Georgia State University
Digital Archive @ GSU

Mathematics Theses | Department of Mathematics and Statistics

11-15-2012

The Topology and Algebraic Functions on Affine Algebraic Sets Over an Arbitrary Field

Anthony J. Preslicka
apreslicka1@gsu.edu

Follow this and additional works at: http://digitalarchive.gsu.edu/math_theses

Recommended Citation
Preslicka, Anthony J., "The Topology and Algebraic Functions on Affine Algebraic Sets Over an Arbitrary Field" (2012). *Mathematics Theses.* Paper 121.

This Thesis is brought to you for free and open access by the Department of Mathematics and Statistics at Digital Archive @ GSU. It has been accepted for inclusion in Mathematics Theses by an authorized administrator of Digital Archive @ GSU. For more information, please contact digitalarchive@gsu.edu.

THE TOPOLOGY AND ALGEBRAIC FUNCTIONS ON AFFINE ALGEBRAIC SETS OVER AN ARBITRARY FIELD

by

ANTHONY PRESLICKA

Under the Direction of Dr. Florian Enescu

ABSTRACT

This thesis presents the theory of affine algebraic sets defined over an arbitrary field K. We define basic concepts such as the Zariski topology, coordinate ring of functions, regular functions, and dimension. We are interested in the relationship between the geometry of an affine algebraic set over a field K and its geometry induced by the algebraic closure of K. Various versions of Hilbert-Nullstellensatz are presented, introducing a new variant over finite fields. Examples are provided throughout the paper and a question on the dimension of irreducible affine algebraic sets is formulated.

INDEX WORDS: Affine algebraic sets, Irreducible affine algebraic sets, Non-algebraically closed fields, Zariski topology, K-radical ideals, Dimension, Coordinate ring, Regular functions

THE TOPOLOGY AND ALGEBRAIC FUNCTIONS ON AFFINE ALGEBRAIC SETS OVER AN ARBITRARY FIELD

by

ANTHONY PRESLICKA

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science

in the College of Arts and Sciences

Georgia State University

2012

Copyright by
Anthony Preslicka
2012

THE TOPOLOGY AND ALGEBRAIC FUNCTIONS ON AFFINE ALGEBRAIC SETS OVER AN ARBITRARY FIELD

by

ANTHONY PRESLICKA

Committee Chair: Dr. Florian Enescu

Committee: Dr. Frank Hall

Dr. Yongwei Yao

Electronic Version Approved:

Office of Graduate Studies

College of Arts and Sciences

Georgia State University

December 2012

This thesis is dedicated to my brother, Addison John Preslicka.

Thank you.

ACKNOWLEDGMENTS

My utmost appreciation goes to Dr. Florian Enescu for his undying persistence and patience. Thank you for your remarkable support and shared wisdom. I thank Frank Hall and Yongwei Yao for their inspirational passion and help finalizing this thesis. The entire Department of Mathematics and Statistics at Georgia State University deserves thanks for all their support and professional guidance.

I am grateful to all my colleagues and friends for their restless encouragement, especially Sara Malec and Harrison Stalvey. Lastly, I thank my family for everything.

TABLE OF CONTENTS

ACKNOWLEDGMENTS . . . . . **v**

CHAPTER 1 BASIC ALGEBRAIC GEOMETRY **1**

1.1 Introduction 1

1.2 Commutative Algebra 2

1.3 Affine Algebraic Sets 6

1.4 Vanishing Ideals 10

1.5 Zariski Topology 16

1.6 Rational Points 23

1.7 Hilbert Nullstellensatz 28

CHAPTER 2 TOPOLOGY AND DIMENSION **36**

2.1 Maps on Irreducible Affine Algebraic Sets 36

2.2 Zariski Topologies 41

2.3 Dimension 45

REFERENCES **50**

CHAPTER 1

BASIC ALGEBRAIC GEOMETRY

1.1 Introduction

Algebraic geometry is a branch of mathematics that is concerned with the geometric structure of the solution set to a system of polynomial equations. Classically, this theory is developed over algebraically closed fields, providing a natural duality between geometry and algebra. Most expositions on the subject consider only this classic case. In an attempt to better understand this interplay, this paper develops basic algebraic geometry over arbitrary fields, particularly non-algebraically closed fields. The theory of affine algebraic sets is emphasized.

We begin with an overview of standard results from commutative algebra. Then proceed to introduce our main objects of study, affine algebraic sets. After examining a number of examples, we study their algebraic counterpart, the vanishing ideals. The paper continues by describing relationships between the two, necessarily providing an introduction to the Zariski topology. The first chapter concludes with the classical Hilbert-Nullstellensatz and its various generalizations.

Chapter 2 begins by defining the maps between affine algebraic sets. We then introduce a generalization of the Zariski topology, which sheds light on our sought after duality. Finally, we end with a few remarks on the dimension of affine algebraic sets.

This paper contains an original generalization of the Hilbert-Nullstellensatz over finite fields. We also give an example of a non-elliptic curve with finitely many rational points.

1.2 Commutative Algebra

It is difficult to escape commutative algebra when developing algebraic geometry. Hence, this section provides an overview of standard commutative algebra results, introducing notation and preliminary definitions. Since this thesis is primarily concerned with the geometric aspects of algebraic objects, we simply state without proof the theorems needed from commutative algebra. The interested reader is kindly referred to [2], [6], and [9] for a more in depth exposition and details concerning the proofs.

The sets of non-negative integers, rationals, reals, and complex numbers are respectively denoted by $\mathbb{N}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. All rings are assumed to be non-zero and commutative with multiplicative identity, 1. A ring homomorphism is assumed to map 1 to 1. We reserve the symbol R to denote a ring.

A *field* is a ring such that every non-zero element is a unit. We reserve the symbol $\mathbb{K}$ to denote an arbitrary field. Throughout this thesis $\mathbb{K}$ is assumed to be a non-algebraically closed field, unless otherwise stated.

Let $\mathbb{K} \subseteqq \mathbb{L}$ be a field extension. An element $c \in \mathbb{L}$ is *algebraic* over $\mathbb{K}$ if there exists some non-zero univariate polynomial $f(x)$ with coefficients in $\mathbb{K}$ such that $f(c) = 0$. A field extension $\mathbb{K} \subseteqq \mathbb{L}$ is *algebraic* if every element of $\mathbb{L}$ is algebraic over $\mathbb{K}$. A field $\mathbb{K}$ is *algebraically closed* if every non-constant univariate polynomial $f(x)$ with coefficients in $\mathbb{K}$ has a *root* in $\mathbb{K}$, i.e., there exists $b \in \mathbb{K}$ such that $f(b) = 0$. Every field $\mathbb{K}$ has an algebraic field extension which is algebraically closed, known as the *algebraic closure* of $\mathbb{K}$, denoted $\overline{\mathbb{K}}$.

Definition 1.2.1. The *polynomial ring* in n-variables over $\mathbb{K}$ is the set of all polynomials in n variables with coefficients from $\mathbb{K}$, that is

$$\mathbb{K}[x_1, x_2, \ldots, x_n] := \left\{ \sum_{\alpha \in \Lambda} a_\alpha x^\alpha \mid \text{ where } \Lambda \subseteqq \mathbb{N}^n \text{ and } |\Lambda| < \infty \text{ with } a_\alpha \in \mathbb{K} \right\}.$$

We will simply denote $\mathbb{K}[x_1, x_2, \ldots, x_n]$ as $\mathbb{K}[\underline{x}]$. Since all fields are commutative, this implies $\mathbb{K}[\underline{x}]$ is also commutative. We now recall types of ideals associated with a ring R.

Definition 1.2.2. Let R be a ring.

(i) Let S be a subset of R. The *ideal generated* by S is the smallest ideal of R that contains S,

$$\langle S \rangle := \left\{ \sum_i r_i s_i \;\middle|\; r_i \in R, s_i \in S \text{ and the sum is finite} \right\}.$$

(ii) An ideal $\mathfrak{p}$ of R is a *prime* ideal if $\mathfrak{p}$ is a proper ideal and $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Equivalently, $R/\mathfrak{p}$ is an integral domain.

(iii) An ideal $\mathfrak{m}$ of R is a *maximal* ideal if $\mathfrak{m}$ is maximal among all proper ideals of R. Equivalently, $R/\mathfrak{m}$ is a field.

(iv) The *radical* of an ideal $\mathfrak{b}$ of R is defined by

$$\sqrt{\mathfrak{b}} := \{ f \in R \mid f^m \in \mathfrak{b} \text{ for some positive integer } m \}.$$

We say $\mathfrak{b}$ is *radical* when $\mathfrak{b} = \sqrt{\mathfrak{b}}$.

Example 1.2.3. Consider $\mathbb{R}[x, y]$ and the chain of ideals,

$$\langle x(x-1) \rangle \subsetneqq \langle x \rangle \subsetneqq \langle x, y \rangle \subsetneqq \langle 1 \rangle = \mathbb{R}[x, y].$$

The first ideal is a radical ideal that is not a prime ideal. The second ideal is a prime ideal that is not a maximal ideal. The third ideal is a maximal ideal.

Every maximal ideal is a prime ideal, and every prime ideal is a radical ideal. However, there exist prime ideals that are not maximal, and radical ideals that are not prime as example 1.2.3 shows. Recall the polynomial ring $\mathbb{K}[\underline{x}]$ is a unique factorization domain. This implies that irreducible elements of $\mathbb{K}[\underline{x}]$ generate prime ideals.

Lemma 1.2.4. Let $\varphi: R \longrightarrow B$ be a ring homomorphism and let $\mathfrak{b}$ be an ideal of B. Then $\varphi^{-1}(\mathfrak{b})$ is an ideal of R. In particular, if $\mathfrak{b}$ is a prime ideal of B, then $\varphi^{-1}(\mathfrak{b})$ is a prime ideal of R.

In Lemma 1.2.4, $\varphi^{-1}(\mathfrak{b})$ is known as the *contraction* of $\mathfrak{b}$ in R, denoted by $\mathfrak{b}^c$. For an ideal $\mathfrak{a} \leq R$, we define the *extension* of $\mathfrak{a}$, $\mathfrak{a}^e$, to be the ideal $\varphi(\mathfrak{a})B$ generated by $\varphi(\mathfrak{a})$ in B.

Lemma 1.2.5. Let $\varphi: R \longrightarrow B$ be a ring homomorphism and let $\mathfrak{b}$ be an ideal of B and $\mathfrak{a}$ be an ideal of R. Then,

$$\sqrt{a}^e \subseteq \sqrt{\mathfrak{a}^e} \text{ and } \sqrt{\mathfrak{b}}^c = \sqrt{\mathfrak{b}^c}.$$

Theorem 1.2.6. Let R be a ring and let I be an ideal of R. The projection $\pi: R \longrightarrow \frac{R}{I}$ induces a bijective correspondence between the ideals of R that contain I and the ideals of $\frac{R}{I}$. In particular, π preserves radical, prime, and maximal ideals for ideals of R containing I.

A ring R is a *local* ring if R has exactly one maximal ideal, $\mathfrak{m}$, denoted $(R, \mathfrak{m})$.

Lemma 1.2.7. A ring R is a local ring if and only if the non-units form an ideal.

Lemma 1.2.8 (Zorn's lemma). If a partially ordered set P has the property that every totally ordered subset has an upper bound in P, then the set P contains a maximal element.

Recall that an *R-module* M is an additive abelian group with scalar multiplication satisfying the following conditions for all $r, s \in R, a, b \in M$:

(i) $r(a+b) = ra + rb$

(ii) $(r+s)a = ra + sa$

(iii) $r(sa) = (rs)a$

(iv) $1a = a$.

Definition 1.2.9. M is a *finitely generated* R-module or is known as *module-finite* if there exist elements $y_1, y_2, \ldots, y_m \in M$ for some $m \in \mathbb{N}$ such that every element of M may be expressed as a linear combination of the y_i with coefficients from R.

Definition 1.2.10. An *R-algebra* is a ring A together with a ring homomorphism $i_A: R \longrightarrow A$.

Definition 1.2.11. An *R-algebra homomorphism* is a homomorphism of rings $\varphi: A \longrightarrow B$ such that $\varphi(i_A(R)) = i_B(R)$.

Definition 1.2.12. A is a *finitely generated* R-algebra if there exist elements $x_1, x_2, \ldots, x_m \in A$ for some $m \in \mathbb{N}$ such that every element of A may be expressed as a polynomial in x_i with coefficients from R, i.e., there is a surjective R-algebra homomorphism $R[x_1, x_2, \ldots, x_n] \longrightarrow A$.

Theorem 1.2.13. Let A be a finitely generated $\mathbb{K}$-algebra that is an integral domain. Let $Frac(A)$ be its field of fractions. Then the Krull dimension of A is equal to the transcendence degree of $Frac(A)$ over $\mathbb{K}$.

An element b of an R-algebra A is *integral* over R if there exists a monic univariate polynomial $f(x)$ with coefficients from R such that $f(b) = 0$. If every element of A is integral over R, then A is *integral* over R. Equivalently, A is an *integral extension* of R

Definition 1.2.14. Let R be a ring. We say R is *Noetherian* if every ascending chain of ideals eventually stabilizes:

$$I_0 \subseteqq I_1 \subseteqq \ldots \subseteqq I_m \subseteqq \ldots \Rightarrow \text{ there exists a positive integer } m \text{ such that } I_m = I_{m+1} = \ldots$$

Equivalently, every ideal of a *Noetherian* ring is generated by a finite number of elements from R.

Theorem 1.2.15 (Hilbert Basis Theorem). If R is a Noetherian ring, then the polynomial ring $R[x]$ is also Noetherian.

Any field $\mathbb{K}$ is a Noetherian ring. Therefore, by the Hilbert Basis Theorem, $\mathbb{K}[x]$ is also Noetherian. Proceeding inductively, we see that $\mathbb{K}[\underline{x}]$ is Noetherian.

Lemma 1.2.16. Let $\mathbb{K}$ be a field and let $\mathbb{F} \subseteqq \mathbb{K}$ be a subring. If $\mathbb{K}$ is a module-finite $\mathbb{F}$-algebra, then $\mathbb{F}$ is also a field.

Theorem 1.2.17. [[6], Theorem 7.5] Let $f\colon A \longrightarrow B$ be a faithfully flat ring homomorphism. If I is an ideal of A then $IB \cap A = I$.

Theorem 1.2.18 (Noether's Normalization Lemma). Let $\mathbb{K}$ be a field and let A be a finitely generated $\mathbb{K}$-algebra. Then there exist $y_1, y_2, \ldots, y_m \in A$ such that the y_j are algebraically independent and A is integral over $\mathbb{K}[y_1, y_2, \ldots, y_m]$. If we assume $\mathbb{K}$ is infinite, we may also choose the y_j to be $\mathbb{K}$-linear combinations of the x_i

1.3 Affine Algebraic Sets

Recall, we assume $\mathbb{K}$ to be an arbitrary field. From $\mathbb{K}$, we define a space.

Definition 1.3.1. The *n-dimensional affine space* over $\mathbb{K}$ is the set of n-tuples of elements of $\mathbb{K}$,

$$\mathbb{A}^n_{\mathbb{K}} := \mathbb{K}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{K}\}.$$

As sets, the n-dimensional affine space over $\mathbb{K}$ is equal to the n-dimensional vector space over $\mathbb{K}$. However, we simply write $\mathbb{A}^n_{\mathbb{K}}$ rather than $\mathbb{K}^n$ to signify a different topology than the Euclidean topology. Additionally, we denote an element of $\mathbb{A}^n_{\mathbb{K}}$ as $\underline{a}$, rather than the more cumbersome $(a_1, a_2, \ldots, a_n)$. In this affine space we will examine certain subsets known as *affine algebraic sets.*

Definition 1.3.2. A subset $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ is an *affine algebraic set* if there exists a subset $B \subseteqq \mathbb{K}[\underline{x}]$ such that

$$V = \mathcal{Z}_{\mathbb{K}}(B), \text{ where } \mathcal{Z}_{\mathbb{K}}(B) := \{\underline{a} \in \mathbb{A}^n_{\mathbb{K}} \mid f(\underline{a}) = 0 \text{ for all } f \in B\}.$$

Notice in definition 1.3.2 that B is a subset of the polynomial ring $\mathbb{K}[\underline{x}]$ rather than an ideal. This distinction is irrelevant as the following proposition shows. Additionally, we refer to an affine algebraic set simply as an algebraic set.

Proposition 1.3.3. Let $B, C \subseteqq \mathbb{K}[\underline{x}]$.

(i) $\mathcal{Z}_{\mathbb{K}}$ is inclusion-reversing: If $B \subseteqq C$, then $\mathcal{Z}_{\mathbb{K}}(C) \subseteqq \mathcal{Z}_{\mathbb{K}}(B)$.

(ii) Affine algebraic sets are defined by ideals: $\mathcal{Z}_{\mathbb{K}}(B) = \mathcal{Z}_{\mathbb{K}}(\langle B \rangle)$ where $\langle B \rangle$ is the ideal generated by B in $\mathbb{K}[\underline{x}]$.

Proof. (i) Assume $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(C)$, then $f(\underline{a}) = 0$ for all $f \in C$ by definition. In particular, $g(\underline{a}) = 0$ for all $g \in B$, since $B \subseteqq C$. Therefore, $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(B)$, proving the inclusion.

(ii) Since $B \subseteqq \langle B \rangle$, by the inclusion-reversing property we have $\mathcal{Z}_{\mathbb{K}}(\langle B \rangle) \subseteqq \mathcal{Z}_{\mathbb{K}}(B)$. For the opposite inclusion, assume $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(B)$. Consider an element $h \in \langle B \rangle$. Since $\langle B \rangle$ is generated by elements of B,

$$h = \sum_{i=1}^{m} r_i b_i$$

for some $m \in \mathbb{N}$ where $b_i \in B$ and $r_i \in \mathbb{K}[\underline{x}]$ for all $i, 1 \leq i \leq m$. Therefore,

$$h(\underline{a}) = \sum_{i=1}^{m} r_i(\underline{a}) \cdot b_i(\underline{a}) = \sum_{i=1}^{m} r_i(\underline{a}) \cdot 0 = 0.$$

Since h is an arbitrary element of $\langle B \rangle$, we may conclude that every element of $\langle B \rangle$ *vanishes* at $\underline{a}$, i.e., $h(\underline{a}) = 0$ for all $h \in \langle B \rangle$. Thus by definition $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(\langle B \rangle)$, concluding equality. □

Example 1.3.4. Consider $\mathbb{R}[x, y]$ and $\mathbb{A}^2_{\mathbb{R}}$.

(i) We have $\mathcal{Z}_{\mathbb{R}}(x, y) = \{(0, 0)\}$ is the origin of the real plane.

(ii) Similarly, $\mathcal{Z}_{\mathbb{R}}(y - x^2) = \{(t, t^2) \mid t \in \mathbb{R}\}$ which traces out a parabola in the real plane.

(iii) $\mathcal{Z}_{\mathbb{R}}(1 - x^2, y - 1)$ is a set of two points $\{(-1, 1), (1, 1)\}$ in the real plane.

