ADDIS ABABA UNIVERSITY

School of Graduate Studies

Department of Mathematics

Graduate Seminar Report

ON

THE IDEAL-VARIETY CORRESPONDENCE

(Submitted in partial fulfillment of M.Sc Degree in Mathematics)

By: EYERUSALEM W/YOHANNES

June, 2010

Addis Ababa

SCIENCE LIBRARY

Acknowledgment

First of all, I would like to thank the almighty God with his mother the Holy Virgin St.Mary.
I would also like to thank my advisor Dr.Tilahun Abebaw for his stimulating and enthusiastic collaboration, comments, suggestions and improvements.

Eyerusalem W/yohannes

PAGE

INTRODUCTION:

This chapter will introduce some of the basic themes of the paper. The geometry we are interested in concerns affine varieties, which are curves and surfaces (and higher dimensional objects) defined by polynomial equations. To understand affine varieties, we will need some algebra, and in particular, we will need to study ideals in the polynomial ring $\mathbf{K}[x_1, x_2 \ldots x_n]$. The basic geometric object of the paper is affine variety and the basic algebraic object is ideal. To link algebra and geometry, we will study polynomials over a field. We are familiar with polynomials in one and two variables, but we will need to discuss polynomials in n variables $x_1,...,x_n$ with coefficients in an arbitrary field K.

In the second chapter, we will need to solve two problems. The questions are:

- **(Ideal description)**: Can every ideal $I \subseteq K[x_1,...,x_n]$ be written as $< f_1, f_2,..., f_s >$ for some $f_1,..., f_s \in K[x_1,...,x_n]$?
- **(Nullstellensatz)**: Given $f_1,..., f_s \in K[x_1,...,x_n]$, what is the exact relation between $< f_1, f_2,..., f_s >$ and $I(V(f_1, f_2,..., f_s))$?

The original German name **Nullstellensatz:** a word formed, in typical German fashion, from three simpler words:
Null (=zero), Stellen (=Places), Satz (=Theorem).

Glossary of symbols

Q	set of all rational numbers
Z	set of all integers
$\Re$	set of all real numbers
C	set of all complex numbers
N	set of natural numbers
$Z_{\geq 0}^{n}$	n-tuples, each entry is greater or equal to zero

CHAPTER ONE

1. PRELIMINARIES

We begin by recalling the definition of **field.** A field is a commutative ring with identity $1 \neq 0$ in which every nonzero element has a multiplicative inverse. The concept of field has a central place in algebra. It has wide applications in Linear Algebra and in the theory of equations, which deals with the study of roots of polynomials. If we do not require multiplicative inverses, then we get a commutative ring.

Definition: A commutative ring consists of a set R and two binary operations "$\bullet$" and "+" defined on R for which the following conditions are satisfied:

i) (associativity): $(a+b)+c = a+(b+c)$ and $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c \in R$.

ii) (commutativity): $a+b = b+a$ and $a \bullet b = b \bullet a$ for all $a, b \in R$.

iii) (distributive): $a \bullet (b+c) = a \bullet b + a \bullet c$ for all $a, b, c \in R$.

iv) (identities): There are $0, 1 \in R$ such that $a+0 = a \bullet 1 = a$ for all $a \in R$.

v) (additive inverses): Given $a \in R$, there is $b \in R$ such that $a+b = 0$.

1.1 POLYNOMIALS AND AFFINE SPACE

Definition 1.1.1: A monomial in $x_1,...,x_n$ is a product of the form

$$x_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$$

where $\alpha_1,\alpha_2,...,\alpha_n$ are nonnegative integers. The total degree of this monomial is the sum $\alpha_1+\alpha_2+...+\alpha_n$.

Example 1: In the variables x, y, z the following are examples of monomials:

$$x^2y^0z^0 = x^2, x^3y^8z^5, x^0y^{54}z^1 = y^{54}z$$

Notation: $x_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$, where $\alpha = (\alpha_1,\alpha_2,...,\alpha_n)$ are n-tuple of nonnegative integers. If $\alpha = (0,0,...,0)$, note that $x^\alpha = 1$, and also $|\alpha| = \alpha_1+\alpha_2+...+\alpha_n$ denote the total degree of monomial x^α.

