Algebraic Geometry I

Base on lectures given by: Prof. Karen E. Smith
Notes by: David J. Bruce

These notes follow a first course in algebraic geometry designed for second year graduate students at the University of Michigan. The recommended texts accompanying this course include *Basic Algebriac Geometry I* by Igor R. Shafarevich, *Algebraic Geometry, A First Course* by Joe Harris, *An Invitation to Algebraic Geometry* by Karen Smith, and *Algebraic Geometry* by Robin Hartshorne. These notes were typed during class and then edited somewhat, and so they may not be error free. Please email me any comments, corrections, or suggestions you have at djbruce@umich.edu.

University of Michigan , Fall 2013

Table of Contents

1. First Principles

1.1 Introductory Remarks

What is algebraic geometry? A short answer to this question is that algebraic geometry is the study of algebraic varieties. Of course this begs the question: What is an algebraic variety?

Roughly speaking an algebraic variety is a geometric object modeled on zero sets of polynomials. By geometric object we mean that it is a topological space with some additional structure. A few examples of geometric objects are:

- smooth manifolds whose additional structure is a differentiable structure–the ability to differentiate functions and talk about tangent spaces.
- complex manifolds whose additional structure is a holomorphic structure,
- Riemannian manifolds whose additional structure is a Riemann metric

As a slight foreshadowing of things to come, we note that these first two objects can be described succinctly as a topological space with a sheaf of rings of functions on that space. A sheaf $\mathcal{R}$ of rings of functions on a topological space X is simply a way to assign to each open set U some natural class of functions $\mathcal{R}(U)$. The set $\mathcal{R}(U)$ should form a ring (under the usual function pointwise addition and multiplication), and the restriction of a function in $\mathcal{R}(U)$ to a smaller open set V should be in $\mathcal{R}(V)$. One additional axiom—the *sheaf axiom*— is imposed to ensure that are functions are defined by "local properties". Without getting formal, we look at a few examples:

Example 1.1.1. If X is a topological space then the continuous functions (say, to $\mathbb{R}$) form a sheaf of rings $\mathcal{C}^0_X$. For every open subset $U \subset X$, the set of continuous real valued functions on U, denoted $\mathcal{C}^0_X(U)$, forms a ring under pointwise addition and multiplication of functions. The restriction of a continuous function to a smaller open set is also continuous. Finally, the sheaf axiom in this case says that a function $U \to \mathbb{R}$ is continuous if and only if if it continuous in a neighborhood of each point of U. The sheaf $\mathcal{C}^0_X$ captures a lot of the geometry of a topological space. In fact, if X is a mildly nice space, say compact and Hausdorff, then entire space and its topology is determined solely by $\mathcal{C}^0_{\mathbb{R}}(X)$!

Example 1.1.2. If X is not just a topological space, but is also a smooth manifold then there is a sheaf of rings of smooth $\mathbb{R}$-valued functions on X. If $U \subset X$ is an open subset, then the set of smooth $\mathbb{R}$-valued functions on U denoted $\mathcal{C}^\infty_X(U)$ has a natural ring structure, and restriction provided a natural ring homomorphism $\mathcal{C}^\infty_X(U) \to \mathcal{C}^\infty_X(V)$ whenever $V \subset U$ are open sets. Again, the sheaf axiom is satisfied because a function $U \to \mathbb{R}$ is smooth if and only if it is smooth in a neighborhood of each point in U. Of course, in this above example we could replace smooth with k-times continuously differentiable function.

Example 1.1.3. Let $\mathcal{A}$ be the sheaf of analytic functions on $\mathbb{C}$ (or any complex manifold), assigning to each open set U the ring of analytic functions $\mathcal{A}(U)$ on U. Again, restriction to a smaller set will also be analytic, so we have natural ring homomorphism $\mathcal{A}(U) \to \mathcal{A}(V)$, and the sheaf axiom is satisfied since analyticity can be checked locally in a neighborhood of each point.

In a similar way, we will soon understand an algebraic variety (over, say, the field k) to be a topological space X with sheaf of rings of functions (to k) on it, denoted $\mathcal{O}_X$, called the sheaf of regular functions. However, unlike the case of smooth manifolds, where the local picture is always just an open set in $\mathbb{R}^n$, an algebraic variety can have considerably variable and interesting local structure. So we will spend a good deal of time understanding first the local picture of an algebraic variety.

1.2 Algebraic Sets

We need to formalize and understand what "modeled on zero sets of polynomials" actually means. The local picture of an algebraic variety will be an *algebraic set:*

Definition 1.2.1. Fix a ground field k. An **algebraic set** is the common zero set in k^n of a collection of polynomials $\{f_\lambda\}_{\lambda\in\Lambda}$ in $k[x_1,\ldots,x_n]$.

