and any algebraic set has a decomposition into a union of irreducible algebraic sets. We will call these ireducible algebraic sets *affine varieties*, or simply *varieties*, from now on. According to our correspondence in Corollary (4.4), we will be working also primarily with prime ideals.

We wish to study the different functions on a variety V, in particular the different functions which arise as polynomials of the coordinates $X_1, \ldots, X_n$. We have the following definitions:

Definition 5.1. Let $V \in \mathbb{A}^n$ be a non-empty affine variety. Then, $I(V)$ is prime, so $\Gamma(V) = k[X_1, X_2, \ldots, X_n]/I(V)$ is a domain. Call $\Gamma(V)$ the *coordinate ring* of V.

Definition 5.2. Let V be a variety and $f \in \mathcal{F}(V, k)$, where $\mathcal{F}(V, k)$ is the ring of functions from V to k. We will say that f is a *polynomial function* if there exists $F \in k[X_1, X_2, \ldots, X_n]$ such that $f = F$ on V, i.e., $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$ for all $(a_1, \ldots, a_n) \in V$.

Note that two polynomials $F, G \in k[X_1, X_2, \ldots, X_n]$ correspond to the same $f \in \mathcal{F}(V, k)$ if and only if $F(P) = G(P)$ for all $P \in V$ if and only if $F - G \in I(V)$. We may thus identify as follows:

$$\Gamma(V) = k[X_1, X_2, \ldots, X_n]/I(V) \cong \{\text{polynomial functions on } V\} \subseteq \mathcal{F}(V, k)$$

Our correspondence from Corollary (4.4) extends to $\Gamma(V)$ because of the correspondence of ideals in a ring and its quotient:

Proposition 5.3. *Let $V \subseteq \mathbb{A}^n$ be a variety. Then, there are natural correspondences:*

$$\{\textit{radical ideals in } \Gamma(V)\} \longleftrightarrow \{\textit{algebraic subsets of } V\}$$
$$\{\textit{prime ideals in } \Gamma(V)\} \longleftrightarrow \{\textit{subvarieties of } V\}$$
$$\{\textit{maximal ideals in } \Gamma(V)\} \longleftrightarrow \{\textit{points of } V\}$$

Proposition 5.4. *Let $V \subseteq \mathbb{A}^n$ be a variety, and $W \subseteq V$ a subvariety. Define $I_V(W) \subseteq \Gamma(V)$ be the ideal corresponding to W; that is, $I_V(W)$ is the ideal of polynomial functions on V that vanish on W. Then, the following are true:*

(a) Every polynomial function on V restricts to a polynomial function on W.
(b) The map $\phi : \Gamma(V) \to \Gamma(W)$ defined in part (a) is surjective homomorphism with $\ker(\phi) = I_V(W)$, so that $\Gamma(W) \cong \Gamma(V)/I_V(W)$.

The above proposition is clear; mapping an element of $\Gamma(V)$ to $\Gamma(W)$ can be thought of as disregarding the behavior of the polynomial function outside of V, so that two polynomial functions on V are the same in $\Gamma(W)$ if they agree on W, i.e. if their difference is in $I_V(W)$.

Proposition 5.5. *Let $V \subseteq \mathbb{A}^n(k)$ be a non-empty variety. Then, the following are equivalent:*

(i) V is a point;
(ii) $\Gamma(V) \cong k$;
(iii) $\dim_k(\Gamma(V)) < \infty$.

Proof. $(i) \implies (ii)$: $V = \{P\}$ is a point, so any polynomial function $V \to k$ is determined solely by its value at P. Thus, $\Gamma(V) = k$.

$(ii) \implies (iii)$: Clear.

$(iii) \implies (i)$: By Corollary (4.5), if $\Gamma(V)$ is finite-dimensional over k, then V is a finite set. But V is irreducible, so V is a point. □

We will now study maps between varieties, and the relationship of these to the coordinate ring.

Definition 5.6. Let $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ be varietes. A mapping $\varphi : V \to W$ is a *polynomial mapping* if there are polynomials $T_1, \ldots, T_m \in k[X_1, X_2, \ldots, X_n]$ such that $\varphi(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n))$ for all $(a_1, \ldots, a_n) \in V$.