(iv) Let us now consider $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2 + 1)$. In this case there are no points in the real plane that satisfy $x^2 + y^2 + 1 = 0$ since $x^2 + y^2 \geq 0$ for all $x, y, \in \mathbb{R}$. Hence, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2 + 1) = \varnothing$.

(v) $\mathcal{Z}_{\mathbb{R}}(0) = \mathbb{R}^2$ is the entire real plane.

For a moment we express a different perspective of elements from the polynomial ring $\mathbb{K}[\underline{x}]$. Consider a polynomial $f \in \mathbb{K}[\underline{x}]$. By evaluating f at points of $\mathbb{A}^n_{\mathbb{K}}$, f naturally induces a map between affine spaces.

$$\varphi_f \colon \mathbb{A}^n_{\mathbb{K}} \longrightarrow \mathbb{A}_{\mathbb{K}}$$

$$\underline{a} \longmapsto f(\underline{a}).$$

The elements of $\mathbb{A}^n_{\mathbb{K}}$ that map to zero under φ_f are precisely the points that make up the affine algebraic set defined by f, $\mathcal{Z}_{\mathbb{K}}(f)$. Consider for a moment the set of all functions from $\mathbb{A}^n_{\mathbb{K}}$ to $\mathbb{A}_{\mathbb{K}}$, denoted by $\mathcal{F}(\mathbb{A}^n_{\mathbb{K}}, \mathbb{A}_{\mathbb{K}})$. We have just shown that a polynomial $f \in \mathbb{K}[\underline{x}]$ determines a function $\varphi_f \in \mathcal{F}(\mathbb{A}^n_{\mathbb{K}}, \mathbb{A}_{\mathbb{K}})$. We call φ_f a *polynomial function*, i.e., a function from $\mathbb{A}^n_{\mathbb{K}}$ to $\mathbb{A}_{\mathbb{K}}$ that may be represented or evaluated as a polynomial from $\mathbb{K}[\underline{x}]$. More on this idea in the next section. We now give an example of a non-algebraic set.

Example 1.3.5. (i) Consider the function $h\colon \mathbb{A}^2_{\mathbb{R}} \longrightarrow \mathbb{A}_{\mathbb{K}}$, where $h(x,y) = y - \sin(\pi x)$. The *zero set* of h is the inverse image of $\{0\}$,

$$h^{-1}(0) := \left\{(x,y) \in \mathbb{A}^2_{\mathbb{R}} \mid y - \sin(\pi x) = 0\right\}.$$

We show that $h^{-1}(0)$ is not an algebraic set.

Proof. Assume there is a subset $B \subseteqq \mathbb{R}[x,y]$ such that $\mathcal{Z}(B) = h^{-1}(0)$. There must exist a non-zero polynomial $p(x,y) \in B$, since $h^{-1}(0)$ is not the entire real plane. Consider the line $y = a$ where $a \in \mathbb{R}$. There exists an a with $-1 \leq a \leq 1$ such that $p(x,a)$ is still non-zero, otherwise this contradicts the fact that $p(x,y) \neq 0$. We now have that

$$\mathcal{Z}_{\mathbb{R}}(B) = \bigcap_{f \in B} \mathcal{Z}_{\mathbb{R}}(f) \subseteqq \mathcal{Z}_{\mathbb{R}}(p(x,y)).$$

Intersect now with the line $y = a$ to get

$$\mathcal{Z}_{\mathbb{R}}(B) \cap \mathcal{Z}_{\mathbb{R}}(y-a) \subseteqq \mathcal{Z}_{\mathbb{R}}(p(x,y)) \cap \mathcal{Z}_{\mathbb{R}}(y-a) = \mathcal{Z}_{\mathbb{R}}(p(x,a)).$$

Since our a is between -1 and 1, we know the intersection on the left must be infinite. However, $p(x,a)$ has only a finite number of zeros since it is a polynomial in one variable over a domain. Thus, $\mathcal{Z}(p(x,a))$ must be finite, showing there is an infinite set contained in a finite set. This is an obvious contradiction, proving $h^{-1}(0)$ is not an algebraic set. $\square$

(ii) We may identify the intersection of $h^{-1}(0)$ with $y = 0$ as $\mathbb{Z}$. Thus, Example 1.3.5.(i) necessarily shows $\mathbb{Z} \subseteqq \mathbb{A}_{\mathbb{R}}$ is also not an algebraic set.

We now describe basic properties of the correspondence $\mathcal{Z}_{\mathbb{K}}$ induces between the polynomial ring $\mathbb{K}[\underline{x}]$ and the affine space $\mathbb{A}^n_{\mathbb{K}}$.

$$\mathcal{Z}_{\mathbb{K}}\colon \mathcal{P}(\mathbb{K}[\underline{x}]) \longrightarrow \mathcal{P}(\mathbb{A}^n_{\mathbb{K}})$$

$$\{\text{subsets of } \mathbb{K}[\underline{x}]\} \longmapsto \{\text{affine algebraic sets of } \mathbb{A}^n_{\mathbb{K}}\}$$

We have already shown from Proposition 1.3.3(i) that $\mathcal{Z}_{\mathbb{K}}$ is inclusion-reversing. Notice, however, this property does not hold for strict inclusions. For instance, consider $\mathbb{K}[x,y]$ and let $I = \langle x, y\rangle$ and $J = \langle x^2, y\rangle$. We have $J \subsetneqq I$ but

$$\mathcal{Z}_{\mathbb{K}}(J) = \mathcal{Z}_{\mathbb{K}}(I) = \{(0,0)\}.$$

Thus, $\mathcal{Z}_{\mathbb{K}}$ is not in general an injective map. However, if we restrict ourselves to the algebraic subsets of $\mathcal{P}(\mathbb{A}^n_{\mathbb{K}})$, then Proposition 1.3.3(ii) does show that $\mathcal{Z}_{\mathbb{K}}$ is surjective, i.e., we need only consider ideals of the polynomial ring $\mathbb{K}[\underline{x}]$ rather than arbitrary subsets. Hence, we reveal ideal theoretic properties of $\mathcal{Z}_{\mathbb{K}}$.

Proposition 1.3.6. Let I, J be ideals of $\mathbb{K}[\underline{x}]$. Then

(i) $\mathcal{Z}_{\mathbb{K}}(I) \cup \mathcal{Z}_{\mathbb{K}}(J) = \mathcal{Z}_{\mathbb{K}}(IJ)$. More generally, any finite union of affine algebraic sets is still an affine algebraic set.

(ii) $\mathcal{Z}_{\mathbb{K}}(I) \cap \mathcal{Z}_{\mathbb{K}}(J) = \mathcal{Z}_{\mathbb{K}}(I + J)$. More generally, any intersection of affine algebraic sets is still an affine algebraic set.

(iii) $\mathcal{Z}_{\mathbb{K}}(0) = \mathbb{A}^n_{\mathbb{K}}$. The whole affine space is an affine algebraic set.

(iv) $\mathcal{Z}_{\mathbb{K}}(1) = \varnothing$. The empty set is an affine algebraic set.

Proof. (i) Since $IJ \subseteqq I$ and $IJ \subseteqq J$, we may apply the inclusion revering property to get $\mathcal{Z}_{\mathbb{K}}(I) \subseteqq \mathcal{Z}_{\mathbb{K}}(IJ)$ and $\mathcal{Z}_{\mathbb{K}}(J) \subseteqq \mathcal{Z}_{\mathbb{K}}(IJ)$. Therefore, $\mathcal{Z}_{\mathbb{K}}(I) \cup \mathcal{Z}_{\mathbb{K}}(J) \subseteqq \mathcal{Z}_{\mathbb{K}}(IJ)$. For the reverse inclusion, let $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(IJ)$ and $\underline{a} \notin \mathcal{Z}_{\mathbb{K}}(I)$. Then $\exists f \in I$ such that $f(\underline{a}) \neq 0$. However,

$$\forall g \in J, fg \in IJ \Rightarrow (fg)(\underline{a}) = f(\underline{a})g(\underline{a}) = 0 \Rightarrow g(\underline{a}) = 0.$$

Therefore, $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(J)$ and we may conclude $\mathcal{Z}_{\mathbb{K}}(IJ) \subseteqq \mathcal{Z}_{\mathbb{K}}(I) \cup \mathcal{Z}_{\mathbb{K}}(J)$. One proceeds inductively to acquire the general statement.

(ii) We prove the most general form:

$$\mathcal{Z}_{\mathbb{K}}(\sum_{i\in\Lambda} J_i) = \bigcap_{i\in\Lambda} \mathcal{Z}_{\mathbb{K}}(J_i).$$

Let $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(\sum_{i\in\Lambda} J_i)$. Then $f(\underline{a}) = 0$ for all $f \in \sum_{i\in\Lambda} J_i$. Specifically, $f(\underline{a}) = 0$ for all $f \in J_i$. Hence, $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(J_i) \Rightarrow \underline{a} \in \bigcap_{i\in\Lambda} \mathcal{Z}_{\mathbb{K}}(J_i)$. For the opposite inclusion, let $\underline{a} \in \bigcap_{i\in\Lambda} \mathcal{Z}_{\mathbb{K}}(J_i)$, so $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(J_i)$ for all $i \in \Lambda$. Then $f(\underline{a}) = 0$ for all $f \in J_i$. An element $g \in \sum_{i\in\Lambda} J_i$ has the form $g = \sum_{j=1}^{m} g_j$ for some $m \in \mathbb{N}$ and $g_j \in J_{i_j}$. Therefore $g(\underline{a}) = \sum_{j=1}^{m} g_j(\underline{a}) = 0$ since $g_j(\underline{a}) = 0$ for all $j, 1 \leq j \leq m$. Thus $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(\sum_{i\in\Lambda} J_i)$, concluding the proof.

(iii) The zero polynomial vanishes all points of $\mathbb{A}^n_{\mathbb{K}}$, i.e., $0(\underline{a}) = 0$ for all $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$. Hence,

$$\mathbb{A}^n_{\mathbb{K}} \subseteqq \mathcal{Z}_{\mathbb{K}}(0) \subseteqq \mathbb{A}^n_{\mathbb{K}}.$$

(iiii) A non-zero constant polynomial vanishes nowhere. □

Example 1.3.7 ([10], Example 1.6). We show that Proposition 1.3.6(i) may be a strict inclusion when considering infinite unions of affine algebraic sets. For instance, consider the ideals $\langle x - q\rangle$ where $q \in \mathbb{Q}$ of the polynomial ring $\mathbb{R}[x]$. Clearly there is no non-zero polynomial in $\mathbb{R}[x]$ that is divisible by $\langle x - q\rangle$ for all $q \in \mathbb{Q}$. Thus, we must have $\bigcap_{q\in\mathbb{Q}} \langle x - q\rangle = \langle 0\rangle$. Therefore,

$$\mathbb{Q} = \bigcup_{q\in\mathbb{Q}} \mathcal{Z}_{\mathbb{R}}(x - q) \subsetneqq \mathcal{Z}_{\mathbb{R}}(\bigcap_{q\in\mathbb{Q}} \langle x - q\rangle) = \mathcal{Z}_{\mathbb{R}}(0) = \mathbb{A}_{\mathbb{R}}.$$

1.4 Vanishing Ideals

We have already seen that ideals that define algebraic sets are not unique. For instance, considering $\mathbb{A}^2_{\mathbb{R}}$ and $\mathbb{R}[x, y]$,

$$\mathcal{Z}_{\mathbb{R}}(x, y) = \mathcal{Z}_{\mathbb{R}}(x^2 + y^2) = \{(0, 0)\}.$$

In fact, any affine algebraic set $\mathcal{Z}_{\mathbb{R}}(f_1, f_2, \ldots, f_r)$ of $\mathbb{A}^n_{\mathbb{R}}$ may be defined by a single polynomial, $\mathcal{Z}_{\mathbb{R}}(f_1^2 + f_2^2 + \ldots + f_r^2)$, which prompts the following definition.

Definition 1.4.1. Let V be an affine algebraic set of $\mathbb{A}^n_{\mathbb{K}}$. The vanishing ideal of V is the set

$$\mathcal{I}_{\mathbb{K}}(V) := \{f \in \mathbb{K}[\underline{x}] \mid f(\underline{a}) = 0 \text{ for all } \underline{a} \in V\}$$

Proposition 1.4.2. $\mathcal{I}_{\mathbb{K}}(V)$ is in fact an ideal of $\mathbb{K}[\underline{x}]$.

Proof. $0 \in \mathcal{I}_{\mathbb{K}}(V)$ because the zero polynomial vanishes at all points in $\mathbb{A}^n_{\mathbb{K}}$, particularly V. Let $f, g \in \mathcal{I}_{\mathbb{K}}(V)$ and $\underline{a} \in V$, then $f(\underline{a}) + g(\underline{a}) = 0 + 0 = 0$. Hence, $f + g$ also vanishes at all point of V, i.e., $f + g \in \mathcal{I}_{\mathbb{K}}(V)$. Similarly, let $h \in \mathbb{K}[\underline{x}]$ with $f \in \mathcal{I}_{\mathbb{K}}(V)$ and $\underline{a} \in V$, then $f(\underline{a}) \cdot h(\underline{a}) = 0 \cdot h(\underline{a}) = 0$. Thus, $h \cdot f$ vanishes at all points of V, i.e, $f \cdot h \in \mathcal{I}_{\mathbb{K}}(V)$ for all $h \in \mathbb{K}[\underline{x}]$. Therefore, $\mathcal{I}_{\mathbb{K}}(V)$ is an ideal of $\mathbb{K}[\underline{x}]$. □

In the previous section we showed that a polynomial from $\mathbb{K}[\underline{x}]$ determines a polynomial function of $\mathcal{F}(\mathbb{A}^n_{\mathbb{K}}, \mathbb{A}_{\mathbb{K}})$. If we now vary f over $\mathbb{K}[\underline{x}]$ we obtain a map between function spaces, namely,

$$\varsigma\colon \mathbb{K}[\underline{x}] \longrightarrow \mathcal{F}(\mathbb{A}^n_{\mathbb{K}}, \mathbb{A}_{\mathbb{K}})$$

$$\{\text{polynomial}\} \longmapsto \{\text{polynomial function}\}$$

Let us now restrict $\mathbb{A}^n_{\mathbb{K}}$ by an affine algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$, which then induces the restriction

$$\varsigma \restriction_V \colon \mathbb{K}[\underline{x}] \longrightarrow \mathcal{F}(V, \mathbb{A}_{\mathbb{K}})$$

where $\mathcal{F}(V, \mathbb{A}_{\mathbb{K}})$ is the set of all functions from V to $\mathbb{A}_{\mathbb{K}}$. Under point-wise operations of functions $\mathcal{F}(V, \mathbb{A}_{\mathbb{K}})$ becomes a $\mathbb{K}$-algebra and $\varsigma \restriction_V$ becomes a $\mathbb{K}$-algebra homomorphism. An element of $\mathbb{K}[\underline{x}]$ mapping to the zero function on V must belong to the vanishing ideal of V by definition. Hence, the kernel of $\varsigma \restriction_V$ is precisely the vanishing ideal of V, which is yet another reason why $\mathcal{I}_{\mathbb{K}}(V)$ is an ideal. Notice also the image of $\overline{\varsigma}$ is the set of all polynomial functions from V to $\mathbb{A}_{\mathbb{K}}$. By the first isomorphism theorem, this image is equivalent to $\frac{\mathbb{K}[\underline{x}]}{\mathcal{I}_{\mathbb{K}}(V)}$, known as the *coordinate ring of functions* of V.

Definition 1.4.3. Let V be an algebraic set of $\mathbb{A}^n_{\mathbb{K}}$. The *coordinate ring of functions* of V is

$$\mathbb{K}[V] := \frac{\mathbb{K}[\underline{x}]}{\mathcal{I}_{\mathbb{K}}(V)}.$$

The previous paragraph shows that the coordinate ring of V may be identified with the ring of maps $\alpha\colon V \longrightarrow \mathbb{A}_{\mathbb{K}}$ such that α may be represented by a polynomial from $\mathbb{K}[\underline{x}]$. We expand on

this idea in Chapter 2. We now focus on properties of the reverse correspondence,

$$\mathcal{I}_{\mathbb{K}} : \mathcal{P}(\mathbb{A}^n_{\mathbb{K}}) \longrightarrow \mathcal{P}(\mathbb{K}[\underline{x}])$$

$$\{\text{subsets of } \mathbb{A}^n_{\mathbb{K}}\} \longmapsto \{\text{ideals of } \mathbb{K}[\underline{x}]\}.$$

Proposition 1.4.4. Let $\mathcal{I}_{\mathbb{K}}$ be defined as above, and let U, W be subsets of $\mathbb{A}^n_{\mathbb{K}}$.

(i) $\mathcal{I}_{\mathbb{K}}$ is inclusion-reversing: if $U \subseteqq W$, then $\mathcal{I}_{\mathbb{K}}(W) \subseteqq \mathcal{I}(U)$.

(ii) $\mathcal{I}_{\mathbb{K}}(\varnothing) = \mathbb{K}[\underline{x}]$.

(iii) $\mathcal{I}_{\mathbb{K}}(\mathbb{A}^n_{\mathbb{K}}) = \langle 0 \rangle$, if $\mathbb{K}$ is an infinite field.

(iv) $\mathcal{I}_{\mathbb{K}}(W) \cap \mathcal{I}_{\mathbb{K}}(U) = \mathcal{I}_{\mathbb{K}}(W \cup U) =$ for any $U, W \subseteqq \mathbb{A}^n_{\mathbb{K}}$. More generally, an intersection of vanishing ideals is still a vanishing ideal.

(v) $\mathcal{I}_{\mathbb{K}}(W) + \mathcal{I}_{\mathbb{K}}(U) \subseteqq \mathcal{I}_{\mathbb{K}}(W \cap U)$ for any $U, W \subseteqq \mathbb{A}^n_{\mathbb{K}}$. More generally, a sum of vanishing ideals is contained in a vanishing ideal.

Proof. (i) Assume $U \subseteqq W$ and let $f \in \mathcal{I}_{\mathbb{K}}(W)$. By definition, $f(\underline{a}) = 0$ for all $\underline{a} \in W$. Particularly, $f(\underline{a}) = 0$ for all $\underline{a} \in U$ since $U \subseteqq W$. Thus, $f \in \mathcal{I}_{\mathbb{K}}(U)$.

(ii) This is vacuously true, i.e., every polynomial vanishes at nothing.

(iii) The zero polynomial vanishes the whole affine space $\mathbb{A}^n_{\mathbb{K}}$, providing the reverse containment.We now prove the zero polynomial is the only polynomial from $\mathbb{K}[\underline{x}]$ with this property (assuming $\mathbb{K}$ is infinite), which provides the forward containment.

Proposition 1.4.5. Let $\mathbb{K}$ be infinite and $f \in \mathbb{K}[\underline{x}]$. If $f\colon \mathbb{A}^n_{\mathbb{K}} \longrightarrow \mathbb{A}_{\mathbb{K}}$ is the zero function, then $f = 0$.