Stated another way, an algebraic set is a subset of k^n of the form:

$$\mathbb{V}(\{f_\lambda\}_{\lambda\in\Lambda}) := \{(a_1,\ldots,a_n)\in k^n \mid f_\lambda(a_1,\ldots,a_n)=0,\ \forall\lambda\in\Lambda\}\subset k^2$$

where $\{f_\lambda\}_{\lambda\in\Lambda}$ is some subset of polynomials in $k[x_1,\ldots,x_n]$. Note that in the definition, this set of polynomials need not be finite or even countable for that matter.

Example 1.2.1. Many of the graphs of functions common to us from high school algebra are in fact algebraic sets. For example, the unit circle is given by the algebraic set $\mathbb{V}(x^2+y^2-1)$ (see Figure 1). The hyperbola $y = 1/x$ is also an algebraic set since it is given by $\mathbb{V}(xy-1)$ (see Figure 2). Below we depict what these algebraic sets look like if we take out ground field to be the real numbers. In general we would prefer to work over an algebraically closed field, and so it is more common for us to be thinking about these as algebraic sets in $\mathbb{C}^2$. However, picturing $\mathbb{C}^2$ or $\mathbb{C}^3$ is quite difficult so we want to visualizing algebraic sets we will almost always draw our pictures over $\mathbb{R}$.

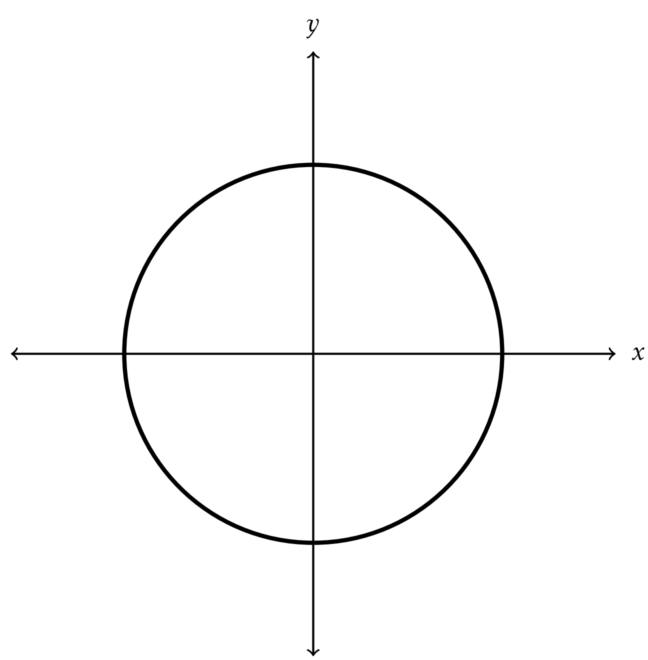


Figure 1. $\mathbb{V}(x^2+y^2-1$

Many familiar three dimensional surfaces are also algebraic sets. For example, the 'unit' cone along the z-axis is given by the algebraic set $\mathbb{V}(x^2+y^2-z^2)$ (see Figure 3). Notice at the origin this algebraic set is not a smooth manifold since it is singular. This is our first example of showing how the local properties of algebraic sets can be quite interesting!