Definition 1.1.2: A polynomial f in $x_1,...,x_n$ with coefficients in K is a finite linear combination (with coefficients in K) of monomials. We will write a polynomial f in the form

$$f = \sum_\alpha a_\alpha x^\alpha, a_\alpha \in K$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1,\alpha_2,...,\alpha_n)$.

The set of all polynomials in $x_1,...,x_n$ with coefficients in K is denoted $K[x_1,...,x_n]$.

Example 2: $f = 4x^5yz^2 + \frac{1}{2}x^3z + 3yz - y^3$ is a polynomial in $Q[x,y,z]$.

Definition 1.1.3: Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $K[x_1,...,x_n]$

i) We call a_α the coefficient of monomial x^α.

ii) If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a term of f.

iii) The total degree of f, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient $a_\alpha \neq 0$.

Example 3: $f = 4x^5yz^2 + \frac{1}{2}x^3z + 3yz - y^3$ has four terms and total degree eight.

Definition 1.1.4: Given a field K and a positive integer n, we define the n-dimensional **affine space** over K to be the set

$$K^n = \{(a_1,...,a_n) : a_1,...,a_n \in K\}.$$

Example 4: Consider $K = \Re$, we call $K^1 = K$ the affine line and K^2 the affine plane.

Let us next see how polynomials relate to affine space. A polynomial $f = \sum_{\alpha} a_\alpha x^\alpha \in K[x_1,...,x_n]$ gives a function $f : K^n \to K$ by

$$(a_1,a_2,...,a_n) \mapsto f(a_1,a_2,...,a_n) \in K,$$

where $(a_1,a_2,...,a_n) \in K^n$. The ability to regard a polynomial as a function is what makes it possible to link algebra and geometry. This dual nature of polynomials has some unexpected consequences.

Example 5: $f = 0$ has two potential meanings,

i) f is the zero polynomial, i.e. all of its coefficients a_α are zero.

ii) f is the zero function, i.e. $f(a_1,...,a_n) = 0$ for all $(a_1,a_2,...,a_n) \in K^n$.

These two statements are not equivalent in general, for example;

Consider $\mathbf{F}_2 = \{\bar{0},\bar{1}\}$, $x^2 - x = x(x-1) \in \mathbf{F}_2[x]$.

Since this polynomial vanishes at 0 and 1. Then we have found a nonzero polynomial which gives the zero function on the affine space $\mathbf{F}_2^1$. However, as long as K is infinite, there is no problem.

Proposition 1.1.5: Let K be an infinite field and let $f \in K[x_1,x_2,...,x_n]$. Then $f = 0$ in $K[x_1,...,x_n]$ if and only if $f : K^n \to K$ is the zero function.

Proof: Suppose $f \in K[x_1,x_2,...,x_n]$ is the zero polynomial. Which implies all the coefficients of f $a_\alpha = 0$. Thus, f is the zero function.

To prove the converse, we will use induction on the number of variables n.

If n = 1, since a nonzero polynomial in K[x] of degree m has at most m distinct roots. In particular, assume for $f \in K[x]$, $f(a) = 0$ for all $a \in K$. Since K is infinite, and then f has infinitely many roots, and hence must be the zero polynomial.

Now assume that the converse is true for n-1, and let $f \in K[x_1, x_2, ..., x_n]$ such that $f(a_1, ..., a_n) = 0$ for all $(a_1, a_2, ..., a_n) \in K^n$, then we can write

$$f = \sum_{i=0}^{N} g_i(x_1, x_2, ..., x_{n-1}) x_n^i \quad , \text{where } g_i \in K[x_1, x_2, ..., x_{n-1}]. \qquad ..... (1)$$

We need to show that, each g_i is the zero polynomial in n-1 variables.