Proof. We prove the statement by induction on the number of variables n. For the base case, let n=1. This is just the contrapositive of the fact that a non-zero polynomial $f(x) \in \mathbb{K}[x]$ of degree m has at most m distinct roots in $\mathbb{K}$, a finite number of zeros. Therefore, $f(x)$ must be the zero polynomial.

We now assume this holds true for $n-1$ variables and prove for n variables. We have that f is the zero function from $\mathbb{A}^n_{\mathbb{K}}$ to $\mathbb{A}_{\mathbb{K}}$ and $f \in \mathbb{K}[x_1, x_2, \ldots, x_n] = \mathbb{K}[x_1, x_2, \ldots, x_{n-1}][x_n]$. We may

write

$$f = \sum_{i=0}^{m} f_i(x_1, x_2, \ldots, x_{n-1}) x_n^i.$$

Let us fix the first $n-1$ variables with $(a_1, a_2, \ldots, a_{n-1}) \in \mathbb{A}_{\mathbb{K}}^{n-1}$. Then $f(a_1, a_2, \ldots, a_{n-1}, x_n)$ is the zero function for an infinite number of values of $x_n \in \mathbb{K}$. Hence, we are reduced to the base case and may conclude $f_i(a_1, a_2, \ldots, a_{n-1}) = 0$. However since the $(a_1, a_2, \ldots, a_{n-1}) \in \mathbb{A}_{\mathbb{K}}^{n-1}$ was arbitrary, we have that $f_i(x_1, x_2, \ldots, x_{n-1})$ are the zero functions on $\mathbb{A}_{\mathbb{K}}^{n-1}$ for all $i, 1 \leq i \leq m$. The induction hypothesis then implies $f_i(x_1, x_2, \ldots, x_{n-1}) = 0$ for $i, 1 \leq i \leq m$. Thus,

$$f = \sum_{i=0}^{m} f_i(x_1, x_2, \ldots, x_{n-1}) x_n^i = \sum_{i=0}^{m} 0 x_n^i = 0.$$

□

(iv) We prove by equivalences, $f \in \mathcal{I}_{\mathbb{K}}(W) \cap \mathcal{I}_{\mathbb{K}}(U) \Leftrightarrow f \in \mathcal{I}_{\mathbb{K}}(W)$ and $f \in \mathcal{I}_{\mathbb{K}}(U)$

$$\Leftrightarrow f(\underline{a}) = 0 \text{ for all } \underline{a} \in W \text{ and } f(\underline{b}) = 0 \text{ for all } \underline{b} \in U$$

$$\Leftrightarrow f(\underline{c}) = 0 \text{ for all } \underline{c} \in W \cup U \Leftrightarrow f \in \mathcal{I}_{\mathbb{K}}(W \cup U).$$

(v) Let $f \in \mathcal{I}_{\mathbb{K}}(W) + \mathcal{I}_{\mathbb{K}}(U)$. By definition,

$$f = h + g \text{ for some } h \in \mathcal{I}_{\mathbb{K}}(w) \text{ and } g \in \mathcal{I}_{\mathbb{K}}(U).$$

Consider now an element $\underline{a} \in W \cap U$ then

$$f(\underline{a}) = h(\underline{a}) + g(\underline{a}) = 0 + 0 = 0.$$

Hence, $f \in \mathcal{I}_{\mathbb{K}}(W \cap U)$ and the result follows. □

In Proposition 1.4.4(iii), it was important for us to have $\mathbb{K}$ be an infinite field. In Section 1.7, we introduce the Hilbert Nullstellensatz, where we will give an analogous result for a finite field $\mathbb{K}$.

Remark 1.4.6. (i) Proposition 1.4.4(iii) implies that the polynomial ring $\mathbb{K}[\underline{x}]$ injects into the ring of functions $\mathcal{F}(\mathbb{A}^n_{\mathbb{K}}, \mathbb{A}_{\mathbb{K}})$, when $\mathbb{K}$ is an infinite field.

(ii) $\mathcal{I}_{\mathbb{K}}$ is neither a injective or surjective. Consider $\mathbb{A}_{\mathbb{R}}$ and $\mathbb{R}[x]$, we will soon show that $\mathcal{I}_{\mathbb{K}}(\mathbb{Z}) = \mathcal{I}_{\mathbb{K}}(\mathbb{A}_{\mathbb{R}}) = \langle 0 \rangle$. Additionally, we shall show $\langle x^n \rangle$ will never be in the image of $\mathcal{I}_{\mathbb{K}}$ for any $n > 1$.

When we restrict our attention to affine algebraic sets and vanishing ideals, the following Proposition shows they are in one to one correspondence.

Proposition 1.4.7.

(i) For any ideal $J \subseteqq \mathbb{K}[\underline{x}]$ and any subset $W \subseteqq \mathbb{A}^n_{\mathbb{K}}$, $J \subseteqq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))$ and $W \subseteqq \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(W))$.

(ii) The maps $\mathcal{Z}_{\mathbb{K}}$ and $\mathcal{I}_{\mathbb{K}}$ are inverses to each other when restricting to affine algebraic sets and vanishing ideals: $J = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))$ and $U = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(U))$ when $J = \mathcal{I}_{\mathbb{K}}(V)$ for some $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ and $U = \mathcal{Z}_{\mathbb{K}}(I)$ for some $I \subseteqq \mathbb{K}[\underline{x}]$.

Proof. (i) Let $f \in J$, then $f(\underline{a}) = 0$ for all $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(J)$. Hence, $f \in \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))$ by definition. Now let $\underline{a} \in W$, then $f(\underline{a}) = 0$ for all $f \in \mathcal{I}_{\mathbb{K}}(W)$. Therefore, $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(W))$.

(ii) We simply apply $\mathcal{I}_{\mathbb{K}}$ and $\mathcal{Z}_{\mathbb{K}}$. From proposition 1.4.7(i), we have that

$$V \subseteqq \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V)) \Rightarrow \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V))) \subseteqq \mathcal{I}_K(V).$$

However, proposition 1.4.7(i) also implies

$$\mathcal{I}_K(V) \subseteqq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V))).$$

Thus, $\mathcal{I}_{\mathbb{K}}(V) = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V)))$ where $\mathcal{I}_{\mathbb{K}}(V) = J$.

Similarly, $J \subseteqq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I)) \Rightarrow \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I)) \subseteqq \mathcal{Z}_{\mathbb{K}}(I)$, and proposition 1.4.7($i$) implies $\mathcal{Z}_{\mathbb{K}}(I) \subseteqq \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I)) \subseteqq \mathcal{Z}_{\mathbb{K}}(I)$, where $\mathcal{Z}_{\mathbb{K}}(I) = U$. $\square$

Remark 1.4.8.

(i) From Proposition 1.4.7(ii),we have that $\mathcal{I}_{\mathbb{K}}$ becomes injective when restricting to affine algebraic sets,

$$\mathcal{I}_{\mathbb{K}}(V) = \mathcal{I}_{\mathbb{K}}(U) \Rightarrow \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V)) = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(U)) \Rightarrow V = U.$$

(ii) We have that the inclusion-reversing property holds over strict inclusions of affine algebraic sets

$$V \subsetneqq U \Rightarrow \mathcal{I}_{\mathbb{K}}(U) \subsetneqq \mathcal{I}_{\mathbb{K}}(V), \text{ where } V = \mathcal{Z}_{\mathbb{K}}(I) \text{ and } U = \mathcal{Z}_{\mathbb{K}}(J).$$

Proof. Let $V = \mathcal{Z}_{\mathbb{K}}(I) \subsetneqq U = \mathcal{Z}_{\mathbb{K}}(J)$ and assume the vanishing ideals are equal,

$$\mathcal{I}_{\mathbb{K}}(U) = \mathcal{I}_{\mathbb{K}}(V).$$

After applying $\mathcal{Z}_{\mathbb{K}}$, one gets

$$\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(U)) = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V)).$$

Then by Proposition 1.4.7(ii), $V = U$, contradicting our assumption. □

We finish the section with a few results pertaining to radical ideals.

Proposition 1.4.9. Let $I \subseteqq \mathbb{K}[\underline{x}]$ be an ideal and $W \subseteqq \mathbb{A}^n_{\mathbb{K}}$ be an arbitrary subset.

(i) $\mathcal{Z}_{\mathbb{K}}(I) = \mathcal{Z}_{\mathbb{K}}(\sqrt{I})$.

(ii) $\mathcal{I}_{\mathbb{K}}(W)$ is radical.

(iii) $I \subseteqq \sqrt{I} \subseteqq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))$

Proof. (i) By 1.1.9(i), we have $\mathcal{Z}_{\mathbb{K}}(\sqrt{I}) \subseteqq \mathcal{Z}_{\mathbb{K}}(I)$, since $I \subseteqq \sqrt{I}$. For the opposite inclusion, let $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(I)$. Consider $f \in \sqrt{I}$. Then by definition of radical ideal, $f^m \in I$ for some $m \in \mathbb{N}$. Hence, $f^m(\underline{a}) = 0$, but this implies $f(\underline{a}) = 0$ since $\mathbb{K}[\underline{x}]$ is an integral domain. Therefore, $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(\sqrt{I})$.

(ii) We start with the reverse inclusion. Assume $f \in \sqrt{\mathcal{I}_{\mathbb{K}}(W)}$, then $f^s \in \mathcal{I}_{\mathbb{K}}(W)$ for some $s \in \mathbb{N}$, i.e., $f^s(\underline{a}) = 0$ for all $\underline{a} \in W$. Once again, $f^s(\underline{a}) = 0$ implies $f(\underline{a}) = 0$. Therefore. $f(\underline{a}) = 0$ for all $\underline{a} \in W$, i.e., $f \in \mathcal{I}_{\mathbb{K}}(W)$. The forward inclusion, $\mathcal{I}_{\mathbb{K}}(W) \subseteqq \sqrt{\mathcal{I}_{\mathbb{K}}(W)}$, is immediate.

(iii) From Proposition 1.4.7(i), we have $I \subseteqq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))$. After taking radicals of both sides and considering Proposition 1.4.9(ii), we have $\sqrt{I} \subseteqq \sqrt{\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))} = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))$. $\square$

We had mentioned before that $\langle x^n \rangle$ will never be in the image of $\mathcal{I}_{\mathbb{K}}$ for any $n > 1$. This is now easy to see because $\langle x^n \rangle$ is never radical for $n > 1$, and proposition 1.4.9(ii) shows all vanishing ideals are radical.

1.5 Zariski Topology

Let us first recall some basic notions from topology. A *topology* defined on any set X is a subset $\mathcal{T} \subseteqq \mathcal{P}(X)$ satisfying the following conditions:

- $\varnothing, X \in \mathcal{T}$.
- $\mathcal{T}$ is closed under arbitrary unions.
- $\mathcal{T}$ is closed under finite intersections.

Elements of $\mathcal{T}$ are called *open sets*. Their compliments in X are called *closed sets*. We call the set X with a topology $\mathcal{T}$ a *topological space*, denoted $(X, \mathcal{T})$. Notice that since closed sets define open sets and vice versa, we therefore have synonymous defining conditions for a topology in terms of closed sets:

- $\varnothing, X$ are closed.
- finite unions of closed sets are closed.
- arbitrary intersections of closed sets are closed.

For any topological space $(X, \mathcal{T})$ and any subset $Y \subseteqq X$, Y inherits an induced topology from X by defining $U \cap Y$ to be open whenever U is open in X. Similarly, $V \cap Y$ is closed whenever V is closed in X.

We may now define a topology for $\mathbb{A}^n_{\mathbb{K}}$ through the map $\mathcal{Z}_{\mathbb{K}}$. Proposition 1.3.6 give the defining conditions for a topology in terms of closed sets as mentioned above. This will be known as the Zariski Topology.

Definition 1.5.1. The *Zariski topology* on $\mathbb{A}^n_{\mathbb{K}}$ is the topology defined by letting the closed sets be the algebraic sets of $\mathbb{A}^n_{\mathbb{K}}$. The collection of all the closed sets in this topology is denoted by $\mathfrak{Z}_{\mathbb{K}}$. We have an induced topology for any subset $W \subseteqq \mathbb{A}^n_{\mathbb{K}}$, i.e., $W \cap V$ is closed whenever V is closed in $\mathbb{A}^n_{\mathbb{K}}$. This will be known as the Zariski topology on W. The collection of all the closed sets in the induced topology is denoted by $\mathfrak{Z}_{\mathbb{K}} \restriction_W$.

Example 1.5.2. We examine the Zariski topology $\mathfrak{Z}_{\mathbb{K}}$ of the affine line $\mathbb{A}_{\mathbb{K}}$, with $\mathbb{K}$ infinite. Hence, we consider the ideals of the polynomial ring $\mathbb{K}[x]$ since they define the closed sets of $\mathbb{A}_{\mathbb{K}}$. Notice the polynomial ring is equal to the coordinate ring of functions over $\mathbb{A}_{\mathbb{K}}$,

$$\mathbb{K}[\mathbb{A}_{\mathbb{K}}] = \frac{\mathbb{K}[x]}{\mathcal{I}_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})} = \frac{\mathbb{K}[x]}{\langle 0 \rangle} = \mathbb{K}[x].$$

Since $\mathbb{K}[x]$ is a principal ideal domain, any ideal is generated by one element $f(x) \in \mathbb{K}[x]$. If $f(x) = 0$ then $\mathcal{Z}_{\mathbb{K}}(f(x)) = \mathbb{A}_{\mathbb{K}}$. We now assume $f(x)$ is non-zero. Since $f(x)$ may have only a finitely many zeros in $\mathbb{K}$, we have that any proper closed set of $\mathbb{A}_{\mathbb{K}}$ is a finite collection of points. However, $f(x)$ may have no zeros in $\mathbb{K}$, which implies $\mathcal{Z}_{\mathbb{K}}(f(x)) = \varnothing$. Thus, the only proper closed sets are finite.

Definition 1.5.3. Let $(X, \mathcal{T})$ be a topological space and let us consider an arbitrary subset $S \subseteqq X$.

(i) The *closure* of S, denoted $\overline{S}$ is the intersection of all the closed sets containing S. Notice X contains S, so the intersection is not empty. Since arbitrary intersections of closed sets are closed in any topological space, we necessarily have that $\overline{S}$ is the smallest closed set containing S.

(ii) The subset S is called *dense* in X if its closure is X, i.e., $\overline{S} = X$.

Proposition 1.5.4. [[7], Proposition 3.1] Let X be a non-empty topological space. The following are equivalent:

(i) If we can write X in the form $X = F \cup G$, where F and G are closed sets in X, then $X = F$ or $X = G$.

(ii) If U and V are two open sets of X and $U \cap V = \varnothing$, then $U = \varnothing$ or $V = \varnothing$.

(iii) Any non-empty open set of X is dense in X.

Under these conditions we say that X is irreducible.

Proof. (i)⇒(ii): Let U, V be open sets of X such that $U \cap V = \varnothing$. Then $X \setminus U$ and $X \setminus V$ are closed sets of X such that $(X \setminus U) \cup (X \setminus V) = X$. Then by (i), we have that $X \setminus U = X$ or $X \setminus V = X$. This implies $U = \varnothing$ or $V = \varnothing$.

(ii)⇒(iii) Let W be a non-empty open set of X. Consider the closure of W in X, $\overline{W}$. We may then form an intersection of two open sets which is empty, $(X \setminus \overline{W}) \cap W = \varnothing$. Since W is non-empty, (ii) implies $(X \setminus \overline{W}) = \varnothing$, which then implies $\overline{W} = X$.

(iii)⇒(i) Let $X = F \cup G$, where F and G are closed sets in X and $X \neq F$. Then $X \setminus F$ must be a non-empty open set of X. Since $X = F \cup G$, we have that $X \setminus F = G \setminus F \subseteqq G$. Therefore the closure of $X \setminus F$ is containted in G. By (iii) we must have the closure of $X \setminus F$ to be X. Thus, we have X is contained in G. This implies X must be equal to G. □

We will now interpret these notions in terms of the Zariski topology.

Proposition 1.5.5. Consider the Zariski topology on $\mathbb{A}^n_{\mathbb{K}}$. Let $S \subseteqq \mathbb{A}^n_{\mathbb{K}}$ be an arbitrary subset.

$$\overline{S} = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(S)).$$

Proof. $S \subseteqq \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(S)$ by proposition 1.4.9, which is closed in $\mathbb{A}^n_{\mathbb{K}}$. Therefore by definition of $\overline{S}$, $\overline{S} \subseteqq \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(S)$. For the second inclusion, notice we alway have that $S \subseteqq \overline{S}$. After applying $\mathcal{I}_{\mathbb{K}}$ then $\mathcal{Z}_{\mathbb{K}}$, we get $\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(S) \subseteqq \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(\overline{S}) = \overline{S}$ by Proposition 1.4.7(ii). □

Example 1.5.6. (i) If $\mathbb{K}$ is an infinite field, we have that $\mathbb{A}^n_{\mathbb{K}}$ is irreducible. This follows from Proposition 1.5.7(iii) since $\mathcal{I}_{\mathbb{K}}(\mathbb{A}^n_{\mathbb{K}}) = 0$ is prime of $\mathbb{K}[\underline{x}]$.

(ii) Let $\mathbb{K}$ be an infinite field containing $\mathbb{Z}$. The closure of $\mathbb{Z}$ in $\mathbb{A}_{\mathbb{K}}$ is $\mathbb{A}_{\mathbb{K}}$, i.e., $\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(\mathbb{Z})) = \mathbb{A}_{\mathbb{K}}$. This is due to the fact that the only non-empty closed sets of $\mathbb{A}_{\mathbb{K}}$ are finite sets or the whole space. Since $\mathbb{Z}$ contains an infinite number of points, the only closed set that contains $\mathbb{Z}$ is the whole space $\mathbb{A}_{\mathbb{K}}$. We now take $\mathcal{I}_{\mathbb{K}}$ of both sides to get the expression $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(\mathbb{Z}))) = \mathcal{I}_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$. Then by Proposition 1.4.7(ii), the left side becomes $(\mathcal{I}_{\mathbb{K}}(\mathbb{Z}) = \mathcal{I}_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}) = 0$, which we had mentioned earlier.

(iii) Consider $\mathbb{K}[\underline{x}]$ and $\mathbb{A}^n_{\mathbb{K}}$. Recall $\underline{a} = (a_1, a_2, \ldots, a_n)$ is a point in $\mathbb{A}^n_{\mathbb{K}}$. We have that for any $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$,

$$\mathfrak{m}_{\underline{a}} := \mathcal{I}(a_1, a_2, \ldots, a_n) = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle \text{ is a maximal ideal and } \mathcal{Z}(\mathfrak{m}_a) = a.$$

Thus there is a bijection between maximal ideals of the form $\mathfrak{m}_{\underline{a}}$ for some $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$ and points of $\mathbb{A}^n_{\mathbb{K}}$. This bijection follows from Theorem 1.7.3 from the next section.

(iv) Let us consider $\mathbb{R}[x]$ and $\mathbb{A}_{\mathbb{R}}$. Here we have maximal ideals that do not correspond to points in $\mathbb{A}_{\mathbb{R}}$ For instance, $\mathcal{Z}_{\mathbb{R}}(x^2 + 1) = \varnothing$, but $\langle x^2 + 1 \rangle$ is a maximal ideal since $\mathbb{R}[x]/\langle x^2 + 1 \rangle \simeq \mathbb{C}$. So when working over general fields there exist more maximal ideals in the polynomial ring than points in $\mathbb{A}^n_{\mathbb{K}}$.