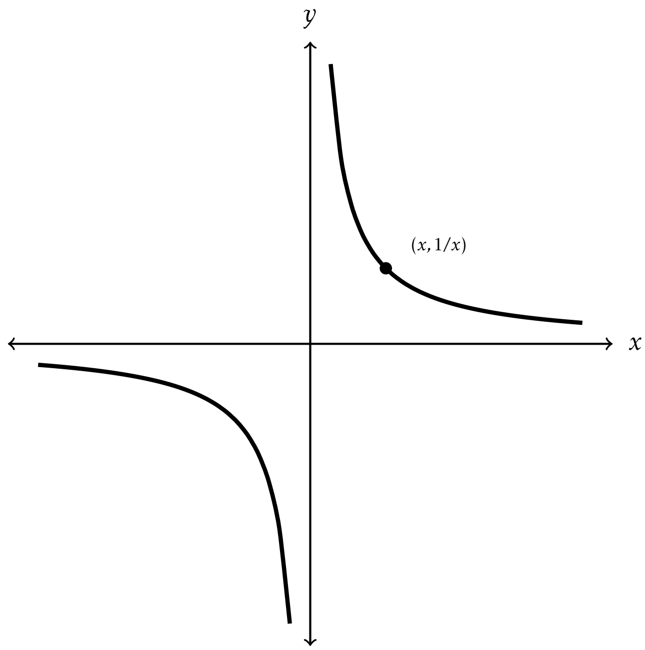


FIGURE 2. $\mathbb{V}(xy-1) \subset \mathbb{R}^2$

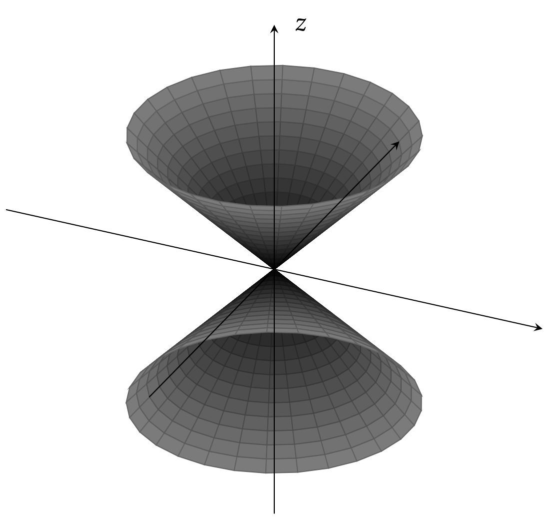


FIGURE 3. $\mathbb{V}(x^2+y^2-z^2) \subset \mathbb{R}^3$

While the above three examples are all somewhat different they are all a special type of algebraic set since they are generated by one polynomial equation.

Definition 1.2.2. A **hypersurface** in k^n is a (proper, non-empty) algebraic set which can be defined by one polynomial.

Of course not all algebraic set are hypersurfaces. For example, the algebraic set $\mathbb{V}(xz, yz)$ is not a hypersurface.

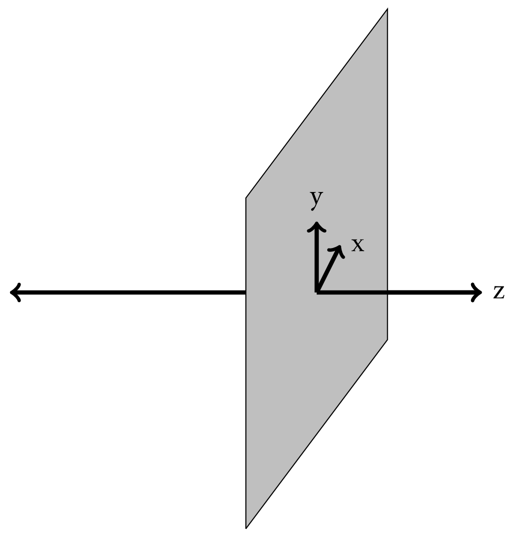


FIGURE 4. $\mathbb{V}(xz, yz) \subset \mathbb{R}^3$

From the above illustration it is clear that $\mathbb{V}(xz, yz)$ consists of the xy-plane and the z-axis. This makes sense since xz and yz are both zero when either $x = y = 0$ or $z = 0$. Therefore, this algebraic set is composed of two 'components' and $\mathbb{V}(xz, yz) = \mathbb{V}(x, y) \cup \mathbb{V}(z)$.

Note just because an algebraic set is presented as the zero set of multiple polynomials does not necessarily mean it is not a hypersurface. Consider for example the algebraic set $\mathbb{V}(\{(y - x^2)^{17+t}\}_{t \in \mathbb{N}})$. Although this algebraic set is presented by infinitely many polynomials all polynomials of the form $(y - x^2)^{17+t}$ vanish precisely when $y = x^2$. So in fact this algebraic set is a hypersurface since it is the same as $\mathbb{V}(y - x^2)$.

1.3 Some Algebraic Remarks

As noted above in our definition of algebraic sets the collection of polynomials in question need not be finite or even countable. However, we have also seen in a few examples that certain algebraic sets defined by infinite collections of polynomials can also be defined by finite collections of polynomials. Amazingly it turns out that this is always case!

Theorem 1.3.1 (**Hilbert's Basis Theorem I**). *Any algebraic set in k^n can always be defined by finitely many polynomials.*

In fact if $\mathbb{V}(\{f_\lambda\}_{\lambda \in \Lambda})$ is an algebraic set and Λ is an infinite set then their exists a finite subset $\Sigma \subset \Lambda$ such that:

$$\mathbb{V}(\{f_\lambda\}_{\lambda \in \Lambda}) = \mathbb{V}(\{f_\lambda\}_{\lambda \in \Sigma}).$$

In order to prove Hilbert's Basis Theorem we need the following lemma:

Lemma 1.3.1. *If $S \subset k[x_1, \ldots, x_n]$ is any set of polynomials and $\langle S \rangle$ is the ideal generated by S then:*

$$\mathbb{V}(S) = \mathbb{V}(\langle S \rangle) \subset k^n$$

Proof. By definition the ideal generated by S clearly contains S itself. Therefore if every element of $\langle S\rangle$ vanishes at a point $p \in k^n$ then every element of S also vanishes at p. So we know we have the following inclusion

Working towards the other inclusion suppose $p \in \mathbb{V}(S)$. In order to show that $p \in \mathbb{V}(\langle S\rangle)$ we need to show that if $f \in \langle S\rangle$ then $f(p) = 0$. However, every element of $\langle S\rangle$ is a linear combination of S. So if $f \in \langle S\rangle$ then we have that

$$f(p) = \sum_{g\in S} \lambda_g g(p).$$

So since everything in S vanishes at p so does f and hence $V(S) = \mathbb{V}(\langle(S)\rangle)$. □

With this lemma in hand we can now prove Hilbert's Basis Theorem.