If we fix $(a_1, a_2, ..., a_{n-1}) \in K^{n-1}$, then $(f(a_1, a_2, ..., a_{n-1}, x^n) \in K[x^n]$

By our hypothesis on f,

$$f(a_n) = 0 \text{ for every } a_n \in K .$$

It follows from the first case, i.e. n = 1 that $f(a_1, a_2, ..., a_{n-1}, x_n)$ is the zero polynomial in $K[x_n]$. Using (1), the coefficients of $f(a_1, a_2, ..., a_{n-1}, x_n)$ are $g_i(a_1, a_2, ..., a_{n-1})$. Thus $g_i(a_1, a_2, ..., a_{n-1}) = 0$ for all i.

Since $(a_1, a_2, ..., a_{n-1})$ is arbitrary in K^{n-1}, it follows that each $g_i \in K[x_1, x_2, ..., x_{n-1}]$ gives the zero function on K^{n-1}.

Therefore, f is the zero polynomial in $K[x_1, x_2, ..., x_n]$.

Corollary 1.1.6: Let K be an infinite field and let $f, g \in K[x_1, x_2, ..., x_n]$. Then $f = g$ in $K[x_1, x_2, ..., x_n]$ if and only if $f : K^n \to K$ and $g : K^n \to K$ are the same function.

Proof: Suppose $f = g$ in $K[x_1, x_2, ..., x_n]$.

$\Rightarrow f - g = 0$ in $K[x_1, x_2, ..., x_n]$.

$\Rightarrow$ all the coefficients of $f - g$ are zero.

Then, $f - g$ vanishes at all points of K^n.

Therefore, $f, g \in K[x_1, x_2, ..., x_n]$ gives the same function on K^n.

Conversely; assume $f, g \in K[x_1, x_2, ..., x_n]$ gives the same function on K^n.

Then f-g vanishes at all points of K^n, that is, $f - g$ is the zero function.

By the above proposition, f-g is the zero polynomial.

Therefore, $f = g$ in $K[x_1, x_2, ..., x_n]$.

1.2 AFFINE VARIETIES

Definition 1.2.1: Let K be a field and $f_1, f_2, ..., f_s$ be polynomials in $K[x_1, x_2, ..., x_n]$. Then we set

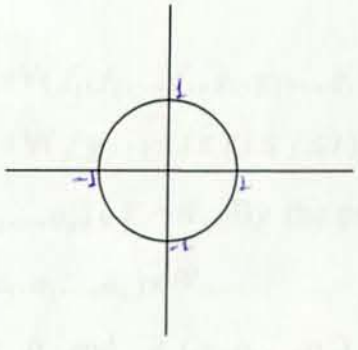
$$V(f_1, ..., f_s) = \{(a_1, a_2, ..., a_n) \in K^n : f_i(a_1, a_2, ..., a_n) = 0 \, for all \, 1 \le i \le s\}.$$

We call $V(f_1, f_2, ..., f_s)$ the **affine variety** defined by $f_1, f_2, ..., f_s$ .Thus, an affine varieties $V(f_1, f_2, ..., f_s) \subseteq K^n$ is the set of all solutions of the system of equations:

$$f_1(x_1, x_2, ..., x_n) = ... = f_s(x_1, x_2, ..., x_n) = 0$$

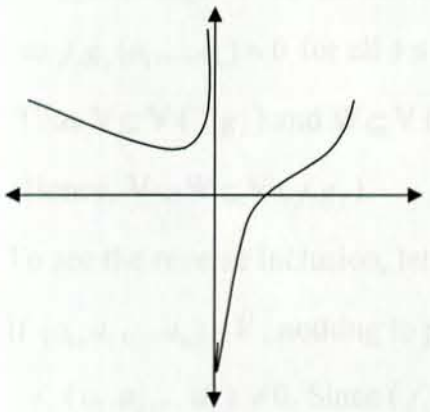
We will use the letter V, W, etc to denote affine varieties.

Examples 1.a) Consider the plane $\Re^2$ with the variety $V(x^2 + y^2 - 1)$ which is the circle of radius 1 centered at the origin.



b) Graphs of polynomial functions are affine varieties. (the graph of y =f(x) is V(y-f(x))).

c) Graphs of rational functions are affine varieties. For example, the graph of $y = \frac{x^3 - 1}{x}$ is the affine variety $V(xy - x^3 + 1)$.



d) Consider K=$\Re$, then $V(x^2 + y^2 + 1) = \phi$. Since $x^2 + y^2 = -1$ has no real solution. (Although there are solutions when K= **C**).