Proposition 1.5.7. Let $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ be a non-empty affine algebraic set. Then

$$V \text{ is irreducible } \Leftrightarrow \mathcal{I}_{\mathbb{K}}(V) \text{ is a prime ideal.}$$

Proof. Assume V is irreducible and let $f \cdot g \in \mathcal{I}_{\mathbb{K}}(V)$. Notice,

$$V = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V)) \subseteqq \mathcal{Z}_{\mathbb{K}}(f) \cup \mathcal{Z}_{\mathbb{K}}(g).$$

Therefore,

$$V = (\mathcal{Z}_{\mathbb{K}}(f) \cap V) \cup (\mathcal{Z}_{\mathbb{K}}(g) \cap V)$$

Both sets are closed in the induced subspace topology. Since V is irreducible and without loss of generality, we have

$$V = (\mathcal{Z}_{\mathbb{K}}(f) \cap V) \Rightarrow V \subseteqq \mathcal{Z}_{\mathbb{K}}(f).$$

Hence, $f \in \mathcal{I}_{\mathbb{K}}(V)$, proving that $\mathcal{I}_{\mathbb{K}}(V)$ is a prime ideal by definition. For the opposite implication, assume $\mathcal{I}_{\mathbb{K}}(V)$ is prime. Suppose we may write $V = V_1 \cup V_2$ such that V_1 and V_2 are closed and are strictly contained in V. Then $\mathcal{I}_{\mathbb{K}}(V) \subsetneqq \mathcal{I}_K(V_1)$ and $\mathcal{I}_{\mathbb{K}}(V) \subsetneqq \mathcal{I}_{\mathbb{K}}(V_2)$. Because of the strict

inclusion, there must exist an $f_1 \in \mathcal{I}_{\mathbb{K}}(V_1) \setminus \mathcal{I}_{\mathbb{K}}(V)$ and $f_2 \in \mathcal{I}_{\mathbb{K}}(V_2) \setminus \mathcal{I}_{\mathbb{K}}(V)$. Consider,

$$f_1 \cdot f_2 \in \mathcal{I}_{\mathbb{K}}(V_1) \cdot \mathcal{I}_{\mathbb{K}}(V_2) \subseteqq \mathcal{I}_{\mathbb{K}}(V_1) \cap \mathcal{I}_{\mathbb{K}}(V_2) = \mathcal{I}_{\mathbb{K}}(V_1 \cup V_2) = \mathcal{I}_{\mathbb{K}}(V)).$$

Therefore, $f_1 \cdot f_2$ vanishes on V or $f_1 \cdot f_2 \in \mathcal{I}_{\mathbb{K}}(V)$. However, this contradicts the fact that $\mathcal{I}_{\mathbb{K}}(V)$ is a prime ideal, since $f_1, f_2 \notin \mathcal{I}_{\mathbb{K}}(V) \Rightarrow f_1 \cdot f_2 \notin \mathcal{I}_{\mathbb{K}}(V)$. □

Remark 1.5.8. (i) If we assume $\mathbb{K}$ is an infinite field, we have that the Zariski topology on $\mathbb{A}^n_{\mathbb{K}}$ is never Hausdorff. A Hausdorff space (also known as a T_2-space) is defined as a topological space with the property that for any two distinct points $\underline{a}, \underline{b} \in \mathbb{A}^n_{\mathbb{K}}$ there exist disjoint open sets $O_1, O_2 \subseteqq \mathbb{A}^n_{\mathbb{K}}$ such that $\underline{a} \in O_1$ and $\underline{b} \in O_2$. If this were so, then we would be able to write $\mathbb{A}^n_{\mathbb{K}}$ as a finite union of closed sets, but this contradicts Proposition 1.5.4 since $\mathbb{A}^n_{\mathbb{K}}$ is irreducible.

The Zariski Topology on $\mathbb{A}^n_{\mathbb{K}}$ is a T_1-space, i.e., a topological space with the property that for any two distinct points $\underline{a}, \underline{b} \in \mathbb{A}^n_{\mathbb{K}}$ there exist open sets $O_1, O_2 \subseteqq \mathbb{A}^n_{\mathbb{K}}$ such that $\underline{a} \in O_1 \setminus O_2$ and $\underline{b} \in O_2 \setminus O_1$. However, when $\mathbb{K}$ is a finite field, we do have that $\mathbb{A}^n_{\mathbb{K}}$ is a Hausdorff space.

A common inquiry is whether every affine algebraic set may be defined by a finite number of polynomials. It is neat to notice that this is a reflection of a result from commutative algebra. Before we may appreciate this insight, we recall a *Noetherian topological space*.

Definition 1.5.9. Let $(X, \mathcal{T})$ be a topological space. We say $(X, \mathcal{T})$ is a Noetherian topological space if every chain of descending closed sets eventually stabilizes.

Remark 1.5.10. (i) Let us consider $\mathbb{K}[\underline{x}]$. After inductively applying the Hilbert Basis Theorem, we have that $\mathbb{K}[\underline{x}]$ is a Noetherian ring. Therefore, every ideal $J \subseteqq \mathbb{K}[\underline{x}]$ is generated by finitely many polynomials, so $J = \langle f_1, f_2, \ldots, f_s \rangle$ for some $s \in \mathbb{N}$, where $f_i \in \mathbb{K}[\underline{x}]$. Now apply $\mathcal{Z}$ to both sides and using Proposition 1.1.9.(i),

$$\mathcal{Z}(J) = \mathcal{Z}(f_1, f_2, \ldots, f_s) = \mathcal{Z}(f_1) \cup \mathcal{Z}(f_2) \cup \ldots \mathcal{Z}(f_s).$$

Since J was an arbitrary ideal and every variety is defined by an ideal, we must have that every variety is defined by a finite number of polynomials. Hence, the reflection of a

commutative algebra result.

(ii) This comment follows closely that of [5], Page 21. It is easy to see that the Noetherian nature of $\mathbb{K}[\underline{x}]$ implies that $\mathbb{A}^n_{\mathbb{K}}$ is a Noetherian topological space. Consider a strictly descending chain of algebraic sets

$$V_0 \supsetneqq V_1 \supsetneqq \ldots \supsetneqq V_m \supsetneqq \ldots.$$

This then corresponds to a strictly increasing chain of ideals by *Remark* 1.4.8,

$$\mathcal{I}_{\mathbb{K}}(V_0) \subsetneqq \mathcal{I}_{\mathbb{K}}(V_1) \subsetneqq \ldots \subsetneqq \mathcal{I}_{\mathbb{K}}(V_m) \subsetneqq \ldots.$$

However, this chain of ideals that must stabilize due to the Noetherian nature of $\mathbb{K}[\underline{x}]$. After applying $\mathcal{Z}_{\mathbb{K}}$ to the stabilizing chain of ideals, we get that our strictly descending chain of algebraic sets must stabilize as well.

(iii) It follows from an application of Zorn's Lemma that every non-trivial system of algebraic sets in $\mathbb{A}^n_{\mathbb{K}}$ has a minimal element.

Proof. Consider the collection of all algebraic sets in $\mathbb{A}^n_{\mathbb{K}}$, denote this collection by Λ. We define a reverse ordering on Λ, by $V_1 \leq V_2$ if $V_1 \supseteqq V_2$. It is obvious that Λ is non-empty since $\mathbb{A}^n_{\mathbb{K}} \in \Lambda$. Let us now consider a totally ordered chain of algebraic sets $\{V_\lambda\}_{\lambda \in \Lambda}$ and their intersection $\bigcap_{\lambda \in \Lambda} V_\lambda$. By Proposition 1.3.6, we have that $\bigcap_{\lambda \in \Lambda} V_\lambda$ is an algebraic set. We also have that $\bigcap_{\lambda \in \Lambda} V_\lambda \subset V_\lambda$ for all $\lambda \in \Lambda$. Thus, by our reverse-ordering we have $V_\lambda \leq \bigcap_{\lambda \in \Lambda} V_\lambda$ for all $\lambda \in \Lambda$, showing that the intersection is necessarily an upper bound on our totally ordered set. We may now apply Zorn's Lemma so that there exists a maximal element $W \in \Lambda$. However, due to our reverse-ordering, W corresponds to a minimal algebraic set of $\mathbb{A}^n_{\mathbb{K}}$.

$\square$

We actually may be a little more precise with our decomposition of affine algebraic sets as the following Proposition shows.

Proposition 1.5.11. [[7], Theorem 3.6] For every non-empty affine algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$, we may write V uniquely (up to permutation of factors) in the form

$$V = V_1 \cup V_2 \cup \ldots \cup V_n$$

where V_i are irreducible affine algebraic sets and $V_i \nsubseteqq \bigcup_{i \neq j} V_j$ for all i where $1 \leq i \leq n$.

Proof. Existence: By contradiction, we assume $\exists$ affine algebraic sets that cannot be decomposed as a finite union of irreducible algebraic sets, denote this collection of sets by Λ. By Remark 1.5.10.(iii), there exists a minimal element $W \in \Lambda$. We have that W is not irreducible since otherwise $W \notin \Lambda$. Hence, W is reducible:

$$W = T_1 \cup T_2, \text{ where } T_1, T_2 \text{ are algebraic sets in } \mathbb{A}^n_{\mathbb{K}} \text{ and } T_1, T_2 \neq W.$$

Since W is minimal, it now follows that T_1 and T_2 are not in Λ, implying that they are decomposable into a union of irreducible algebraic sets. This then implies that W is decomposable, which gives a contradiction. After removing the redundant V_i's, if any, we can further obtain a decomposition such that $V_i \nsubseteqq \bigcup_{i \neq j} V_j$ for all i where $1 \leq i \leq n$.

Uniqueness: Hence, we may now assume we have two decompositions for an algebraic set V as stated in Proposition 1.5.11:

$$V = V_1 \cup V_2 \cup \ldots \cup V_n = W_1 \cup W_2 \cup \ldots \cup W_m.$$

We set

$$V_i = V \cap V_i = (W_1 \cap V_i) \cup (W_2 \cap V_i) \cap \ldots \cap (W_m \cap V_i).$$

Since V_i is irreducible, we must have that $V_i = W_j \cap V_i$ for some $j \in [1, m]$, which implies $V_i \subseteqq W_j$. By the same argument, we have that $\exists k \in [1, n]$ such that $W_j \subseteqq V_k$. Hence $V_i \subseteqq V_k$. However, if $k \neq i$, then $V_i \subseteqq \bigcup_{i \neq j} V_j$, which is a contradiction. Therefore, $V_i = W_j$. $\square$

1.6 Rational Points

In the previous section Proposition 1.5.7 states that an irreducible algebraic set $V \subseteq \mathbb{A}^n_{\mathbb{K}}$ defines a prime ideal $\mathcal{I}_{\mathbb{K}}(V) \leq \mathbb{K}[\underline{x}]$. Conversely, if $\mathcal{I}_{\mathbb{K}}(V) \leq \mathbb{K}[\underline{x}]$ is prime for some algebraic set $V \subseteq \mathbb{A}^n_{\mathbb{K}}$, then V is irreducible. We now examine a dual nature of Proposition 1.5.7.

Question 1.6.1.

(i) If $\mathcal{Z}_{\mathbb{K}}(P)$ is irreducible for some ideal $P \leq \mathbb{K}[\underline{x}]$, may we conclude P is prime in $\mathbb{K}[\underline{x}]$?

(ii) For a prime ideal $P \leq \mathbb{K}[\underline{x}]$, may we conclude $\mathcal{Z}_{\mathbb{K}}(P)$ is irreducible?

It turns out Question 1.6.1(i) and (ii) both have counter-examples. This section is dedicated to showing such examples. We first remind the reader of useful results and definitions.

Definition 1.6.2. A *Pythagorean triple* is a set of three integers x, y, z such that $x^2 + y^2 = z^2$; the triple is said to be *primitive* if $\gcd(x, y, z) = 1$.

Lemma 1.6.3. [[1], Chapter 11, Lemma 1] If x, y, z is a primitive Pythagorean triple, then one of the integers x and y is even, while the other is odd.

Lemma 1.6.4. [[1], Chapter 11, Lemma 2] If $ab = c^n$, where $\gcd(a, b) = 1$, then a and b are nth powers; that is, there exist positive integers a_1, b_1 for which $a = a_1^n, b = b_1^n$.

Theorem 1.6.5. [[1], Theorem 11.1] All the solutions of the Pythagorean equation

$$x^2 + y^2 = z^2$$

satisfying the conditions

$$\gcd(x, y, z) = 1 \qquad 2 \mid x \qquad x > 0 \qquad y > 0 \qquad z > 0$$

are given by the formulas

$$x = 2st \qquad y = s^2 - t^2 \qquad z = s^2 + t^2$$

for integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$.

We now give a counter-example to Question 1.6.1(ii). Consider the curve

$$f(x,y) = x^2y + y^2 - 1 \in \mathbb{Q}[x,y].$$

We first show $f(x,y)$ is irreducible. Hence, $f(x,y)$ generates a prime ideal in $\mathbb{Q}[x,y]$. However, we then show $\mathcal{Z}_{\mathbb{Q}}(x^2y+y^2-1) = \{(0,-1),(0,1)\}$ is a union of two points, which is a reducible affine algebraic set.

Proposition 1.6.6. The polynomial $f(x,y) = (x^2y + y^2 - 1)$ is irreducible over $\mathbb{Q}[x,y]$ and

$$\mathcal{Z}_{\mathbb{Q}}(x^2y + y^2 - 1) = \{(0,-1),(0,1)\}.$$

Proof. Suppose $f(x,y)$ is reducible. That is $f(x,y) = h(x,y)g(x,y)$ for some non-units $h(x,y), g(x,y) \in \mathbb{Q}[x,y]$. Since $f(x,y)$ is quadratic in the variable y, we only need consider two cases: either both $h(x,y)$ and $g(x,y)$ are linear in y or one is quadratic in y and the other is a polynomial in only x. For the first case we have,

$$f(x,y) = h(x,y)g(x,y) = (yh_0(x) + h_1(x))(yg_0(x) + g_1(x))$$

After distributing and equating degrees, we must have

$$h_0(x)g_0(x) = 1, h_1(x)g_0(x) + g_1(x)h_0(x) = x^2, \text{ and } h_1(x)g_1(x) = -1.$$

The first and the last relation imply $h_0(x), h_1(x), g_0(x), g_1(x) \in \mathbb{Q}$ but this contradicts $h_1(x)g_0(x) + g_1(x)h_0(x) = x^2$ since $\deg(h_1(x)g_0(x) + g_1(x)h_0(x)) = 0 \neq \deg(x^2) = 2$. As for the second case and without loss of generality, let $h(x)$ be quadratic in y. Then,

$$(y^2h_0(x) + yh_1(x) + h_2(x))g(x) = f(x,y)$$

However, this implies $g(x) \in \mathbb{Q}$, proving $f(x,y)$ is irreducible by definition. Thus we may conclude $f(x,y)$ is irreducible and generates a prime ideal in $\mathbb{Q}[x,y]$.

We now find the zeros for $f(x,y)$ over $\mathbb{Q}$. After solving $f(x,y) = x^2y + y^2 - 1 = 0$ for y, one gets

$$y = \pm\frac{\sqrt{x^4+4} - x^2}{2}.$$

We can see that y is rational if and only if $\sqrt{x^4+4}$ is rational. Thus, let $\frac{a}{b} = \sqrt{x^4+4}$ and $x = \frac{c}{d}$, where $\gcd(a,b) = 1$ and $\gcd(c,d) = 1$. After squaring both sides,

$$\frac{a^2}{b^2} = \frac{c^4}{d^4} + 4,$$

where $\gcd(a,b) = 1$ and $\gcd(c,d) = 1$. Cross multiplying gives us

$$a^2 \cdot d^4 = (c^4 + 4d^4) \cdot b^2 \Rightarrow b^2 \mid d^4 \Rightarrow b \mid d^2.$$

Thus, $b \cdot k = d^2$ for some $k \in \mathbb{Z}$. We then substitute and factor:

$$a^2 \cdot k^2 = c^4 + 4b^2 \cdot k^2 \Rightarrow k^2(a^2 - 4b^2) = c^4 \Rightarrow k^2 \mid c^4 \Rightarrow k \mid c^2.$$

We have that k divides both c^2 and d^2; however, $\gcd(c,d) = 1 \Rightarrow \gcd(c^2,d^2) = 1$. We may conclude that $k = 1$. We now have $a^2 = c^4 + 4d^4$ with $\gcd(a,b) = 1$, $\gcd(c,d) = 1$, and $d^2 = b$. Let

$$\gcd(a,c) = w \Rightarrow a_1 \cdot w = a, c_1 \cdot w = c.$$

After substitution,

$$a_1^2 \cdot w^2 = c_1^4 \cdot w^4 + 4d^4 \Rightarrow w^2(a_1^2 - c_1^4 \cdot w^2) = 4d^4 \Rightarrow w^2 \mid 4d^4.$$

Notice that $\gcd(c,d) = 1 \Rightarrow \gcd(w,d) = 1$, hence $w^2 \mid 4 \Rightarrow w = 1$ or $w = 2$. Let us consider first the case when $\gcd(a,c) = 1$. Assume an integer solution exists for $a^2 = c^4 + 4d^4$. Of all the integer solutions, we consider the solution with $|a|$ to be the smallest. Notice that a, c must both be odd or must both be even. In this case, a, c must both be odd. Therefore, $\gcd(a,2d) = 1$ and $\gcd(a,d) = 1$ because $\gcd(a,b^2) = 1$. We also have that $\gcd(c,2d) = 1$ since c is odd and $\gcd(c,d) = 1$. We may

now apply Theorem 1.6.5,

$$\exists m, n \in \mathbb{Z}, \text{ where } a = m^2 + n^2, c^2 = m^2 - n^2, 2d^2 = 2m \cdot n.$$

The last expression gives $d^2 = m \cdot n$; however, $\gcd(m, n) = 1$. Then we must have that $d^2 = m_1^2 \cdot n_1^2$, where $m_1^2 = m$ and $n_1^2 = n$. We also have that $c^2 + n^2 = m^2$. We apply Theorem 1.6.5 again because $\gcd(d, c) = 1 \Rightarrow (c, n, m) = 1$. Thus,

$$\exists s, t \in \mathbb{Z} \text{ where } s > t > 0 \text{ and } \gcd(s, t) = 1 \text{ such that}$$

$$m = s^2 + t^2, n = 2s \cdot t, c = s^2 - t^2.$$

We also know that $s \not\equiv t \pmod 2$. Without loss of generality, assume s is odd and t is even. Since $t = 2t_1$,

$$n = 2s \cdot t = 2s \cdot 2t_1 \Rightarrow \frac{n}{4} = t_1 \cdot s.$$

However since $\gcd(t_1, s) = 1$,

$$n = n_1^2 \Rightarrow (\frac{n_1}{2})^2 = t_1 \cdot s \Rightarrow t_1 = t_2^2, s = s_1^2.$$

Notice now that

$$m = s^2 + t^2 \Rightarrow m_1^2 = s_1^4 + 4t_1^2 \Rightarrow m_1^2 = s_1^4 + 4t_2^4.$$

Therefore, (m_1, s_1, t_2) is another integral solution such that

$$m_1 \leq m_1^2 = m \leq m^2 < m^2 + n^2 = a.$$

This is a contradiction to our assumption that a was the smallest solution. In the second case we have $\gcd(a, c) = 2$. This implies that

$$\exists a_1, c_1 \in \mathbb{Z} \text{ such that } 2a_1 = a \text{ and } 2c_1 = c.$$

We then have

$$4a_1^2 = 16c_1^4 + 4d^4 \Rightarrow a_1^2 = 4c_1^4 + d^4.$$

Notice that $\gcd(a_1, c_1) = 1, \gcd(c_1, d) = 1$, and $(a_1, d^2) = 1$ since $\gcd(a, b^4) = 1$. Once again, a_1 and d must be of the same parity, and in this case they are both odd. Therefore $(a_1, 2c^2) = 1$ and $(d^2, 2c_1^2) = 1$, which brings us back to the first case. Hence, the proof is exactly the same as before, showing that $a^2 = c^4 + 4d^4$ has no non-trivial solutions. Therefore, $\sqrt{x^4 + 4}$ is never rational for $x \neq 0$, so the only rational solutions to $f(x, y) = x^2y + y^2 - 1$ are $(0, \pm 1)$. $\square$

As for a counterexample over $\mathbb{R}$, consider the curve $h(x, y) = (x^2 - 1)^2 + y^2 \in \mathbb{R}[x, y]$. The irreducibility of $h(x, y)$ is similar to that of the argument given above. As for the solutions of $h(x, y)$ over $\mathbb{R}$, we have

$$\mathcal{Z}_{\mathbb{R}}((x^2 - 1)^2 + y^2) = \mathcal{Z}_{\mathbb{R}}(x^2 - 1, y) = \mathcal{Z}_{\mathbb{R}}(x^2 - 1) \cap \mathcal{Z}_{\mathbb{R}}(y) = \{(\pm 1, 0)\}$$

Hence, $\mathcal{Z}_{\mathbb{R}}((x^2 - 1)^2 + y^2)$ is once again reducible since it is a union of two points, although $(x^2 - 1)^2 + y^2$ generates a prime ideal.