Proof of Hilbert's Basis Theorem. Let S be a subset of $k[x_1, x_2, \dots, x_n]$ and $\langle(S)\rangle$ be the ideal generated by S. By our above lemma we know

$$\mathbb{V}(S) = \mathbb{V}(\langle S\rangle)$$

Since $k[x_1, x_2, \dots, x_n]$ is a Noetherian ring every ideal is finitely generated. In particular the ideal $\langle(S)\rangle$ is finitely generated meaning there exists a finite subset $I \subset \langle S\rangle$ such that $\langle I\rangle = \langle S\rangle$. Applying the above lemma one final time gives us

$$\mathbb{V}(S) = \mathbb{V}(\langle S\rangle) = \mathbb{V}(\langle I\rangle) = \mathbb{V}(I)$$

completing the proof. □

Of course the above theorem relies upon the following facts from commutative algebra which we shall assume are know to the reader or which the reader may blackbox and assume on faith.

ALGEBRA BLACKBOX:

Definition 1.3.1. A ring A satisfies the **ascending chain condition (ACC)** if and only if given any ascending chain of ideals

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$$

there exists and $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.

Proposition 1.3.1. *A ring is **Noetherian** if and only if every ideal is finitely generated.*

Theorem 1.3.2 (Hilbert's Basis Theorem II). *A is a Noetherian commutative ring then $A[x]$ is also Noetherian.*

A nice useful corollary of Hilbert's Basis Theorem is that every algebraic set is actually the intersection of finitely many hypersurfaces

Corollary 1.3.1. *Every (proper, non-empty) algebraic set in k^n is the intersection of finitely many hypersurfaces.*

Proof. By Hilbert's Basis Theorem we know that if V is an algebraic subset of k^n then $V = \mathbb{V}(f_1, \dots, f_k)$. However, by definition:

$$V = \mathbb{V}(f_1, \dots, f_k) = \mathbb{V}(f_1) \cap \mathbb{V}(f_2) \cap \cdots \cap \mathbb{V}(f_k).$$

□

1.4 The Zariski Topology

Previously we said that algebraic sets should be geometric objects in that they show be topological spaces together with some additional structure. Now that we understand algebraic sets as sets we figure out how to put a topology, or topologize, an algebraic set.

Of course if our ground field where $\mathbb{C}$ or $\mathbb{R}$ then we endow an algebraic set with the subspace Euclidean topology. Recall that if X is a topological space with topology τ and U is a subset of X then the open sets in the subspace topology on U are of the form $U \cap S$ where $S \in \tau$. However, the topology induced by the standard Euclidean topology on $\mathbb{R}$ or $\mathbb{C}$ is not really the topology we wish to work with. Additionally since we are interested in working over arbitrary fields the Eulclidean topology is not always available to us. Luckily using what we have so far done we can topologize k^n by having the algebraic sets be the closed sets in our topology.

Proposition 1.4.1. *The collection of algebraic sets $\mathcal{Z}$ in k^n form the closed sets for a topology in k^n called the* ***Zariski topology****.*

Proof. In order to check that this does in fact define a topology we must check that the following four axioms of a topology hold:

(1) k^n is closed.

(2) $\varnothing$ is closed.

(3) $\mathcal{Z}$ is closed under finite union.

(4) $\mathcal{Z}$ is closed under arbitrary intersection.

Axioms (1) and (2) are easy to check First, since the constant polynomial with value zero is zero on all of k^n we have that $\mathbb{V}(0) = k^n$. Similarly, any non-zero constant polynomial vanishes nowhere meaning $\mathbb{V}(c) = \varnothing$ for any $c \in k \setminus \{0\}$. Thus, both the empty set and all of k^n are closed.

Checking the fourth axiom is not much harder. In particular if $\{S_\lambda\}_{\lambda\in\Lambda}$ is an collection of subset of $k[x_1,\dots,x_n]$ then

$$\bigcap_{\lambda\in\Lambda} \mathbb{V}(S_\lambda) = \{p \in k^n : p \in \mathbb{V}(S_\lambda),\ \forall \lambda \in \Lambda\}.$$

However, expanding the chasing through what it means for a point p to be in $\mathbb{V}(S_\lambda)$ we find that

$$\bigcap_{\lambda\in\Lambda} \mathbb{V}(S_\lambda) = \mathbb{V}\left(\bigcup_{\lambda\in\Lambda} S_\lambda\right).$$

Meaning that $\mathcal{Z}$ is closed under arbitrary intersection.