Lemma 1.2.2: If V, W$\subseteq K^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.

Proof: Suppose that V=**V**$(f_1, f_2, ..., f_s)$ and W=**V**$(g_1, g_2, ..., g_t)$. Then we claim that:

i) $V \cap W$ =**V**$(f_1, f_2, ..., f_s, g_1, g_2, ..., g_t)$

ii) $V \cup W$ =**V**$(f_i g_j : 1 \le i \le s, 1 \le j \le t)$

To prove (i), let $(a_1, a_2, ..., a_n) \in V \cap W$. By the property of intersection, we have $(a_1, a_2, ..., a_n) \in V$ and $(a_1, a_2, ..., a_n) \in W$.

$\Rightarrow$ $f_i(a_1, a_2, ..., a_n) = 0$ and $g_j(a_1, a_2, ..., a_n) = 0$ for all $1 \le i \le s, 1 \le j \le t$ respectively.

Thus, $(a_1, a_2, ..., a_n) \in$ **V**$(f_1, f_2, ..., f_s, g_1, g_2, ..., g_t)$.

Going the other way, choose $(b_1,b_2,...,b_n) \in \mathbf{V}(f_1,f_2,...,f_s,g_1,g_2,...,g_t)$. Then $f_i(b_1,b_2,...,b_n) = 0 = g_j(b_1,b_2,...,b_n)$ for all $1 \le i \le s, 1 \le j \le t$ respectively.

Thus, $(b_1,b_2,...,b_n) \in \mathbf{V}(f_1,f_2,...,f_s)$ and $(b_1,b_2,...,b_n) \in \mathbf{V}(g_1,g_2,...,g_t)$.

Hence $V \cap W = \mathbf{V}(f_1,f_2,...,f_s,g_1,g_2,...,g_t)$.

ii) Let $(a_1,a_2,...,a_n) \in V$.

$\Rightarrow f_i(a_1,...,a_n) = 0$ for all $1 \le i \le s$

$\Rightarrow f_i g_j(a_1,...,a_n) = 0$ for all $1 \le i \le s, 1 \le j \le t$.

Thus $V \subseteq \mathbf{V}(f_i g_j)$ and $W \subseteq \mathbf{V}(f_i g_j)$ follows similarly.

Hence, $V \cup W \subseteq \mathbf{V}(f_i g_j)$.

To see the reverse inclusion, let $(a_1,a_2,...,a_n) \in \mathbf{V}(f_i g_j)$.

If $(a_1,a_2,...,a_n) \in V$, nothing to prove. Suppose not, then there exist i_o such that $f_{i_o}(a_1,a_2,...,a_n) \neq 0$. Since $(f_{i_o} g_j)(a_1,a_2,...,a_n) = 0$ for all j, then

$g_j(a_1,a_2,...,a_n) = 0$ for all j.

$\Rightarrow (a_1,a_2,...,a_n) \in W$.

This shows that $\mathbf{V}(f_i g_j) \subseteq V \cup W$.

Therefore, $V \cup W = \mathbf{V}(f_i g_j : 1 \le i \le s, 1 \le j \le t)$.

Example 2.a) Consider the union of the (x, y) -plane and the z-axis in affine 3-space. We have V (z) $\cup$ V(x, y) = V(zx, zy).

b) The twisted cubic $V(y-x^2, z-x^3)$ in $\Re^3$

$V(y-x^2) \cap V(z-x^3) = V(y-x^2, z-x^3)$.

1.3 IDEALS

Definition 1.3.1: A subset $I \subseteq K[x_1, x_2, ..., x_n]$ is an ideal if it satisfies the following conditions:

i) $0 \in I$

ii) If $f, g \in I$, then $f + g \in I$

iii) If $f \in I$ and $h \in K[x_1, x_2, ..., x_n]$, then $hf \in I$.

The first natural example of an ideal is the ideal generated by a finite number of polynomials.