We now consider Question 1.6.1(i). We will see in Chapter 2 that with an extra hypothesis on the prime ideal P the statement becomes valid. For the moment, we give a counter example:

Example 1.6.7. Consider the set $\mathcal{Z}_{\mathbb{R}}((x^2 + 1)x, (x^2 + 1)y) \subseteqq \mathbb{A}_{\mathbb{R}}$. We have that

$$\mathcal{Z}_{\mathbb{R}}((x^2 + 1)x, (x^2 + 1)y) = \mathcal{Z}_{\mathbb{R}}(x^2 + 1) \cup \mathcal{Z}_{\mathbb{R}}(x, y) = \varnothing \cup \mathcal{Z}_{\mathbb{R}}(y) = \mathcal{Z}_{\mathbb{R}}(x, y),$$

which is the origin of the coordinate plane over $\mathbb{R}$. The origin is a single point of the affine plane, so is irreducible. One easily notices however, that the ideal $\langle (x^2 + 1)x, (x^2 + 1)y) \rangle$ is not prime in $\mathbb{R}[x, y]$.

1.7 Hilbert Nullstellensatz

This section will introduce the classical Hilbert-Nullstellensatz and give a few variations. We first start with an algebraic interpretation, known as *Zariski's lemma*. Recall not all finitely generated $\mathbb{K}$-algebras are finitely generated as $\mathbb{K}$-modules. For instance, the polynomial ring $\mathbb{K}[x]$ is a finitely generated $\mathbb{K}$-algebra but has a countably infinite basis as a $\mathbb{K}$-module,

$$\left\{x^0, x^1, x^2, x^3, \ldots, x^m, \ldots\right\}.$$

Zariski's lemma equates these notions.

Theorem 1.7.1 (Zariski's Lemma). Let $\mathbb{K} \subseteqq \mathbb{L}$ be a field extension. If $\mathbb{L}$ is a finitely generated $\mathbb{K}$-algebra then $\mathbb{L}$ is algebraic over $\mathbb{K}$, i.e., a finitely generated $\mathbb{K}$-module.

Proof. Let $\mathbb{L}$ be a finitely generated $\mathbb{K}$-algebra,

$$\mathbb{L} = \mathbb{K}[x_1, x_2, \ldots, x_s] \text{ for some } s \in \mathbb{N}.$$

Then by Noether normalization, there exist $y_1, y_2, \ldots, y_m \in \mathbb{L}$ for some $m \leq s$ such that

$$\mathbb{K}[y_1, y_2, \ldots, y_m] \subseteqq \mathbb{L}$$

is a finite extension, i.e., $\mathbb{L}$ is a module-finite $\mathbb{K}[y_1, y_2, \ldots, y_m]$-algebra. However, Lemma 1.2.16 implies $\mathbb{K}[y_1, y_2, \ldots, y_m]$ is a field. This can only be the case when $m = 0$. Therefore $\mathbb{L}$ is a finite extension of $\mathbb{K}$, i.e., an algebraic extension of $\mathbb{K}$. $\square$

Corollary 1.7.2. For a finitely generated $\mathbb{K}$-algebra B and a maximal ideal $\mathfrak{m} \leq B$,

$$\frac{B}{\mathfrak{m}} \text{ is finite extension of } \mathbb{K}.$$

This interpretation of the Hilbert-Nullstellensatz does not assume $\mathbb{K}$ is an algebraically closed field. Hence, we may get an insight into what happens with maximal ideals in a general ploynomial

ring $\mathbb{K}[\underline{x}]$. For instance in $\mathbb{R}[x]$, there exist two kinds of maximal ideals. Let $\mathfrak{m} \leq \mathbb{R}[x]$. If $\frac{\mathbb{R}[x]}{\mathfrak{m}} \cong \mathbb{R}$, then we recover Theorem 1.7.3 and $\mathfrak{m}$ is of the form $\langle x - a \rangle$ for some $a \in \mathbb{R}$. However, we may have $\frac{\mathbb{R}[x]}{\mathfrak{m}} \cong \mathbb{C}$. In this case $\frac{\mathbb{R}[x]}{\mathfrak{m}}$ is a degree two extension of $\mathbb{R}$. We have that $\mathcal{Z}_{\mathbb{R}}(\mathfrak{m}) = \varnothing$, However, $\mathfrak{m}$ corresponds to two points in $\mathbb{A}_{\mathbb{C}}$. To see this notice the isomorphism implies there is a surjective homomorphism $\varphi: \mathbb{R}[x] \longrightarrow \mathbb{C}$ with $\ker(\varphi) = \mathfrak{m}$. Consider now the image of x in $\mathbb{C}$, $\varphi(x) = a + bi$ for some $a, b \in \mathbb{R}$. Since

$$2 = [\mathbb{C} : \mathbb{R}] = [\mathbb{R}(a + bi) : \mathbb{R}][\mathbb{C} : \mathbb{R}(a + bi)]$$

We must have $[\mathbb{R}(a + bi) : \mathbb{R}] = 2$. Therefore the minimal polynomial of $a + bi$ has $a - bi$ as a zero as well. Thus, we must have $(x - (a + bi))(x - (a - bi)) \in \ker(\varphi) = \mathfrak{m}$. Hence, $\mathfrak{m}$ corresponds to a conjugate pair of points in $\mathbb{A}_{\mathbb{C}}$. In general, for a maximal ideal $\mathfrak{m} \leq \mathbb{K}[x]$, $\mathfrak{m}$ corresponds to d (not necessarily distinct) conjugate points in a finite extension of $\mathbb{K}$, where $d = deg(f)$ with $\langle f \rangle = \mathfrak{m}$.

Theorem 1.7.3. [Weak Hilbert-Nullstellensatz *I*] Let $\mathbb{K}$ be an algebraically closed field. There is a one to one correspondence between maximal ideals of $\mathbb{K}[\underline{x}]$ and points of $\mathbb{A}^n_{\mathbb{K}}$; i.e., every maximal ideal of $\mathbb{K}[\underline{x}]$ has the form

$$\mathfrak{m}_{\underline{a}} := \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle \text{ for some } \underline{a} \in \mathbb{A}^n_{\mathbb{K}}.$$

Proof. For any point $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$, we have a homomorphism

$$\mathbb{K}[\underline{x}] \longrightarrow \mathbb{K}$$

$$f \longmapsto f(\underline{a}).$$

This map induces the isomorphism, $\frac{\mathbb{K}[\underline{x}]}{\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle} \cong \mathbb{K}$. Hence, $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$ is a maximal ideal.

Now let $\mathfrak{m} \leq \mathbb{K}[\underline{x}]$ be a maximal ideal. Since, $\frac{\mathbb{K}[\underline{x}]}{\mathfrak{m}}$ is a finitely generated $\mathbb{K}$-algebra, we may apply Zariski's Lemma, showing $\mathbb{K} \subseteqq \frac{\mathbb{K}[\underline{x}]}{\mathfrak{m}}$ is an algebraic field extension. However, since $\mathbb{K}$ is algebraically closed,

$$\mathbb{K} \subseteqq \frac{\mathbb{K}[\underline{x}]}{\mathfrak{m}} \subseteqq \mathbb{K} \Rightarrow \mathbb{K} \cong \frac{\mathbb{K}[\underline{x}]}{\mathfrak{m}},$$

which is an isomorphism of $\mathbb{K}$-algebras. Hence, we have a surjective $\mathbb{K}$-algebra homomorphism

$$\varphi\colon \mathbb{K}[\underline{x}] \longrightarrow \mathbb{K}$$

where $\ker\varphi = \mathfrak{m}$. Therefore, the images of the x_i under φ must be elements of $\mathbb{K}$ for all $i, 1 \leq i \leq n$. Let $\varphi(x_i) = a_i$, then $a_i \equiv x_i \pmod{\mathfrak{m}}$, and

$$\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle \subseteqq \mathfrak{m}.$$

We then necessarily have equality since $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$ is already maximal. □

Theorem 1.7.4. [Weak Hilbert-Nullstellensatz *II*] Let $\mathbb{K}$ be an algebraically closed field and let $I \nleq \mathbb{K}[\underline{x}]$ be a proper ideal. Then,

$$\mathcal{Z}_{\mathbb{K}}(I) \neq \varnothing.$$

Proof. By a standard application of Zorn's Lemma, there exists a maximal ideal $\mathfrak{m}$ containing I. This maximal ideal must be one of the form $\mathfrak{m}_{\underline{a}}$ for some $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$, by Theorem 1.7.3. Due to the inclusion-reversing property of $\mathcal{Z}_{\mathbb{K}}$,

$$I \subseteqq \mathfrak{m}_{\underline{a}} \Rightarrow \mathcal{Z}_{\mathbb{K}}(\mathfrak{m}_{\underline{a}}) = \{\underline{a}\} \subseteqq \mathcal{Z}(I).$$

Hence, $\mathcal{Z}_{\mathbb{K}}(I) \neq \varnothing$. □

Theorem 1.7.5. [Strong Hilbert-Nullstellensatz *I*] Let $\mathbb{K}$ be an algebraically closed field and let $I \leq \mathbb{K}[\underline{x}]$. Then

$$\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I)) = \sqrt{I}.$$

Proof. We have that $I \subseteqq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))$ from Proposition 1.4.7. After taking radicals of both sides, Proposition 1.4.9 implies

$$\sqrt{I} \subseteqq \sqrt{\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))} = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I)).$$

The argument for the forward containment is known as the *Rabinowitsch's Trick*. Let $f \in \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))$. From Hilbert's basis theorem, we know that I is finitely generated, say

$I = \langle f_1, f_2, \ldots, f_m \rangle$. We introduce a new variable y and define an ideal

$$\tilde{I} := \langle f_1, f_2, \ldots, f_m, 1 - f \cdot y \rangle \leq \mathbb{K}[x_1, x_2, \ldots, x_n, y].$$

We now consider the affine algebraic set, $\mathcal{Z}_{\mathbb{K}}(\tilde{I}) \subseteqq \mathbb{A}_{\mathbb{K}}^{n+1}$ and show $\mathcal{Z}_{\mathbb{K}}(\tilde{I}) = \varnothing$. Assume this is not the case, so that $\mathcal{Z}_{\mathbb{K}}(\tilde{I}) \neq \varnothing$. Then the exists a point $(a_1, a_2, \ldots, a_n, a_{n+1}) \in \mathcal{Z}_{\mathbb{K}}(\tilde{I})$. Let us consider I as an ideal of $\mathbb{K}[x_1, x_2, \ldots, x_n, y]$ and notice $I \subseteqq \tilde{I}$, hence $\mathcal{Z}_{\mathbb{K}}(\tilde{I}) \subseteqq \mathcal{Z}_{\mathbb{K}}(I)$. Thus, $(a_1, a_2, \ldots, a_n) \in \mathcal{Z}_{\mathbb{K}}(I)$ and $f_i(a_1, a_2, \ldots, a_n) = 0$ for all $i, 1 \leq i \leq m$. By our hypothesis, $f(a_1, a_2, \ldots, a_n) = 0$ as well. However,

$$(1 - f \cdot y)(a_1, a_2, \ldots, a_n, a_{n+1}) = 1 - f(a_1, a_2, \ldots, a_n) \cdot a_{n+1} = 1 - 0 = 1,$$

contradicting the fact that $(a_1, a_2, \ldots, a_n, a_{n+1}) \in \mathcal{Z}_{\mathbb{K}}(\tilde{I})$. We then may conclude that $\mathcal{Z}_{\mathbb{K}}(\tilde{I}) = \varnothing$. The contrapositive of the Weak Hilbert-Nullstellensatz then implies $1 \in \tilde{I}$. Thus,

$$\sum_{i=1}^{m} h_i \cdot f_i + h_{n+1} \cdot (1 - f \cdot y) = 1, \text{ where } h_i \in \mathbb{K}[x_1, x_2, \ldots, x_n, y] \text{ for all } i, 1 \leq i \leq n+1.$$

If we now substitute $\frac{1}{f}$ for y, we get the following expression

$$\sum_{i=1}^{m} h_i(x_1, x_2, \ldots, x_n, \frac{1}{f}) \cdot f_i(x_1, x_2, \ldots, x_n) = 1.$$

After obtaining a common denominator, we have

$$\frac{\sum_{i=1}^{m} h_i'(x_1, x_2, \ldots, x_n) \cdot f_i(x_1, x_2, \ldots, x_n)}{f^m} = 1 \Rightarrow f^m = \sum_{i=1}^{m} h_i'(x_1, x_2, \ldots, x_n) \cdot f_i(x_1, x_2, \ldots, x_n),$$

where $h_i'(x_1, x_2, \ldots, x_n) = h_i(x_1, x_2, \ldots, x_n) \cdot$ (a power of f). Therefore, $f \in \sqrt{I}$, finishing the proof. □

Theorem 1.7.6. [[5], Corollary 1.17, Strong Hilbert-Nullstellensatz II] Let $\mathbb{K}$ be an algebraically closed field. There is a bijective correspondence between the following pairs of sets:

$$\{\text{affine algebraic sets}\} \text{ and } \{\text{radical ideals}\}$$

$$\{\text{Irreducible affine algebraic sets}\} \text{ and } \{\text{prime ideals}\}$$

$$\{\text{points}\} \text{ and } \{\text{maximal ideals}\}$$

Proof. For every algebraic set $X \subseteq \mathbb{A}^n_{\mathbb{K}}$, we have $\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V)) = V$ by Proposition 1.4.7. Conversely, by Theorem 1.7.5, for every ideal J we have $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J)) = \sqrt{J}$, providing the first bijection. The second bijection follows from Proposition 1.5.7. The fact that points correspond to maximal ideals is precisely that statement of Theorem 1.6.4. □

Consider an irreducible algebraic set V. Notice that the projection $\pi\colon \mathbb{K}[\underline{x}] \longrightarrow \mathbb{K}[V]$ induces a bijective correspondence between ideals of $\mathbb{K}[V]$ and ideals of $\mathbb{K}[\underline{x}]$ that contain $\mathcal{I}_{\mathbb{K}}(V)$ by Theorem 1.2.6. Thus there is an induced bijective correspondence:

$$\{\text{affine algebraic subsets of } V\} \leftrightarrow \{\text{radical ideals of } \mathbb{K}[V]\}$$

$$\{\text{Irreducible affine algebraic subsets of } V\} \leftrightarrow \{\text{prime ideals of } \mathbb{K}[V]\}$$

$$\{\text{points of } V\} \leftrightarrow \{\text{maximal ideals of } \mathbb{K}[V]\}$$

We may in particular apply the Hilbert-Nullstellensatz to the coordinate ring of functions $\mathbb{K}[V]$ for al irreducible algebraic set V.

Theorem 1.7.7. [[2], Corollary 33, Strong Hilbert Nullstellensatz III] Let $\mathbb{K}$ be any field where $\overline{\mathbb{K}}$ is the algebraic closure and let $J \leq \mathbb{K}[\underline{x}]$. Then $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)) = \sqrt{J}$, where $\mathcal{Z}_{\overline{\mathbb{K}}}(J)$ is the zero set in $\overline{\mathbb{K}}^n$ of polynomials from J, and $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J))$ is the ideal of polynomials from $\mathbb{K}[x_1, \ldots, x_n]$ vanishing at all points of $\mathcal{Z}_{\overline{\mathbb{K}}}(J)$.

Proof. Consider the integral extension

$$\varphi : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \overline{\mathbb{K}}[x_1, \ldots, x_n].$$

Extend J to $\overline{\mathbb{K}}[x_1, \ldots, x_n]$ and apply Hilbert Nullstellensatz,

$$\mathcal{I}_{\overline{\mathbb{K}}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n])) = \sqrt{J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n]}.$$

Then contract the left side of the equality back to $\mathbb{K}[x_1, \ldots, x_n]$,

$$\mathcal{I}_{\overline{\mathbb{K}}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n])) \cap \mathbb{K}[x_1, \ldots, x_n] = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n])) = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)),$$

with the first equality given by set theoretic definitions and the second by Proposition 1.3.3(ii) (J is considered a set in $\overline{\mathbb{K}}[x_1, \ldots, x_n]$). The contraction of the right side of the equality above gives,

$$\sqrt{J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n]} \cap \mathbb{K}[x_1, \ldots, x_n].$$

However by Lemma 1.2.5, we have

$$\sqrt{J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n]} \cap \mathbb{K}[x_1, \ldots, x_n] = \sqrt{J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n] \cap \mathbb{K}[x_1, \ldots, x_n]}.$$

The following Lemma shows that $J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n] \cap \mathbb{K}[x_1, \ldots, x_n] = J$ for all $J \leq \mathbb{K}[x_1, \ldots, x_n]$. Thus

$$\sqrt{J \cdot \overline{\mathbb{K}}[x_1, \ldots, x_n] \cap \mathbb{K}[x_1, \ldots, x_n]} = \sqrt{J},$$

so $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)) = \sqrt{J}$. □

Lemma 1.7.8. Consider the integral extension $\varphi: \mathbb{K}[\underline{x}] \longrightarrow \overline{\mathbb{K}}[\underline{x}]$. Then for all ideals $\mathfrak{b} \leq \mathbb{K}[\underline{x}]$, we have

$$\mathfrak{b}\overline{\mathbb{K}}[\underline{x}] \cap \mathbb{K}[\underline{x}] = \mathfrak{b},$$

where $\mathfrak{b}\overline{\mathbb{K}}[\underline{x}]$ is the ideal generated by its image under φ in $\overline{\mathbb{K}}[\underline{x}]$.