So we are left to verify the axiom (3) above. Towards this let $\mathbb{V}(\{f_i\}_{i\in I})$ and $\mathbb{V}(\{g_j\}_{j\in J}$ be two algebraic sets. Now clearly $\mathbb{V}(\{f_i g_j\}_{(i,j)\in I\times J})$ is also an algebraic closed set. Further, since $f_i g_j$ vanishes at a point p if and only if either $f_i(p) = 0$ or $g_j(p) = 0$ we have that

$$\mathbb{V}(\{f_i g_j\}_{(i,j)\in I\times J}) = \mathbb{V}(\{f_i\}_{i\in I}) \cup \mathbb{V}(\{g_j\}_{j\in J}.$$

Thus, the union of two algebraic sets is itself an algebraic set, and so by induction $\mathcal{Z}$ is closed under finite union. □

Let us familiarize ourselves with the Zariski topology by considering the following questions:

(1) On $\mathbb{R}^n$ how does the Zariski topology compare to the Euclidean topology?

(2) Is the Zariski topology in k^n Hausdorff?

Example 1.4.1. If k is an infinite field, for example $\mathbb{C}$ or $\mathbb{R}$, then closed sets in Zariski topology on k are the algebraic sets. However, a polynomial in $k[x]$ has only finitely many roots, and so any algebraic set in k can contain only finitely many roots. For example, if $k = \mathbb{R}$ this means that $\mathbb{Z}$ or $\mathbb{Q}$ are not Zariski closed subset. So the Zariski closed sets in k are precisely finite subsets of k; meaning the Zariski topology on k is just the confine topology!

On the other hand if k is a finite field then any subset S of k is also finite. Therefore, by letting

$$f(x) = \prod_{s\in S}(x - s)$$

we see that S is an algebraic subset of k. Hence every subset of k is closed meaning the topology on k is just the discrete topology!

Now that we have some understanding of what the Zariski topology looks like on k let us consider how it compares to other topologies, namely the Euclidean topology on $\mathbb{R}^n$. If V is a closed subset of $\mathbb{R}^n$ in the Zariski topology then by Corrollary 1.3.1:

$$V = \mathbb{V}(f_1) \cap \mathbb{V}(f_2) \cap \cdots \cap \mathbb{V}(f_k).$$

However, the zero set of a f_i is precisely $f_i^{-1}(\{0\})$. Since polynomials are continuous in the Euclidean topology this means $\mathbb{V}(f_i)$ is closed and hence V is closed. So any Zariski closed set is always closed in the Euclidean topology. Of course the converse of this statement is not true as clearly there are sets closed in the Euclidean topology, which are not the vanishing set of a collection of polynomials. Thus, the Zariski topology is much coarser than the Euclidean topology in the sense that it has a lot fewer closed sets. It turns out the Zariski topology in general the Zariski topology on k^n has very few closed sets. In fact, under the Zariski topology k^n is what is called a Noetherian space.

Definition 1.4.1. A topological space X is **Noetherian Space** if and only if for every chain of closed subsets

$$U_1 \supset U_2 \supset U_3 \supset \cdots$$

there exists and $N \in \mathbb{N}$ such that $U_n = U_N$ for $n \geq N$.

Right now we shall not prove the k^n with the Zariski topology is in fact Noetherian, however, we it will become obvious once we prove one big theorem. Not only does the Zariski topology have few open sets, but the case when k is infinite the open sets are massive. In fact not only is the Zariski topology not Hausdorff , but any two open sets have nonempty intersection. Note to show this it is in fact equivalent to show that the union of two proper closed subsets cannot be all of k^n. To see this notice by our above work it suffices to consider the union of two proper hypersurfaces $\mathbb{V}(f)$ and $\mathbb{V}(g)$. By Proposition **??** we know that $\mathbb{V}(f) \cup \mathbb{V}(g)$ is equal to $\mathbb{V}(fg)$, which is only k^n if $fg \equiv 0$. However, since both $\mathbb{V}(f)$ and $\mathbb{V}(g)$ are proper closed subsets neither f nor g is the zero polynomial and hence fg is also not the zero polynomial. Therefore, the intersection of proper Zariski closed subsets of k^n cannot itself be k^n. So if k is infinite the Zariski topology is not Hausdorff!

2. Building Our Algebra-Geometry Dictionary

In many ways the main idea underlying algebraic geometry is the notion that the geometry of algebraic sets can be captured and described algebraically. In this way we might hope that difficult geometric questions may be translated into more tractable algebraic questions. However, before we can begin translating we must first build a dictionary that allows us to move between the world of geometry and the world of algebra.

2.1 Functions vs. Expressions

Before we begin building up our dictionary let us take a few minutes to review a notions, which although basic is often confusion and will be fundamental later on. In particular, we need to understand the difference between polynomials expressions and polynomial functions.