Definition 1.3.2: Let $f_1, f_2, ..., f_s \in K[x_1, x_2, ..., x_n]$. Then we set

$$< f_1, f_2, ..., f_s >= \{\sum_{i=1}^{s} h_i f_i : h_1, h_2, ..., h_s \in K[x_1, x_2, ..., x_n]\}.$$

The crucial fact is that $< f_1, f_2, ..., f_s >$ is an ideal.

Lemma 1.3.3: If $f_1, f_2, ..., f_s \in K[x_1, x_2, ..., x_n]$, then $< f_1, f_2, ..., f_s >$ is an ideal of $K[x_1, x_2, ..., x_n]$. We will call $< f_1, f_2, ..., f_s >$ the ideal generated by $f_1, f_2, ..., f_s$.

Proof: First, $0 \in < f_1, f_2, ..., f_s >$, since $0 = \sum_{i=1}^{s} 0 f_i$.

Next, let f, g$\in < f_1, f_2, ..., f_s >$, that is, $f = \sum_{i=1}^{s} p_i f_i$, g$= \sum_{i=1}^{s} q_i f_i$ and

h$\in K[x_1, x_2, ..., x_n]$.

Then, $f + g = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i$.

$$= \sum_{i=1}^{s} (p_i f_i + q_i f_i)$$

$$= \sum_{i=1}^{s} (p_i + q_i) f_i$$

Thus, $f + g \in < f_1, ..., f_s >$.

And also, $hf = h\sum_{i=1}^{s} p_i f_i = \sum_{i=1}^{s} h(p_i f_i) = \sum_{i=1}^{s} (hp_i) f_i$.

$\Rightarrow hf \in < f_1, f_2, ..., f_s >$.

Therefore, $< f_1, f_2, ..., f_s >$ is an ideal of $K[x_1, x_2, ..., x_n]$.

Proposition 1.3.4: If $f_1, f_2, ..., f_s$ and $g_1, g_2, ..., g_t$ are bases of the same ideal in $K[x_1, x_2, ..., x_n]$, so that $< f_1, ..., f_s >=< g_1, ..., g_t >$, then

$V(f_1, ..., f_s) = V(g_1, ..., g_t)$

Proof: Assume that $< f_1, f_2, ..., f_s > = < g_1, g_2, ..., g_t >$. We need to show that,

$V(f_1, f_2, ..., f_s) = V(g_1, g_2, ..., g_t)$.

Let $(a_1, a_2, ..., a_n) \in V(f_1, f_2, ..., f_s)$

$\Rightarrow f_i(a_1, a_2, ..., a_n) = 0$ for all i=1, 2,…, s.

Since $g_i \in < f_1, f_2, ..., f_s >$ for all i=1, 2,…, t.

Then, $g_i(a_1, a_2, ..., a_n) = 0$ for all i= 1, 2,…, t.

Hence $(a_1, a_2, ..., a_n) \in V(g_1, g_2, ..., g_t)$. Which implies that,

$V(f_1, f_2, ..., f_s) \subseteq V(g_1, g_2, ..., g_t)$.

Similarly we have $V(g_1, g_2, ..., g_t) \subseteq V(f_1, f_2, ..., f_s)$.

Therefore, $V(f_1, f_2, ..., f_s) = V(g_1, g_2, ..., g_t)$.

Example 1: Consider the variety V(x+y, x-y). To show, V(x+y, x-y) = V(x, y)

First, we have to show that, <x+y, x-y> = <x, y>. Since x, y∈<x, y>.

$\Rightarrow$ x+y, x-y∈<x, y> by the definition of ideal.

Thus, <x+y, x-y>⊆<x, y>.

Next, since x+y, x-y ∈<x+y, x-y>.

Then, (x+y) +(x-y) = 2x∈<x+y, x-y>.

$\Rightarrow$ x∈<x+y, x-y>

And also (x+y)-(x-y) = 2y∈<x+y, x-y>,

$\Rightarrow$ y∈<x+y, x-y>.

Thus, $\langle x, y\rangle \subseteq \langle x+y, x-y\rangle$.

Hence $\langle x, y\rangle = \langle x+y, x-y\rangle$, so that $V(x+y, x-y) = V(x, y) = \{(0, 0)\}$.