Proof. We will show the integral extension $\varphi : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \overline{\mathbb{K}}[x_1, \ldots, x_n]$ is a faithfully flat homomorphism, which by Theorem 1.2.17 concludes the result. Notice $\overline{\mathbb{K}}$ is a free $\mathbb{K}$-module since its a vector space over $\mathbb{K}$, hence $\overline{\mathbb{K}} = \bigoplus_{i \in I} \mathbb{K} := \mathbb{K}^{(I)}$. Note also that $\overline{\mathbb{K}}$ is flat over $\mathbb{K}$ since it is free over $\mathbb{K}$. For any nonzero module, M, we have

$$\overline{\mathbb{K}} \otimes_{\mathbb{K}} M = \mathbb{K}^{(I)} \otimes_{\mathbb{K}} M = M^{(I)} \neq 0.$$

Thus $\overline{\mathbb{K}}$ is faithfully flat over $\mathbb{K}$. Now by the change of base property for faithfully flatness, we

have that

$$\overline{\mathbb{K}}[x_1,\ldots,x_n] = \mathbb{K}[x_1,\ldots,x_n] \otimes_{\mathbb{K}} \overline{\mathbb{K}} = \mathbb{K}[x_1,\ldots,x_n]^{(I)}$$

is faithfully flat as a $\mathbb{K}[x_1,\ldots,x_n]$-module. This implies that φ is a faithfully flat homomorphism. Finally by Theorem 1.2.17, the result follows. □

Before we get to a variant of the Hilbert Nullstellensatz for finite fields, we would now like to consider $J \subseteq \mathbb{F}_q[x_1,\ldots,x_n]$ where $\mathbb{F}_q$ is the finite field with q elements($q = p^e$ for some prime p) and $\mathcal{Z}_{\mathbb{L}}(J) = \mathcal{Z}_{\overline{\mathbb{F}}_q}(J) \cap \mathbb{L}$, where $\mathbb{L} = \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \ldots \times \mathbb{F}_{q_n}$ with each q_i as an arbitrary power of p. We need one more lemma before we get there:

Lemma 1.7.9. [[3], Lemma 3.1.1.] If $J \subseteq \mathbb{F}_q[x_1,\ldots,x_n]$, then $J + \langle x_1^{q_1} - x_1, x_2^{q_2} - x_2, \ldots, x_n^{q_n} - x_n\rangle$ is a radical ideal, where each q_i is an arbitrary power of p.

Proof. Let $f \in \sqrt{J + \langle x_1^{q_1} - x_1, x_2^{q_2} - x_2, \ldots, x_n^{q_n} - x_n\rangle}$. Then

$$f^m \in J + \langle x_1^{q_1} - x_1, x_2^{q_2} - x_2, \ldots, x_n^{q_n} - x_n\rangle,$$

for some $m \in \mathbb{N}$. Consider the surjection

$$\varphi : \mathbb{F}_q[x_1,\ldots,x_n] \to \mathbb{F}_q[x_1,\ldots,x_n]/\langle x_1^{q_1} - x_1, x_2^{q_2} - x_2, \ldots, x_n^{q_n} - x_n\rangle.$$

Then $(\tilde{f})^m \in \tilde{J}$. Notice $(\tilde{f})^l = \tilde{f}$, where $l = \mathrm{lcm}(q, q_1, q_2, \ldots, q_n)$. This follows from Fermat's Little Theorem and the fact that $l = \mathrm{lcm}(q, q_1, q_2, \ldots, q_n)$. Therefore, $(\tilde{f})^m(\tilde{f})^{l-m} = (\tilde{f})^l = \tilde{f}$. So, $\tilde{f} \in \tilde{J}$ or $f \in J + \langle x_1^{q_1} - x_1, x_2^{q_2} - x_2, \ldots, x_n^{q_n} - x_n\rangle$. The opposite containment is obvious. □

Theorem 1.7.10 (A variant of Hilbert Nullstellensatz over finite fields). Let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^e$ for some prime p and let $J \subseteq \mathbb{F}_q[x_1,\ldots,x_n]$. Also let $\mathbb{L} = \mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \ldots \times \mathbb{F}_{q_n}$ where each q_i is an arbitrary power of p. Then

$$\mathcal{I}_{\mathbb{F}_q}(\mathcal{Z}_{\mathbb{L}}(J)) = J + \langle x_1^{q_1} - x_1, x_2^{q_2} - x_2, \ldots, x_n^{q_n} - x_n\rangle$$

Proof. By the variant we have that,

$$\begin{aligned}\mathcal{I}_{\mathbb{F}_q}(\mathcal{Z}_{\overline{\mathbb{F}}_q}(J+\langle x_1^{q_1}-x_1, x_2^{q_2}-x_2, \ldots, x_n^{q_n}-x_n\rangle)) &= \sqrt{J+\langle x_1^{q_1}-x_1, x_2^{q_2}-x_2, \ldots, x_n^{q_n}-x_n\rangle} \\ &= J+\langle x_1^{q_1}-x_1, x_2^{q_2}-x_2, \ldots, x_n^{q_n}-x_n\rangle,\end{aligned}$$

by Lemma 1.7.9. However,

$$\begin{aligned}\mathcal{Z}_{\overline{\mathbb{F}}_q}(J+\langle x_1^{q_1}-x_1, x_2^{q_2}-x_2, \ldots, x_n^{q_n}-x_n\rangle) &= \mathcal{Z}_{\overline{\mathbb{F}}_q}(J)\cap\mathcal{V}_{\overline{\mathbb{F}}_q}(\langle x_1^{q_1}-x_1, x_2^{q_2}-x_2, \ldots, x_n^{q_n}-x_n\rangle) \\ &= \mathcal{Z}_{\overline{\mathbb{F}}_q}(J)\cap\mathbb{L} \\ &= \mathcal{Z}_{\mathbb{L}}(J),\end{aligned}$$

by definition. Now apply $\mathcal{I}_{\mathbb{F}_q}$ to both sides. □

Theorem 1.7.11. [[3], Theorem 3.2, Strong Hilbert-Nullstellensatz over finite fields] Let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^e$ for some prime p and let $J \leq \mathbb{F}_q[x_1, \ldots, x_n]$. Then

$$\mathcal{I}_{\mathbb{F}_q}(\mathcal{Z}_{\mathbb{F}_q}(J)) = J+\langle x_1^q-x_1, x_2^q-x_2, \ldots, x_n^q-x_n\rangle.$$

Proof. This is a special case of the variant proved above, where $q = q_1 = q_2 = \ldots = q_n$. □

We mentioned we would show the vanishing ideal of $\mathbb{A}^n_{\mathbb{K}}$ over a finite field $\mathbb{K}$.

Corollary 1.7.12. Let $|\mathbb{K}| = q$ where $q = p^e$ for some prime $p \in \mathbb{N}$ and some $e \in \mathbb{N}$, then

$$\mathcal{I}_{\mathbb{K}}(\mathbb{A}^n_{\mathbb{K}}) = \langle x_1^q-x_1, x_2^q-x_2, \ldots, x_n^q-x_n\rangle \leq \mathbb{K}[\underline{x}].$$

Proof. Take J to be the zero ideal of $\mathbb{F}_q[x_1, \ldots, x_n]$ in Theorem 1.7.11. □

CHAPTER 2

TOPOLOGY AND DIMENSION

2.1 Maps on Irreducible Affine Algebraic Sets

In this section, our exposition closely follows that of [4] and [5]. We assume $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ to be an irreducible affine algebraic set throughout this section. Recall a *polynomial function* defined on V is function from V to $\mathbb{A}_{\mathbb{K}} = \mathbb{K}$ that may be represented as a polynomial from $\mathbb{K}[\underline{x}]$. In Section 1.4, we identified the set of all such functions with the *coordinate ring* of V,

$$\{f \mid f \text{ is a polynomial function on } V\} \cong \mathbb{K}[V] = \frac{\mathbb{K}[\underline{x}]}{\mathcal{I}_{\mathbb{K}}(V)}.$$

Therefore from now on we will identify the elements of $\mathbb{K}[V]$ as polynomial functions from V to $\mathbb{K}$.

Additionally, since we are assuming V is irreducible, Proposition 1.5.7 states that $\mathcal{I}_{\mathbb{K}}(V)$ is a prime ideal. Hence $\mathbb{K}[V]$ is an integral domain and we may consider then the field of fractions of $\mathbb{K}[V]$.

Definition 2.1.1. Let $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ be an irreducible affine algebraic set. The field of fractions of $\mathbb{K}[V]$ is known as the *field of rational functions* on V, denoted $\mathbb{K}(V)$.

Definition 2.1.2. An $h \in \mathbb{K}(V)$ is *regular* at a point $p \in V$ if there exist elements $f, g \in \mathbb{K}[V]$ such that $h = \frac{f}{g}$ and $g(p) \neq 0$.

Definition 2.1.3. The *ring of regular functions* at a point $p \in V$ is the set of all regular functions at p,

$$\mathcal{O}_{V,p} := \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathbb{K}[V] \text{ and } g(p) \neq 0 \right\} \subset \mathbb{K}(V).$$

Remark 2.1.4. (i) $\mathcal{O}_{V,p}$ is a local ring. We have that the unique maximal ideal of $\mathcal{O}_{V,p}$ is

$$m_{V,p} := \left\{ \frac{f}{g} \in \mathbb{K}(V) \;\middle|\; f(p) = 0, g(p) \neq 0 \right\} \leq \mathcal{O}_{V,p}.$$

We see this by noticing $\mathcal{O}_{V,p} \smallsetminus m_{V,p}$ is the set of invertible elements of $\mathcal{O}_{V,p}$. If $h \in \mathcal{O}_{V,p} \smallsetminus m_{V,p}$, then $h(p) \neq 0$. Hence, h may be inverted, showing $\mathcal{O}_{V,p}$ is a local ring by Lemma 1.2.7.

(ii) The set of all elements $f \in \mathbb{K}[V]$ such that $f(p) = 0$ forms an ideal of $\mathbb{K}[V]$, i.e.,

$$\mathfrak{m}_{V,p} := \{ f \in \mathbb{K}[V] \mid f(p) = 0 \} \leq \mathbb{K}[V].$$

Consider the natural surjection $\pi\colon \mathbb{K}[\underline{x}] \longrightarrow \mathbb{K}[V]$. Ideals of $\mathbb{K}[\underline{x}]$ that contain $\mathcal{I}_{\mathbb{K}}(V)$ bijectively correspond to ideals of $\mathbb{K}[V]$. Hence the maximal ideal $\mathcal{I}_{\mathbb{K}}(\{p\})$ of $\mathbb{K}[\underline{x}]$ corresponds to the maximal ideal $\mathcal{I}_{\mathbb{K}}(\{p\}) + \mathcal{I}_{\mathbb{K}}(V) = \mathfrak{m}_{V,p}$ of $\mathbb{K}[V]$. Thus, we may then regard $\mathcal{O}_{V,p}$ as the localization of $\mathbb{K}[V]$ by $\mathfrak{m}_{V,p}$,

$$\mathbb{K}[V]_{\mathfrak{m}_{V,p}} = \mathcal{O}_{V,p}.$$

Definition 2.1.5. Let V be a non-empty affine algebraic set. Then the *ring of regular functions* on V is the set

$$\mathcal{O}_V(V) := \bigcap_{p \in V} \mathcal{O}_{V,p} \subset \mathbb{K}(V).$$

Lemma 2.1.6. Let $f \in \mathbb{K}[\underline{x}]$ and let $U \subseteqq V$ be a non-empty open set of V. Then

$$f \restriction_U = 0 \Rightarrow f \restriction_V = 0.$$

Proof. We have that $f \restriction_U = 0$ and let us assume $f \restriction_V \neq 0$. Then there must exist a point $\underline{a} \in (V \smallsetminus U)$ such that $f(\underline{a}) \neq 0$. Consider the set $D_V(f) := \{\underline{v} \in V \mid f(\underline{v}) \neq 0\}$. This set is open in V since $V \smallsetminus (\mathcal{Z}_{\mathbb{K}}(f) \cap V) = D_V(f)$ where $(\mathcal{Z}_{\mathbb{K}}(f) \cap V)$ is obviously a closed set in V. Therefore, we have two non-empty open sets U and $D_V(f)$ in V such that $U \cap D_V(f) = \varnothing$, which contradicts the fact the V is irreducible. Hence, we must have $f \restriction_V = 0$. □

Consider an element $h \in \mathcal{O}_{V,p}$. Then $h = \frac{f}{g}$ for some $f, g \in \mathbb{K}[V]$, which implies h is regular on

the open set $D_V(g)$. Thus we introduce a slightly different but equivalent definition of regularity.

Definition 2.1.7. Let $h: V \longrightarrow \mathbb{A}_{\mathbb{K}}$ be a function. Then h is regular at a point $p \in V$ if there exists an open neighborhood of p, $U_p \subseteqq V$ such that $h(\underline{a}) = \frac{f(\underline{a})}{g(\underline{a})}$ for all $\underline{a} \in U_p$ where $f, g \in \mathbb{K}[\underline{x}]$. We say h is regular if it is regular at every point in V.

Lemma 2.1.8 ([4], Lemma 2.1.8.). Definition 2.1.5 is equivalent to the Definition 2.1.7

Proof. The forward direction is obvious. Conversely, let $h: V \longrightarrow \mathbb{A}_{\mathbb{K}}$ be a regular function as in Definition 2.1.7. Then for any point $p \in V$ there exist polynomials $f, g \in \mathbb{K}[\underline{x}]$ such that $h(\underline{a}) = \frac{f(\underline{a})}{g(\underline{a})}$ and $g(\underline{a}) \neq 0$ for all $\underline{a} \in U_p$, where U_p is an open neighborhood of p in V. We claim $\frac{f}{g} \in \mathbb{K}(V)$ is an element of the ring of regular functions as in Definition 2.1.5. In fact we show this element does not depend on the choices we made. Let us consider another point $q \in V$ (not necessarily distinct from p), and suppose there exists polynomials $f', g' \in \mathbb{K}[\underline{x}]$ such that $h = \frac{f'}{g'}$ for some open neighborhood of q, $U_q \subseteqq V$. Then $fg' = gf'$ on the non-empty open set $U_p \cap U_q$. This implies $fg' - gf' = 0$ on the non-empty open set $U_p \cap U_q$, and by Lemma 2.1.6, $fg' - gf' = 0$ on V. Hence, $fg' - gf' \in \mathcal{I}_{\mathbb{K}}(V)$, which is zero in $\mathbb{K}[V]$. Therefore $\frac{f}{g} = \frac{f'}{g'} \in \mathbb{K}(V)$. □

Proposition 2.1.9. Let $\mathbb{K}$ be an algebraically closed field. Then

$$\mathcal{O}_V(V) = \mathbb{K}[V].$$

Proof. The reverse containment is obvious: if $f \in \mathbb{K}[V]$, then $\frac{f}{1} \in \mathcal{O}_V(V)$. For the forward containment, let $h \in \mathcal{O}_V(V)$. Then for all points $p \in V$ there exists $f_p, g_p \in \mathbb{K}[V]$ such that $h = \frac{f_p}{g_p}$ and $g_p(p) \neq 0$. Consider now the ideal generated by all the g_p, $\langle \{g_p\}_{p \in V} \rangle = G$. Now we must have $\mathcal{Z}_{\mathbb{K}}(G) \cap V = \mathcal{Z}_V(G) = \varnothing$ otherwise would contradict our choices of g_p. Thus apply the contrapositive of Theorem 1.7.4 to the ideal $G \leq \mathbb{K}[V]$, implying $\mathcal{I}_V(\mathcal{Z}_V(G)) = \langle 1 \rangle$ in $\mathbb{K}[V]$, where $\mathcal{I}_V(\mathcal{Z}_V(G)) := \{f \in \mathbb{K}[V] \mid f(v) = 0 \text{ for all } v \in \mathcal{Z}_V(G)\}$. Thus, there exists $k_j \in \mathbb{K}[V]$ and $g_i = g_{p_i} \in G$ for $i = 1, 2, \ldots, m$ such that $\sum_{i=1}^{m} k_i g_i = 1$. If we now multiply both sides by h we get,

$$\sum_{i=1}^{m} k_i g_i h = \sum_{i=1}^{m} k_i f_i = h,$$

where $f_i = f_{p_i}$ for $i = 1, 2, \ldots, m$ and since $h = \frac{f_p}{g_p}$. Therefore h is a sum of products of elements from $\mathbb{K}[V]$, which implies $\mathcal{O}_V(V) \subseteq \mathbb{K}[V]$. $\square$

Remark 2.1.10. Another common definition of regularity: A function $\varphi: V \longrightarrow \mathbb{A}_{\mathbb{K}}$ is regular if there exists a polynomial function $F \in \mathbb{K}[\underline{x}]$ such that $F \restriction_V = \varphi$. Proposition 2.1.9 does in fact show all regular functions are restrictions of polynomials from $\mathbb{K}[\underline{x}]$. However, Proposition 2.1.9 is only true over an algebraically closed field as the following example shows.

Example 2.1.11. Consider $\mathbb{A}_{\mathbb{R}}$. We have that $\frac{1}{x^2+1}$ is regular on all of $\mathbb{A}_{\mathbb{R}}$ and is not a restriction of a polynomial. This example also shows that $\mathbb{K}[V] \subsetneqq \mathcal{O}_V(V)$ when $\mathbb{K}$ is not algebraically closed. Hence, the ring of regular functions lies somewhere in between the coordinate ring of functions and the field of rational functions.

We now examine maps between two affine algebraic sets. Consider two affine algebraic sets $X \subseteq \mathbb{A}^n_{\mathbb{K}}$ and $Y \subseteq \mathbb{A}^m_{\mathbb{K}}$.