Towards this let us begin very generally by considering a the set of all functions from S to k where S is set and k is a field. Note there are many ways to denote this set, but we will most often use either $\mathcal{F}_{S \to k}$ or $\mathrm{Hom}_{\mathbf{Set}}(S, k)$. This set $\mathrm{Hom}_{\mathbf{Set}}(S, k)$ actually has a natural ring structure where addition and multiplication are given by

$$(f+g)(x) = f(x) + g(x) \qquad \text{and} \qquad (f \cdot g)(x) = f(x)f(g).$$

Further, notice if $c \in k$ we can define a function $f : S \longrightarrow k$ by $f(s) = c$ for all $s \in S$. It is easy to check that this set of constant functions on k forms a subring of $\mathcal{F}_{S \to k}$. Thus, the set of k-valued functions on S is not only a ring, but also a k-algebra.

If we take $S = k^n$ where k is a field then $\mathrm{Hom}_{\mathbf{Set}}(k^n, k)$ is the ring of all functions from k^n to k. Within this ring there is the subring of polynomial functions on k^n, but exactly are the polynomial functions on k^n? While we often think about elements of $k[x_1, \ldots, x_n]$ as polynomial *functions* they are in fact formally not functions. Formally elements of $k[x_1,\dots,x_n]$ are just formal sums of monomials in $x_1,\dots,x_n$, which we call polynomial *expressions*. Of course there is a ring homomorphism:

$$k[x_1,\dots,x_n] \longrightarrow \mathrm{Hom}(k^n,k)$$

$$f \longmapsto \begin{bmatrix} f : k^n \longrightarrow k \\ X \longmapsto f(X) \end{bmatrix}$$

In general if k is not finite this map will not be surjective, however, it will be injective. On the other hand if k is finite then this map is in fact surjective, since any function on k takes on finitely many values and hence can be interpolated by a polynomial. However, when k is finite we also know that this map cannot be injective since by Fermat's Little Theorem $x^p = x$. We call the image of this map the ring of polynomial functions, and denote it by $k[k^n]$. For reasons that will become apparent shortly it is important to realize that polynomial functions need not themselves be polynomial expressions, but instead just in the image of this map.

2.2 Coordinate Rings

Now that we understand what the k-algebra of polynomial functions on k^n are we want to generalize this to understand polynomial functions on any algebraic set. This highlights what in many ways is a major theme of modern mathematics. Namely the set morphisms on a space often capture many properties of the space. So if we want to study spaces we really ought to study the set of functions on them. For example, if X is a topological space then many properties of X can be captured by studying the set of maps $S^1 \longrightarrow X$ – in fact this basic notion behind the fundamental group of X.

Definition 2.2.1. The **coordinate ring** of an algebraic set $V \subset k^n$ denoted $k[V]$ is the ring of all polynomial functions on V.

Put another way, the coordinate ring of an algebraic set V is the set:

$$k[V] = \left\{ f \in \mathrm{Hom}_{\mathbf{Set}}(V,k) \,\middle|\, \exists g \in k[x_1,\dots,x_n], g \equiv f|_V \right\}.$$

Note it is often tempting to think of the coordinate ring consists solely of polynomial expression, however, this is not the case. One must be careful to remember that polynomial functions need not be given by polynomial expressions. For example, if we take V to be $\mathbb{V}(x^2-y)$ in $\mathbb{R}^2$ then even though $f(x,y) = e^{x^2} - e^y + xy$ is not a polynomial expression it is contained in $\mathbb{R}[x,y]$. In particular, if $x^2 - y = 0$ then

$$f(x,y) = e^{x^2} - e^y + xy = e^{x^2} - e^{x^2} + x^3 = x^3$$

so $f(x,y)$ is in fact a polynomial function on V.

While the coordinate ring of an algebraic set contains functions, which are not polynomial expressions there is a natural surjective ring homomorphism:

$$k[x_1,\dots,x_n] \longrightarrow k[V]$$
$$f \longmapsto g|_V$$

By the first isomorphism theorem this means that $k[V]$ is isomorphic to $k[x_1,\dots,x_n]$ modulo the kernel of this map, which we shall denote $\mathbb{I}(V)$. However, a polynomial f is in the kernel of this map if and only if f restriction to V is equivalently zero. So $\mathbb{I}(V)$ is precisely the ideal of polynomials in $k[x_1,\dots,x_n]$, which vanish on V i.e.

$$\mathbb{I}(V) = \{ f \in k[x_1,\dots,x_n] \,|\, f|_v \equiv 0 \}$$

This ideal and indeed the coordinate ring of an algebraic set turn out to have quite special algebraic properties. However, before we discuss these we must recall a few notions from basic commutative algebra the exact details of which we shall blackbox:

Algebra Blackbox:

Definition 2.2.2. If I is an ideal in a commutative ring R then the radical of I denoted by either $\sqrt{I}$ or $\mathrm{Rad}(I)$ is

$$\sqrt{I} := \{r \in R \,|\, r^n \in I \text{for some } n > 0\}.$$

Proposition 2.2.1. *The radical ideal of an ideal $I \subset R$ is itself and ideal of R.*

Definition 2.2.3. An ideal I in a commutative ring R is radical if and only if $I = \sqrt{I}$.