Note that any map $\varphi : V \to W$ induces a homomorphism $\widetilde{\varphi} : \mathcal{F}(W, k) \to \mathcal{F}(V, k)$ by $\widetilde{\varphi}(f) = f \circ \varphi$. If φ is a polynomial map, then $\widetilde{\varphi}$ restricts to a homomorphism $\Gamma(W) \to \Gamma(V)$. This is true because if $f \in \Gamma(W)$ is the $I(W)$-residue of a polynomial F, then $\widetilde{\varphi}(f) = f \circ \varphi$ is the $I(V)$-residue of the polynomial $F(T_1, \ldots, T_m)$.

Note also that if $V = \mathbb{A}^n$ and $W = \mathbb{A}^n$, and if $T_1, \ldots, T_m \in k[X_1, X_2, \ldots, X_n]$ determine a polynomial map $T : \mathbb{A}^n \to \mathbb{A}^m$, then the T_i are uniquely determined by T, so we write $T = (T_1, \ldots, T_m)$.

We give two basic properties without proof:

Proposition 5.7. *(a) If $\varphi : V \to W$ and $\psi : W \to Z$ are polynomial maps, then $\widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi}$.*
(b) The composition of two polynomial maps is also a polynomial map.

We now have the following correspondence:

Proposition 5.8. *Let $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ be varieties. There is a natural bijective correspondence between polynomial maps $\varphi : V \to W$ and homomorphisms $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$. Any such φ is the restriction of a polynomial map $\mathbb{A}^n \to \mathbb{A}^m$.*

Proof. We will use the following notation: capital-lettered maps will exist in a polynomial ring, and the corresponding lowercase-lettered maps will be the appropriate residue of those maps in the appropriate coordinate ring.

Suppose $\alpha : \Gamma(W) \to \Gamma(V)$ is a homomorphism. Choose $T_i \in k[X_1, X_2, \ldots, X_n]$ such that $\alpha(x_i) = t_i$ for $i = 1, \ldots, m$. Then, $T = (T_1, \ldots, T_m) : \mathbb{A}^n \to \mathbb{A}^m$ is a polynomial map, inducing a homomorphism $\widetilde{T} : \Gamma(\mathbb{A}^m) \to \Gamma(\mathbb{A}^n)$; that is, $\widetilde{T} : k[X_1, X_2, \ldots, X_m] \to k[X_1, X_2, \ldots, X_n]$.

Clearly, $\widetilde{T}(I(W)) \subseteq I(V)$. This is because, for each $G \in I(W)$, $g = 0$ implies $\alpha(g) = 0$; then, considered as polynomial functions on V, $\alpha(g)$ and $G \circ T$ agree on V by definition of T, so that $G \circ T$ vanishes on V implies $G \circ T \in I(V)$ implies $T(V) \subseteq W$. Thus, T restricts to a polynomial map $\varphi : V \to W$, as desired. It is not difficult to verify that $\widetilde{\varphi} = \alpha$. □

Definition 5.9. A polynomial map $\varphi : V \to W$ is an *isomorphism* if there exists a polynomial map $\psi : W \to V$ such that $\varphi \circ \psi = \mathrm{id}_W$ and $\psi \circ \varphi = \mathrm{id}_V$.

By Proposition (5.8), then, V and W are isomorphic varieties if and only if their coordinate rings are isomorphic over k.

An interesting thing to note is that we are able to define a topology on $\mathbb{A}^n$, known as the *Zariski topology*, in which a set is *closed* if and only if it is algebraic, and in which a closed set is irreducible if and only if it is an affine variety. From the basic properties in the first section of this paper, it is not hard to check that this is a topology. Then, polynomial maps between varieties act as continuous functions in this topology:

Proposition 5.10. *If $\varphi : V \to W$ is a polynomial map, and X is an algebraic subset of W, then φ^{-1} is an algebraic subset of V. Also, if φ^{-1} is irreducible and $X \subset \varphi V$, then X is irreducible.*

Because of the scope of this paper, we will omit the proof of this proposition.

This proposition suggests a connection between algebraic geometry and topology, which has been developed further by Fulton and other authors. What is interesting, however, is that all of these connections exist, and that they are quite solid.

Acknowledgments. I would like to thank my mentors, Ian Shipman and Aaron Marcus, for helping me begin to understand a topic which I find very interesting (and difficult). I would like to thank Ian for reviewing the drafts of this paper. I would have understood the material we covered this summer not even half as well, were it not for all of your patience and guidance during our meetings.

References

[1] William Fulton, Algebraic Curves. Mathematics Lecture Note Series, W.A. Benjamin, 1974, available at `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`