Definition 2.1.12. A map $\varphi: X \longrightarrow Y$ is a *polynomial map* if there exists polynomials $f_1, f_2, \ldots, f_m \in \mathbb{K}[\underline{x}]$ such that $\varphi(\underline{a}) = (f_1(\underline{a}), f_2(\underline{a}), \ldots, f_m(\underline{a})) \in Y \subseteq \mathbb{A}^m_{\mathbb{K}}$ for all $\underline{a} \in X$. We denote the set of polynomial maps from X to Y by $Poly(X, Y)$

Let $\varphi: X \longrightarrow Y$ be a polynomial map, and consider an element $f \in \mathbb{K}[Y]$. Let us define $\varphi^*(f) := f \circ \varphi$. Since we have that f is a polynomial function of Y, when we compose with the polynomial map φ we get back a polynomial function of X. That is there exists a map

$$\varphi^*: \mathbb{K}[Y] \longrightarrow \mathbb{K}[X]$$

$$f \longmapsto \varphi^*(f) = f \circ \varphi.$$

We will show this map is actually a $\mathbb{K}$-algebra homomorphism. We first show it is well-defined. Assume $\hat{f} = \hat{g}$ in $\mathbb{K}[Y]$. Then $f - g \in \mathcal{I}_{\mathbb{K}}(Y)$, which means $f(\underline{b}) = g(\underline{b})$ for all $\underline{b} \in Y \subseteq \mathbb{A}^m_{\mathbb{K}}$. In particular we have $f(\varphi(\underline{a})) = g(\varphi(\underline{a}))$ for all $\underline{a} \in X$, since $\varphi(\underline{a}) \in Y$ for all $\underline{a} \in X$. Thus, $f \circ \varphi - g \circ \varphi \in \mathcal{I}_{\mathbb{K}}(Y)$, i.e., $\varphi^*(f) = \varphi^*(g)$, proving that φ^* is well-defined. Consider now

$$\varphi^*(f + g) = (f + g) \circ \varphi = f \circ \varphi + g \circ \varphi = \varphi^*(f) + \varphi^*(g)$$

and

$$\varphi^*(f \cdot g) = (f \cdot g) \circ \varphi = f \circ \varphi \cdot g \circ \varphi = \varphi^*(f) \cdot \varphi^*(g).$$

Finally, $\varphi^*(k) = k \circ \varphi = k$ for all $k \in \mathbb{K}$, which proves that φ^* is in fact a $\mathbb{K}$-algebra homomorphism. Thus, a polynomial map φ induces a $\mathbb{K}$-algebra homomorphism φ^*.

Proposition 2.1.13. The map $\chi: Poly(X, Y) \longrightarrow Hom_{\mathbb{K}-alg}(\mathbb{K}[Y], \mathbb{K}[X])$ where $\varphi \longmapsto \varphi^*$ is a bijection.

Proof. We show for a $\mathbb{K}$-algebra homomorphism $\mu: \mathbb{K}[Y] \longrightarrow \mathbb{K}[X]$, there exists a polynomial map $\varphi: X \longrightarrow Y$ such that $\varphi^* = \mu$. Consider the coordinate ring $\mathbb{K}[Y] = \mathbb{K}[\overline{y_1}, \overline{y_2}, \ldots, \overline{y_m}]$ where $\overline{y_i} = y_i + \mathcal{I}_{\mathbb{K}}(Y)$. Let $f_i = \mu(\overline{y_i}) \in \mathbb{K}[X]$, then $\varphi = (f_1, f_2, \ldots, f_m)$ is a polynomial map from X to $\mathbb{A}^m_{\mathbb{K}}$. We show the image of φ is contained in Y. Let $g = g(y_1, y_2, \ldots, y_m) \in \mathcal{I}_{\mathbb{K}}(Y)$, then $\overline{g(y_1, y_2, \ldots, y_m)} = g(\overline{y_1}, \overline{y_2}, \ldots, \overline{y_m}) = 0$ in $\mathbb{K}[Y]$. We also have $\mu(g(\overline{y_1}, \overline{y_2}, \ldots, \overline{y_m}) = 0$ since zero maps to zero under a homomorphism. Also,

$$0 = \mu(g(\overline{y_1}, \overline{y_2}, \ldots, \overline{y_m}) = g(\mu(\overline{y_1}), \mu(\overline{y_2}), \ldots, \mu(\overline{y_m})) = g(f_1, f_2, \ldots, f_m),$$

since μ is a $\mathbb{K}$-algebra homomorphism. Thus, $g(f_1, f_2, \ldots, f_m) \in \mathcal{I}_{\mathbb{K}}(X)$, which by definition implies $g(f_1(x), f_2(x), \ldots, f_m(x)) = g(\varphi(x)) = 0$ for all $x \in X$. Since g was chosen arbitrarily from $\mathcal{I}_{\mathbb{K}}(Y)$, we have shown that every element of $\mathcal{I}_{\mathbb{K}}(Y)$ vanishes at $\varphi(x)$ for all $x \in X$. Thus we must have $\varphi(X) \subseteq Y$. Notice the $\overline{y_i}$ generate $\mathbb{K}[Y]$ and $\mu(\overline{y_i}) = \overline{y_i} \circ \varphi = \varphi^*(\overline{y_i}) = f_i$ by definition of f_i. Therefore $\varphi^* = \mu$.

Let $\varphi = (f_1, f_2, \ldots, f_m)$ and $\psi = (g_1, g_2, \ldots, g_m)$ be two polynomial maps from $X \longrightarrow Y$, where $f_i, g_i \in \mathbb{K}[X]$ and $\varphi^* = \psi^*$. Then we must have $y_i \circ \varphi = \varphi^*(\overline{y_i}) = \psi^*(\overline{y_i}) = y_i \circ \psi$. We then apply this equality to points of X to get $f_i(x) = (y_i \circ \varphi)(x) = (y_i \circ \psi)(x) = g_i(x)$ for all $x \in X$. However, this implies $\varphi(x) = \psi(x)$ for all $x \in X$. Therefore we have $\varphi = \psi$, proving injectivity. □

Definition 2.1.14. A polynomial map $\varphi: X \longrightarrow Y$ is an isomorphism if there is a polynomial map $\phi: Y \longrightarrow X$ such that $\varphi \circ \phi = id_Y$ and $\phi \circ \varphi = id_X$.

Corollary 2.1.15 ([5], Proposition 1.48). A polynomial map $\varphi: X \longrightarrow Y$ is an isomorphism of affine algebraic sets if and only if $\varphi^*: \mathbb{K}[Y] \longrightarrow \mathbb{K}[X]$ is an isomorphism of $\mathbb{K}$-algebras.

2.2 Zariski Topologies

We define an extension of the Zariski topology over $\mathbb{K}$, known as the $\mathbb{K}$-*Zariski topology*. We still let ideals from $\mathbb{K}[\underline{x}]$ define closed sets; however, we consider these closed sets as subsets of $\mathbb{A}^n_{\overline{\mathbb{K}}}$ rather than $\mathbb{A}^n_{\mathbb{K}}$.

Definition 2.2.1. The $\mathbb{K}$-*Zariski topology* of $\mathbb{A}^n_{\overline{\mathbb{K}}}$ is defined by taking the closed sets to be $\mathcal{Z}_{\overline{\mathbb{K}}}(J)$ where $J \leq \mathbb{K}[\underline{x}]$. The collection of all closed sets in the $\mathbb{K}$-Zariski topology is denoted by $\mathbb{K}$-$\mathfrak{Z}_{\overline{\mathbb{K}}}$.

Just as in the Zariski topology, we have the topological notion of closure, known as the $\mathbb{K}$-*closure*.

Definition 2.2.2. Consider a subset $W \subseteqq \overline{\mathbb{K}}^n$. Then the $\mathbb{K}$-*closure* is in intersection of all the closed sets in the $\mathbb{K}$-Zariski topology containing W. We will denote this closure with the usual notation, $\overline{W}$. It will be clear from context which closure we are referring to.

Proposition 2.2.3. Let $W \subseteqq \overline{\mathbb{K}}^n$ be an arbitrary subset and $\overline{W}$ be the $\mathbb{K}$-closure of W under the $\mathbb{K}$-Zariski topology. Then,

$$\overline{W} = \mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(W)).$$

Proof. Since $W \subseteqq \mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(W)) \Rightarrow \overline{W} \subseteqq \mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(W))$. For the reverse inclusion, we have $W \subseteqq \overline{W}$. Then after applying $\mathcal{I}_{\mathbb{K}}$ and $\mathcal{Z}_{\overline{\mathbb{K}}}$ we get, $\mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(W)) \subseteqq \mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(\overline{W}))$. Since $\overline{W}$ is closed in the $\mathbb{K}$-Zariski topology, there exists an ideal $J \leq \mathbb{K}[\underline{x}]$ such that $\mathcal{Z}_{\overline{\mathbb{K}}}(J) = \overline{W}$. Therefore, $\mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(W)) \subseteqq \mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(\overline{W})) = \mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)))$. By Theorem 1.7.7 we have that $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)) = \sqrt{J}$. Thus $\mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(W)) \subseteqq \mathcal{Z}_{\overline{\mathbb{K}}}(\sqrt{J}) = \mathcal{Z}_{\overline{\mathbb{K}}}(J) = W$ by Proposition 1.4.9(ii). $\square$

Similarly, we may define the "closure", known as the $\mathbb{K}$-*radical*, of a subset $T \subseteqq \mathbb{K}[\underline{x}]$.

Definition 2.2.4. Let $T \subseteqq \mathbb{K}[\underline{x}]$. Then the $\mathbb{K}$-*radical* of T is the sum of all ideals from $\mathbb{K}[\underline{x}]$ that define the algebraic set, $\mathcal{Z}_{\mathbb{K}}(T)$, denoted $\sqrt[\mathbb{K}]{T}$.

Notice that T defines $\mathcal{Z}_{\mathbb{K}}(T)$, so the sum is not empty. Also the sum of all ideals that define $\mathcal{Z}_{\mathbb{K}}(T)$ is necessarily an upper-bound on this set of ideals. Hence, $\sqrt[\mathbb{K}]{T}$ is the largest ideal that defines $\mathcal{Z}_{\mathbb{K}}(T)$.

Proposition 2.2.5. Let $T \subseteq \mathbb{K}[\underline{x}]$, then the $\mathbb{K}$-radical of T is the vanishing ideal of $\mathcal{Z}_{\mathbb{K}}(T)$:

$$\sqrt[\mathbb{K}]{T} = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(T))$$

.

Proof. By definition of $\mathcal{I}_{\mathbb{K}}$, for all ideals $J \leq \mathbb{K}[\underline{x}]$ such that $\mathcal{Z}_{\mathbb{K}}(J) = \mathcal{Z}_{\mathbb{K}}(T)$ we must have $J \subseteq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(T))$. In particular we have $\sqrt[\mathbb{K}]{T} \subseteq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(T))$. However, by definition of $\sqrt[\mathbb{K}]{T}$ we must also have $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(T)) \subseteq \sqrt[\mathbb{K}]{T}$. □

Definition 2.2.6. We say an ideal $J \subseteq \mathbb{K}[\underline{x}]$ is $\mathbb{K}$-radical if and only if

$$J = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J)) = \sqrt[\mathbb{K}]{J}.$$

Let us recall we defined the Zariski topology over a field $\mathbb{K}$ to be the collection of all closed sets V such that $V = \mathcal{Z}_{\mathbb{K}}(J) \subseteq \mathbb{A}^n_{\mathbb{K}}$ for some $J \leq \mathbb{K}[\underline{x}]$, denoted by $\mathfrak{Z}_{\mathbb{K}}$. Additionally, for any subset $X \subseteq \mathbb{A}^n_{\mathbb{K}}$, we may consider the induced Zariski topology to be the collection of all closed sets V_X where the closed sets are $V_X := \mathcal{Z}_{\mathbb{K}}(J) \cap X$ for some $J \leq \mathbb{K}[\underline{x}]$, denoted by $\mathfrak{Z}_{\mathbb{K}} \restriction_X$. Now let $\overline{\mathbb{K}}$ be the algebraic closure of the field $\mathbb{K}$, and we may therefore consider the induced topology of $\mathbb{K}^n = \mathbb{A}^n_{\mathbb{K}}$ from $\mathfrak{Z}_{\overline{\mathbb{K}}}$, with the collection of closed sets denoted as $\mathfrak{Z}_{\overline{\mathbb{K}}} \restriction_{\mathbb{K}}$. Lastly, we consider the induced topology of $\mathbb{K}^n = \mathbb{A}^n_{\mathbb{K}}$ from the $\mathbb{K}$-Zariski topology, where the collection of closed sets in the induced topology is denoted as $\mathbb{K}$-$\mathfrak{Z}_{\overline{\mathbb{K}}} \restriction_{\mathbb{K}}$. Therefore we have three topologies for $\mathbb{A}^n_{\mathbb{K}}$; namely, $\mathfrak{Z}_{\mathbb{K}}$, $\mathfrak{Z}_{\overline{\mathbb{K}}} \restriction_{\mathbb{K}}$, and $\mathbb{K}$-$\mathfrak{Z}_{\overline{\mathbb{K}}} \restriction_{\mathbb{K}}$. We first show $\mathbb{K}$-$\mathfrak{Z}_{\overline{\mathbb{K}}} \restriction_{\mathbb{K}} = \mathfrak{Z}_{\mathbb{K}}$, which follows from Observation 2.2.7.

Observation 2.2.7. For all ideals $J \leq \mathbb{K}[\underline{x}]$,

$$\mathcal{Z}_{\overline{\mathbb{K}}}(J\overline{\mathbb{K}}[\underline{x}]) \cap \mathbb{K}^n = \mathcal{Z}_{\mathbb{K}}(J).$$

Proof. In general, $\mathcal{Z}_{\mathbb{K}}(J) \subseteq \mathcal{Z}_{\overline{\mathbb{K}}}(J\overline{\mathbb{K}}[\underline{x}])$ for $J \leq \mathbb{K}[\underline{x}]$. If we now intersect with $\mathbb{K}^n$, $\mathcal{Z}_{\mathbb{K}}(J) \subseteq \mathcal{Z}_{\overline{\mathbb{K}}}(J\overline{\mathbb{K}}[\underline{x}]) \cap \mathbb{K}^n$, which proves the reverse containment. Assume now $\underline{a} \in \mathcal{Z}_{\overline{\mathbb{K}}}(J\overline{\mathbb{K}}[\underline{x}]) \cap \mathbb{K}^n$. Then $\underline{a} \in \mathcal{Z}_{\overline{\mathbb{K}}}(J\overline{\mathbb{K}}[\underline{x}])$, and $\underline{a} \in \mathbb{K}^n$. Therefore, $f(\underline{a}) = 0$ for all $f \in J\overline{\mathbb{K}}[\underline{x}]$ and $\underline{a} \in \mathbb{K}^n$. Since J generates $J\overline{\mathbb{K}}[\underline{x}]$ we must also have $f(\underline{a}) = 0$ for all $f \in J$. By definition $\underline{a} \in \mathcal{Z}_{\mathbb{K}}(J)$, proving the forward

containment. □

Observation 2.2.8. For all algebraic sets $V = \mathcal{Z}_{\overline{\mathbb{K}}}(J)$ for some ideal $J \leq \mathbb{K}[\underline{x}]$,

$$\mathcal{I}_{\overline{\mathbb{K}}}(V) \cap \mathbb{K}[\underline{x}] = \mathcal{I}_{\mathbb{K}}(V).$$

Proof. We have that $\mathcal{I}_{\overline{\mathbb{K}}}(V) \cap \mathbb{K}[\underline{x}] = \mathcal{I}_{\overline{\mathbb{K}}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)) \cap \mathbb{K}[\underline{x}] = \sqrt{J\overline{\mathbb{K}}[\underline{x}]} \cap \mathbb{K}[\underline{x}] = \sqrt{J\overline{\mathbb{K}}[\underline{x}] \cap \mathbb{K}[\underline{x}]} = \sqrt{J}$, by the Theorem 1.7.5 and Lemma 1.2.5. Similarly the right side, $\mathcal{I}_{\mathbb{K}}(V) = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)) = \sqrt{J}$, by Theorem 1.7.7. Hence, we have equality. □

Proposition 2.2.9. [[7], Proposition 3.5] Let X be a topological space and let Y be a subspace of X. Then if Y is irreducible so is its closure $\overline{Y}$.

Proof. If $\overline{Y} = F_1 \cup F_2$, where F_i is a closed set of $\overline{Y}$ and is hence a closed set of X. Then $Y = (F_1 \cap Y) \cup (F_2 \cap Y)$, and hence since Y is irreducible , $Y = F_i \cap Y$, or, alternatively, $Y \subset F_i$. But we then have $\overline{Y} \subset F_i$, and hence $\overline{Y} = F_i$. □

Corollary 2.2.10. Let $V \in \mathfrak{Z}_{\mathbb{K}}$. If V is irreducible then $\overline{V} \in \mathbb{K}\text{-}\mathfrak{Z}_{\overline{\mathbb{K}}}$ is irreducible.

Proof. This follows directly from Observation 2.2.7. and Proposition 2.2.9. □

Proposition 2.2.11 ([8], Proposition 1.3). Let $J \subseteqq \mathbb{K}[\underline{x}]$. The following assertions are equivalent:

- J is $\mathbb{K}$-radical
- $\mathcal{Z}_{\mathbb{K}}(J) \in \mathfrak{Z}_{\mathbb{K}}$ is dense under the $\mathbb{K}$-closure in $\mathcal{Z}_{\overline{\mathbb{K}}}(J) \in \mathbb{K}\text{-}\mathfrak{Z}_{\overline{\mathbb{K}}}$ and J is radical.

Proof. Assume J is $\mathbb{K}$-radical. Then $J = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))$. Apply $\mathcal{Z}_{\overline{\mathbb{K}}}$ to both sides to get $\mathcal{Z}_{\overline{\mathbb{K}}}(J) = \mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J)) = \overline{\mathcal{Z}_{\mathbb{K}}(J)}$. We also have that J is a radical ideal because it is equal to $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))$. For the converse, let $\mathcal{Z}_{\mathbb{K}}(J)$ be dense in $\mathcal{Z}_{\overline{\mathbb{K}}}(J)$ with $\sqrt{J} = J$, so by definition of dense in $\mathbb{K}\text{-}\mathfrak{Z}_{\mathbb{K}}$, we have $\mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J)) = \mathcal{Z}_{\overline{\mathbb{K}}}(J)$. Take $\mathcal{I}_{\mathbb{K}}$ of both sides to get $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))) = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J))$. However by Theorem 1.7.7 the left side $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))) = \sqrt{\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))} = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))$, and the right side $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\overline{\mathbb{K}}}(J)) = \sqrt{J} = J$. Hence $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J)) = J$, so J is $\mathbb{K}$-radical. □

Proposition 2.2.12 ([8], Proposition 1.3). For an ideal $J \leq \mathbb{K}[\underline{x}]$, $\mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J)) = \sqrt[\mathbb{K}]{J}$ is the intersection of all $\mathbb{K}$-radical prime ideals containing J.