Definition 2.2.4. A commutative ring R is reduced if and only if there are no nonzero nilpotent elements.

Proposition 2.2.2. *A commutative is reduced if and only if the zero ideal is radical.*

Proposition 2.2.3. *The quotient ring R/I is reduced if and only if I a radical ideal.*

Having reviewed these concepts we can now state the first important property of $\mathbb{I}(V)$.

Proposition 2.2.4. *If V is an algebraic set in k^n then the ideal $\mathbb{I}(V)$ is radical in $k[x_1, \ldots, x_n]$.*

Proof. Clearly, the radical of $\mathbb{I}(V)$ contains $\mathbb{I}(V)$ and so to show that $\mathbb{I}(V)$ is radical we are left to show the other inclusion. Towards this let $f \in \mathrm{Rad}(\mathbb{I}(V))$ meaning that there exists $n \in \mathbb{N}$ such that f^n is in $\mathbb{I}(V)$. If f^n is in $\mathbb{I}(V)$ then f^n vanishes on V, and since $\mathbb{C}[x_1, \ldots, x_n]$ is reduced this implies that f must be zero on V. Therefore, f itself is in $\mathbb{I}(V)$ and so $\mathbb{I}(V)$ is radical. □

Now that we know $\mathbb{I}(V)$ is a radical ideal it follows from Proposition 2.2.3 that $k[V]$ is reduced. Additionally, $k[V]$ clearly contains a copy of k as a subring since the only constant function in $\mathbb{I}(V)$ is the zero function. Therefore, we see that to every algebraic set we can associated a finitely generated, reduced, k-algebra we call its coordinate ring.

2.3 Hilbert's Nullstellensatz

Let us take a brief moment to review what we have so far accomplished. Given an ideal I in $k[x_1, \ldots, x_n]$ we have an associated subset of k^n, the algebraic subset $\mathbb{V}(I)$. Put another way we have a map:

$$\left\{ \begin{matrix} \text{Ideals in} \\ k[x_1, \ldots, x_n] \end{matrix} \right\} \xrightarrow{\mathbb{V}} \left\{ \begin{matrix} \text{Algebraic Subsets} \\ \text{in } k^n \end{matrix} \right\}$$

given by sending and ideal I to $\mathbb{V}(I)$. Additionally we have shown that given an algebraic set V in k^n we can construct an ideal $\mathbb{I}(V)$ by considering the kernel of the restriction from $k[x_1, \ldots, x_n]$ to the coordinate ring $k[V]$. Stated differently this means we have a map:

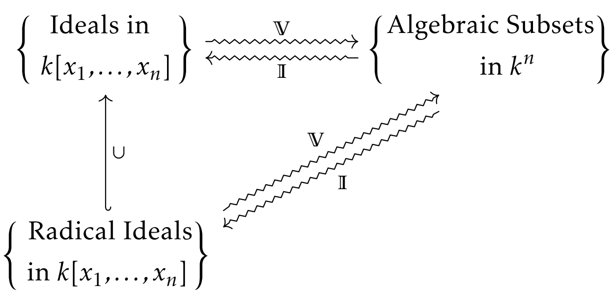
$$\left\{ \begin{matrix} \text{Ideals in} \\ k[x_1, \ldots, x_n] \end{matrix} \right\} \xleftarrow{\mathbb{I}} \left\{ \begin{matrix} \text{Algebraic Subsets} \\ \text{in } k^n \end{matrix} \right\}$$

given by sending an algebraic set V to $\mathbb{I}(V)$. As with $\mathbb{V}$ above this is map is also order reversing. Namely if $V \subset W$ are algebraic sets in k^n then since element of $\mathbb{I}(W)$ vanishes W it also vanishes on V meaning $\mathbb{I}(V) \subset \mathbb{I}(W)$.

This leads one to the natural question: Are $\mathbb{V}$ and $\mathbb{I}$ inverses? However, before we answer this question we should first check whether $\mathbb{I}$ and $\mathbb{V}$ as defined above are even bijective. Recall from Proposition 2.2.4 that if V is an algebraic set then $\mathbb{I}(V)$ is a radical ideal. Further, regardless of the ground field the ideal (x_1^2)

is always not radical in $k[x_1,\ldots,x_n]$. Thus, clearly $\mathbb{I}$ is not a bijection between the algebraic sets in k^n and ideals in $k[x_1,\ldots,x_n]$ since its image is solely radical ideals in $k[x_1,\ldots,x_n]$.

In light of this we might wonder whether $\mathbb{I}$ and $\mathbb{V}$ are inverse if we restrict our attention from all ideals in $k[x_1,\ldots,x_n]$ to only radical ideals in $k[x_1,\ldots,x_n]$?



With this new setup it seems at least plausible that $\mathbb{I}$ and $\mathbb{V}$ are mutually inverse bijections. In fact, if V is an algebraic subset of k^n then $\mathbb{V}(\mathbb{I}(V)) = V$. To see this note that by definition $\mathbb{I}(V)$ is the ideal of all functions vanishing on V, and so clearly V is contained in $\mathbb{V}(\mathbb{I}(V))$. On the other hand suppose $V = \mathbb{V}(I)$ for some ideal I. Since every element of I vanishes on V we have that $I \subset \mathbb{I}(V)$, and so applying the fact that $\mathbb{V}$ is order reversing we can conclude that $\mathbb{V}(\mathbb{I}(V)) \subset \mathbb{V}(I) = V$ and so $\mathbb{V}(\mathbb{I}(V)) = V$.

Additionally, suppose I is any ideal in $k[x_1,\ldots,x_n]$, not necessarily radical. Since every element of I vanishes on $\mathbb{V}(I)$, and $\mathbb{I}(\mathbb{V}(I))$ consists of every polynomial vanishing on $\mathbb{V}(I)$ it is the case that $I \subset \mathbb{I}(\mathbb{V}(I))$. In summary in working towards proving that $\mathbb{V}$ and $\mathbb{I}$ are mutually inverse bijections between algebraic subsets of k^n and the radical ideals in $k[x_1,\ldots,x_n]$ we have shown:

Lemma 2.3.1. *Fix a field k, not necessarily algebraically closed. Let W and V be algebraic sets in k^n such that $W \subset V$ and $I \subset J$ be any ideals in $k[x_1,\ldots,x_n]$ then*

$$\mathbb{V}(V) \subset \mathbb{V}(W) \qquad \textit{and} \qquad \mathbb{I}(J) \subset \mathbb{I}(I).$$

i.e. $\mathbb{V}$ and $\mathbb{I}$ are order reversing maps.

Lemma 2.3.2. *Fix a field k, not necessarily algebraically closed. Let V be an algebraic set in k^n and I be any ideal in $k[x_1,\ldots,x_n]$, not necessarily radical, then*

$$\mathbb{V}(\mathbb{I}(V)) = V \qquad \textit{and} \qquad I \subset \mathbb{I}(\mathbb{V}(I)).$$

Therefore, to show that $\mathbb{I}$ and $\mathbb{V}$ are in fact mutually inverse bijections we are left only to show that $\mathbb{I}(\mathbb{V}(I)) \subset I$. Sadly it turns out that this is not always true even if I is a radical ideal.

Example 2.3.1. For example, let us look at the principle ideal (x^2+y^2) in $\mathbb{R}[x,y]$. Since x^2+y^2 is irreducible over $\mathbb{R}$ this ideal is in fact a prime ideal, and hence is also radical. Further since x^2 and y^2 are both always positive over $\mathbb{R}$ we know that $\mathbb{V}(x^2+y^2) = \{(0,0)\}$. However, clearly the ideal (x,y) also vanishes on $\{(0,0)\}$, and so since (x,y) is a maximal ideal this means the $\mathbb{I}(\mathbb{V}(x^2+y^2)) = (x,y)$. So

Looking closely at the above example it seems the reason that this example worked out as it did is because x^2+y^2 is irreducible over $\mathbb{R}$. Namely if in the above example we change $\mathbb{R}$ to $\mathbb{C}$ then x^2+y^2 is not a radical ideal. It turns out that this is in essence the only problem stoping $\mathbb{I}$ and $\mathbb{V}$ from being mutual inverse. In particular if k is an algebraically closed field then a deep result due to Hilbert says that $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ for any ideal I. Utilizing this result precisely gives us the result we desired, which is one of the many versions of Hilbert's Nullstellensatz

Theorem 2.3.1 (**Hilbert's Nullstellensatz I**). *If k is an algebraically closed field then the mappings $\mathbb{I}$ and $\mathbb{V}$*

$$\left\{\begin{matrix} \textit{Radical Ideals} \\ \textit{in } k[x_1,\ldots,x_n] \end{matrix}\right\} \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} \left\{\begin{matrix} \textit{Algebraic Subsets} \\ \textit{in } k^n \end{matrix}\right\}$$

are mutually inverse order reversing bijections.

We shall not take the time to prove the remaining details of Hilbert's Nullstellensatz, but instead shall blackbox. Those interested in the proof should consult pages 42-44 of [2] or Section 4.5 of [1]. Note however that the requirement that k be algebraically closed is absolutely necessary. If k is not algebraically closed then there exists a polynomial $f \in k[x]$, which does not have a root in k. Taking f to be irreducible we know the principle ideal it generates is prime and hence radical. Further since f has no roots in k it is the case that $\mathbb{V}(f) = \emptyset$, however, $\mathbb{I}(\emptyset) = (1)$ and so the correspondence does not work.

Index

References

[1] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*. New York.
[2] James S. Milne. Algebraic geometry v5.22. Technical report, 2012.