Proof. Suppose P is a $\mathbb{K}$-radical prime containing J. After applying $\mathcal{Z}_{\mathbb{K}}$ then $\mathcal{I}_{\mathbb{K}}$, we get

$$\sqrt[\mathbb{K}]{J} \subseteqq \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(P)) = P.$$

For the reverse containment, suppose $f \notin \sqrt[\mathbb{K}]{J}$. Then f^n is not in $\sqrt[\mathbb{K}]{J}$ for any n because $\sqrt[\mathbb{K}]{J}$ is a radical ideal. We may now consider the set Λ of all ideals $I \leq \mathbb{K}[\underline{x}]$ such that

$$\{f^n\} \cap I = \varnothing \text{ for any } n \in \mathbb{N}.$$

We know $\sqrt[\mathbb{K}]{J} \in \Lambda$, hence is non-empty, and that the ideals in Λ are partially ordered by inclusion. Consider a chain of ideals $\{I_\lambda\}_{\lambda \in \Lambda}$ and consider their union $\bigcup_{\lambda \in \Lambda} I_\lambda$. It is easily verified that $\bigcup_{\lambda \in \Lambda} I_\lambda$ is an ideal and necessarily an upper bound. We have $\bigcup_{\lambda \in \Lambda} I_\lambda \in \Lambda$ as well since each $I_\lambda \in \Lambda$. Therefore, by Zorn's Lemma There exists a maximal element P of Λ. Notice P is a proper ideal, we show P is prime. Let $xy \in P$ and assume P is not prime. Then $\langle P, x\rangle$ and $\langle P, y\rangle$ are strictly larger than P. Hence, $f^n \in \langle P, x\rangle$ and $f^m \in \langle P, y\rangle$ for some $n, m \in \mathbb{N}$. Then

$$f^n = r_1 x + p_1 \text{ and } f^m = r_2 y + p_2$$

where $r_1, r_2 \in \mathbb{K}[\underline{x}]$ and $p_1, p_2 \in P$. We now have

$$f^{n+m} = r_1 r_2 xy + r_1 x p_2 + r_2 y p_1 + p_1 p_2.$$

The right side is in P, but this implies a power of f is in P, contradicting $P \in \Lambda$. Therefore, $x \in P$ or $y \in P$, concluding that P is prime by definition. We now show that P is $\mathbb{K}$-radical. Assume not, then $\sqrt[\mathbb{K}]{P}$ is strictly larger than P. Hence, $\sqrt[\mathbb{K}]{P}$ contains a power of f, which implies $f \in \sqrt[\mathbb{K}]{P}$ since $\sqrt[\mathbb{K}]{P}$ is radical by Proposition 1.4.9(ii). Now apply $\mathcal{Z}_{\mathbb{K}}$ to get $\mathcal{Z}_{\mathbb{K}}(\sqrt[\mathbb{K}]{P}) = \mathcal{Z}_{\mathbb{K}}(P) \subseteqq \mathcal{Z}_{\mathbb{K}}(f)$. Once again this contradicts that fact that $f \notin P \Rightarrow \mathcal{Z}_{\mathbb{K}}(P) \nsubseteqq \mathcal{Z}_{\mathbb{K}}(f)$. Therefore P is a $\mathbb{K}$-radical prime not containing f, concluding the proof. $\square$

We now give a correspondence between $\mathbb{K}$-radical ideals and affine algebraic sets in $\mathbb{A}^n_{\mathbb{K}}$.

Proposition 2.2.13. There is a one to one correspondence between affine algebraic sets in the

Zariski topology defined over $\mathbb{K}$ and $\mathbb{K}$-radical ideals of $\mathbb{K}[\underline{x}]$.

Proof. Let W be an algebraic set. Then there must exist an ideal $I \leq \mathbb{K}[\underline{x}]$ such that $\mathcal{Z}_{\mathbb{K}}(I) = W$. If we now consider the $\mathbb{K}$-radical of I, we have $\mathcal{Z}_{\mathbb{K}}(I) = \mathcal{Z}_{\mathbb{K}}(\sqrt[\mathbb{K}]{I})$. Thus, every algebraic set is described by a $\mathbb{K}$-radical ideal. It is obvious every $\mathbb{K}$-radical ideal defines an algebraic set of $\mathbb{A}^n_{\mathbb{K}}$. □

Proposition 2.2.14. There is a one to one correspondence between irreducible affine algebraic sets in $\mathbb{A}^n_{\mathbb{K}}$ and $\mathbb{K}$-radical prime ideals in $\mathbb{K}[\underline{x}]$.

Proof. Let V be an irreducible affine algebraic set in $\mathbb{A}^n_{\mathbb{K}}$. Then there must exist an ideal $J \leq \mathbb{K}[\underline{x}]$ such that $\mathcal{Z}_{\mathbb{K}}(J) = V$. Now consider the $\mathbb{K}$-radical of J, $\sqrt[\mathbb{K}]{J}$. We have $\sqrt[\mathbb{K}]{J} = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(J))$ by Proposition 2.2.5, which implies $\sqrt[\mathbb{K}]{J}$ is prime by Proposition 1.5.7. Hence, V is described by a $\mathbb{K}$-radical prime ideal. For any $\mathbb{K}$-radical prime ideal $P = \sqrt[\mathbb{K}]{P} = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(P))$, we have that $\mathcal{Z}_{\mathbb{K}}(P)$ is irreducible by Proposition 1.5.7. □

In other words, for all $\mathbb{K}$-radical ideals J of $\mathbb{K}[\underline{x}]$,

$$\mathcal{Z}_{\mathbb{K}}(J) \text{ is irreducible} \Leftrightarrow J \text{ is a prime ideal of } \mathbb{K}[\underline{x}],$$

which resolves our discrepancy discussed in Section 1.6.

2.3 Dimension

Throughout this section, we assume $\mathbb{K}$ is an infinite field.

Definition 2.3.1. Let X be a topological space. Then the *dimension* of X is the maximum of the lengths of chains of distinct irreducible closed sets of X, denoted $\dim(X)$.

Definition 2.3.2. Let R be a $\mathbb{K}$-algebra. The *Krull dimension* of R is the maximum of the lengths of chains of distinct prime ideals of R, denoted $\dim_{\mathbb{K}}(R)$.

Definition 2.3.3. We call an irreducible algebraic set $V \subseteq \mathbb{A}^n_{\mathbb{K}}$ a *curve* if $\dim(V) = 1$ in the Zariski topology defined over $\mathbb{K}$, $\mathfrak{Z}_{\mathbb{K}}$.

Definition 2.3.4. We call an irreducible algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ a *surface* if $\dim(V) = 2$ in the Zariski topology defined over $\mathbb{K}$, $\mathfrak{Z}_{\mathbb{K}}$.

Proposition 2.3.5. [[7], Proposition 1.3] Let X be a topological space and Y a subspace of X. Then $\dim(Y) \leq \dim(X)$

Proof. Let $F_1 \subsetneqq \ldots \subsetneqq F_n$ be a chain of closed irreducible subsets of Y. There is then a sequence $\overline{F_1} \subsetneqq \ldots \subsetneqq \overline{F_n}$ of closed irreducible subsets of X. These closed sets are distinct since, for every $i, F_i = \overline{F_i} \cap Y$, since the sets F_i are closed in Y. □

Proposition 2.3.6. [[7], Proposition 1.4] Let X be topological space. Assume $X = \bigcup_{i=1}^n X_i$ where the sets X_i are closed. Then $\dim(X)$=sup $\dim X_i$.

Proof. From Proposition 2.3.5 we clearly have $\dim(X) \geq$ sup $\dim(X_i)$. Conversely, let p be the sup in question. If p is infinite, the theorem is trivial. Assume not and take a chain in X of length $p+1$,

$$F_1 \subsetneqq \ldots \subsetneqq F_{p+1}.$$

Then $F_{p+1} = \bigcup_{i=1}^n (X_i \cap F_{p+1})$, but since F_{p+1} is irreducible, it is included in one of the sets X_i, which contradicts $\dim(X_i) \leq p$. □

Observation 2.3.7. Let $\mathbb{K} = \overline{\mathbb{K}}$ be an algebraically closed field and let $V \subseteqq \mathbb{A}^n_{\overline{\mathbb{K}}}$ be an algebraic set in the Zariski topology over $\overline{\mathbb{K}}$. Then,

$$\dim_{\mathbb{K}}(\mathbb{K}[V]) = \dim(V).$$

This is due to the bijective correspondence between the prime ideals in $\overline{\mathbb{K}}[V]$ and the irreducible affine algebraic subsets of V given by Theorem 1.7.6. Hence, a natural question arises:

Question 2.3.8. Is $\dim_{\mathbb{K}}(\mathbb{K}[V])$=$\dim(V)$, for an affine algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ in the Zariski topology defined over $\mathbb{K}$?

Consider an algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$. By Proposition 1.5.11, we have that

$$V = V_1 \cup V_2 \cup \ldots \cup V_n$$

where V_i are irreducible affine algebraic subsets of V. By Proposition 2.3.6, we have $\dim(V)$=sup $\dim(V_i)$. Hence, we may restrict ourselves to the case where V is an irreducible affine algebraic set of $\mathbb{A}^n_{\mathbb{K}}$. We rephrase our question:

Question 2.3.9. Is $\dim_{\mathbb{K}}(\mathbb{K}[V])$=$\dim(V)$, for an irreducible affine algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ in the Zariski topology defined over $\mathbb{K}$?

Remark 2.3.10. An affine algebraic set V of dimension 0 is finite. Consider the decomposition into irreducible components by Proposition 1.5.11, $V = V_1 \cup V_2 \cup \ldots \cup V_m$ for some $m \in \mathbb{N}$. We then have that the V_i are irreducible and also must be of dimension 0. Thus each V_i must be a point and we only have finitely many of them.

We now discuss results pertaining to Question 2.3.9.

(i) We already know from Chapter 1 that the ideal of an irreducible affine algebraic set is always prime. Consider an algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$ such that $\dim(V)$=m. Then there must exist a chain of irreducible affine algebraic sets contained in V,

$$\varnothing \neq V_0 \subsetneqq V_1 \subsetneqq \ldots \subsetneqq V_m \subseteqq V, \text{ where the } V_i \text{ are irreducible.}$$

If we now apply $\mathcal{I}_{\mathbb{K}}$ to this chain we will get another chain,

$$\mathcal{I}_{\mathbb{K}}(V) \subseteqq \mathcal{I}_{\mathbb{K}}(V_n) \subsetneqq \mathcal{I}_{\mathbb{K}}(V_{n-1}) \subsetneqq \ldots \subsetneqq \mathcal{I}_{\mathbb{K}}(V_0).$$

The inclusions are strict and each ideal is prime by Remark 1.4.8 and Proposition 1.5.7, respectively. Hence we have just shown the following:

Observation 2.3.11. $\dim_{\mathbb{K}}(\mathbb{K}[V]) \geq \dim(V)$, for an algebraic set $V \subseteqq \mathbb{A}^n_{\mathbb{K}}$.

(ii)

Lemma 2.3.12. The affine space $\mathbb{A}^n_{\mathbb{K}}$ is of dimension n in the Zariski topology defined over $\mathbb{K}$.

Proof. We obviously have

$$\mathbb{A}^0_{\mathbb{K}} \subsetneqq \mathbb{A}_{\mathbb{K}} \subsetneqq \mathbb{A}^2_{\mathbb{K}} \subsetneqq \ldots \subsetneqq \mathbb{A}^n_{\mathbb{K}}$$

as a chain of distinct irreducible algebraic sets. Thus $\dim(\mathbb{A}^n_{\mathbb{K}}) \geq n$. Consider now that coordinate ring of $\mathbb{A}^n_{\mathbb{K}}$, $\mathbb{K}[\mathbb{A}^n_{\mathbb{K}}] = \mathbb{K}[x_1, x_2, \ldots, x_n]$. We have that $\dim_{\mathbb{K}}(\mathbb{K}[x_1, x_2, \ldots, x_n]) = n$ by Theorem 1.2.13, since its field of fractions is $\mathbb{K}(x_1, x_2, \ldots, x_n)$, whose transcendence degree over $\mathbb{K}$ is n. From Observation 2.3.3., we have $\dim(\mathbb{A}^n_{\mathbb{K}}) \leq \dim_{\mathbb{K}}(\mathbb{K}[x_1, x_2, \ldots, x_n]) = n$, concluding $\dim(\mathbb{A}^n_{\mathbb{K}}) = n$. □

Observation 2.3.13. $\dim_{\mathbb{K}}(\mathbb{K}[\mathbb{A}^n_{\mathbb{K}}]) = \dim(\mathbb{A}^n_{\mathbb{K}})$.

(iii) Consider now a point $\underline{a} \in \mathbb{A}^n_{\mathbb{K}}$. The vanishing ideal $\mathcal{I}_{\mathbb{K}}(\underline{a})$ is be maximal by Theorem 1.7.3. Thus $\mathbb{K}[\{\underline{a}\}] = \mathbb{K}[\underline{x}]/\mathcal{I}_{\mathbb{K}}(\underline{a}) = \mathbb{K}$, which has dimension zero over $\mathbb{K}$. Thus, every point of $\mathbb{A}^n_{\mathbb{K}}$ is of dimension zero.

Observation 2.3.14. $\dim_{\mathbb{K}}(\mathbb{K}[\{\underline{a}\}]) = \dim_{\mathbb{K}}(\mathbb{K}) = 0 = \dim(\{\underline{a}\})$.

We now consider each affine space separately.

(i) In $\mathbb{A}_{\mathbb{K}}$, an irreducible set is either the whole space or a point. From our previous Observations we have

$$\dim_{\mathbb{K}}(\mathbb{K}[V]) = \dim(V)$$

for all algebraic sets $V \subseteqq \mathbb{A}_{\mathbb{K}}$.

(ii) We consider now $\mathbb{A}^2_{\mathbb{K}}$. Once again by the previous Observations, we need only consider the irreducible algebraic sets V such that $V \neq \mathbb{A}^2_{\mathbb{K}}$ and V is not a point of $\mathbb{A}^2_{\mathbb{K}}$. Since V is not a point but irreducible, we have a chain

$$\{v_0\} \subsetneqq V,$$

where v_0 is a point on V, which implies $\dim(V) \geq 1$. Similarly, $\dim(V) \leq 1$, otherwise we contradict the fact that $\dim(\mathbb{A}^2_{\mathbb{K}}) = 2$. Therefore, $\dim(V) = 1$, i.e., V is a curve of $\mathbb{A}^2_{\mathbb{K}}$.

Assume now the coordinate ring of V is of dimension 2, $\dim_{\mathbb{K}}(\mathbb{K}[V]) = 2$. This implies $\mathcal{I}_{\mathbb{K}}(V)$ has height zero in $\mathbb{K}[x_1, x_2]$. Therefore, $\mathcal{I}_{\mathbb{K}}(V)$ is a minimal prime of $\mathbb{K}[x_1, x_2]$, but the only minimal prime ideal of $\mathbb{K}[x_1, x_2]$ is the zero ideal. Therefore, $\mathcal{I}_{\mathbb{K}}(V) = 0$, but this implies

$V = \mathbb{A}^2_{\mathbb{K}}$, which contradicts that V is of dimension one. Hence, we must have the coordinate ring of V to be of dimension 1. We may now conclude that for every affine algebraic set V of $\mathbb{A}^2_{\mathbb{K}}$,

$$\dim_{\mathbb{K}}(\mathbb{K}[V]) = \dim(V).$$

(iii) We now consider the space $\mathbb{A}^3_{\mathbb{K}}$. Let V be an algebraic set such that $V \neq \mathbb{A}^3_{\mathbb{K}}$ and V is not a point of $\mathbb{A}^3_{\mathbb{K}}$. So, we examine the two cases: $\dim(V) = 1$ and $\dim(V) = 2$.

Let $\dim(V) = 2$, and assume $\dim_{\mathbb{K}}(\mathbb{K}[V]) = 3$. By the same argument in the previous case, we must have $\mathcal{I}_{\mathbb{K}}(V) = 0$, which implies $V = \mathbb{A}^3_{\mathbb{K}}$, which contradicts our hypotheses on V. We may conclude that $\dim_{\mathbb{K}}(\mathbb{K}[V]) = 2$ as well.

We now examine the case when $\dim(V) = 1$. We assume $\dim_{\mathbb{K}}(\mathbb{K}[V]) = 2$. Since $\dim_{\mathbb{K}}(\mathbb{K}[V]) = 2$, we have that $\mathcal{I}_{\mathbb{K}}(V)$ must be of height one, i.e., $\mathcal{I}_{\mathbb{K}}(V)$ is principal. Thus, $\mathcal{I}_{\mathbb{K}}(V) = \langle f \rangle$ for some $f \in \mathbb{K}[x_1, x_2, x_3]$. Take $\mathcal{Z}_{\mathbb{K}}$ of both sides to get, $\mathcal{Z}_{\mathbb{K}}(f) = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_{\mathbb{K}}(V)) = V$, where the last equality follows from Proposition 1.4.7(ii). Since $\dim(V) = 1$, must have infinitely many solutions in $\mathbb{A}^3_{\mathbb{K}}$. Therefore any proper algebraic set contained in V must be of dimension 0, i.e., finite. Algebraically this implies that for all polynomials g such that $g \notin \langle f \rangle$, we must have $\mathcal{Z}_{\mathbb{K}}(f, g)$ to be finite. This motivates the following question:

Question 2.3.15. Does there exist a polynomial $f \in \mathbb{K}[x_1, x_2, x_3]$ with $\mathcal{Z}_{\mathbb{K}}(f)$ an infinite set of points such that for all polynomials $g \in \mathbb{K}[x_1, x_2, x_3]$ with $g \notin \langle f \rangle$, $\mathcal{Z}_{\mathbb{K}}(g, f)$ is a finite set of points from $\mathbb{A}^3_{\mathbb{K}}$?

Finding such an f would give a counterexample to Question 2.3.9. I believe there is counterexample and that Question 2.3.9. has a negative answer; however, I have yet to be able to prove either. We now give a relation of dimension that relates the K-radical.

Definition 2.3.16. Let R be a $\mathbb{K}$-algebra. The $\mathbb{K}$-*radical dimension* of R is the maximum of the lengths of chains of distinct $\mathbb{K}$- radical prime ideals of R, denoted $\dim_{\mathbb{K}-\mathrm{rad}}(R)$.

Corollary 2.3.17. Let V be an algebraic set of $\mathbb{A}^n_{\mathbb{K}}$. Then $\dim_{\mathbb{K}-\mathrm{rad}}(\mathbb{K}[V])$=$\dim(V)$

Proof. This is a consequence of Proposition 2.2.14. □

REFERENCES

[1] D. Burton, *Elementary Number Theory*, McGraw-Hill, 1998.

[2] D. Dummit and R. Foote *Abstract Algebra* Wiley, 2004.

[3] S. Gao, *Counting Zeros Over Finite Fields Using Grobner Bases*, MS Thesis in Logic and Computation, 2009.

[4] A. Gathmann, *Algebraic Geometry*, Class notes at the University of Kaiserslautern, 2003.

[5] K. Hulek, *Elementary Algebraic Geometry*, Student Mathematical Library, Vol. 20, American Mathematical Society 2003.

[6] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1989.

[7] D. Perrin, *Algebraic Geometry: An Introduction*, Springer-Verlag, 2008.

[8] T. Sander, *Aspects of Algebraic Geometry over Non Algebraically Closed Fields*, International Computer Science Institute.

[9] R. Y. Sharp, *Steps in Commutative Algebra*, Cambridge University Press, 2000.

[10] K. Ueno, *Algebraic Geometry 1: From Algebraic Varieties to Schemes*, Translations of Mathematical Monographs, Vol. 185, American Mathematical Society, 1999.