Definition 1.3.5: Let $V \subseteq K^n$ be an affine variety. Then we set

$$I(V) = \{f \in K[x_1, x_2, ..., x_n] : f(a_1, a_2, ..., a_n) = 0 \text{ for all } (a_1, a_2, ..., a_n) \in V\}.$$

The crucial observation is that $I(V)$ is an ideal.

Lemma 1.3.6: If $V \subseteq K^n$ is an affine variety, then $I(V) \subseteq K[x_1, x_2, ..., x_n]$ is an ideal.

We will call I(V) the ideal of V.

Proof: Now since the zero polynomial vanishes on all of K^n. In particular it vanishes on V. Then $0 \in I(V)$.

Next, suppose that $f, g \in I(V)$ and $h \in K[x_1, x_2, ..., x_n]$.

Let $(a_1, a_2, ..., a_n)$ be an arbitrary point of V.

Then, $(f+g)(a_1, a_2, ..., a_n) = f(a_1, ..., a_n) + g(a_1, ..., a_n)$

$= 0+0 = 0$

Then, $f+g \in I(V)$.

And also, $(hf)(a_1, a_2, ..., a_n) = h(a_1, a_2, ..., a_n) f(a_1, a_2, ..., a_n)$

$= h(a_1, a_2, ..., a_n).0$

$= 0$

Thus, $hf \in I(V)$. Hence I(V) is an ideal.

Example 2: Consider the variety $\{(0, 0)\}$ consisting of the origin in K^2.

Our claim is $I(\{(0, 0)\}) = \langle x, y\rangle$.

Since for any polynomial of the form

A(x, y)x + B(x, y)y vanishes at the origin.

Then $\langle x, y\rangle \subseteq I(\{(0, 0)\})$.

To see the other way, suppose that $f=\sum_{i,j} a_{ij}x^i y^j$ vanishes at the origin.

Then, $a_{00}=f(0, 0)=0$.

Since $f=a_{00}+\sum_{i,j\neq 0} a_{ij}x^i y^j = 0+\left(\sum_{\substack{i,j\\ i>0}} a_{ij}x^{i-1}y^j\right)x+\left(\sum_{j>0} a_{0j}y^{j-1}\right)\in<x, y>$.

Thus, $I(\{(0, 0)\})\subseteq<x, y>$.

Lemma 1.3.7: If $f_1, f_2,..., f_s \in K[x_1, x_2,..., x_n]$, then

$<f_1, f_2,..., f_s>\subset I(V(f_1, f_2,..., f_s))$.

Proof: Let $f\in<f_1, f_2,..., f_s>$, *i.e.*, $f=\sum_{i=1}^{s} h_i f_i$ for some

polynomials $h_1, h_2,..., h_s \in K[x_1, x_2,..., x_n]$. Since $f_1, f_2,..., f_s$ vanish on

$V(f_1, f_2,..., f_s)$, we have

$\sum h_i f_i$ must vanish on $V(f_1, f_2,..., f_s)$.

Thus, f vanishes on $V(f_1, f_2,..., f_s)$. Hence, $f\in I(V(f_1,..., f_s))$.

For the second part of the Lemma, we need an example where

$I(V(f_1, f_2,..., f_s))$ is strictly larger than $<f_1, f_2,..., f_s>$. We will show that the

inclusion $<x^2, y^2>\subset I(V(x^2, y^2))$ is not equality.

First compute $I(V(x^2, y^2))$.

The equations $x^2=y^2=0$

$\Rightarrow V(x^2, y^2)=\{(0,0)\}$.

From the previous example, since $I(\{(0,0)\})=<x, y>$. So that

$I(V(x^2, y^2))=<x, y>$.

To see that $<x, y>\subset I(V(x^2, y^2))$, note that $x\notin<x^2, y^2>$. Since for

polynomials of the form $h_1(x, y)x^2+h_2(x, y)y^2$, every monomial has total

degree at least two.

Proposition 1.3.8: Let V and W be affine varieties in K^n. Then:

i) $V \subseteq W$ if and only if $I(V) \supseteq I(W)$.

ii) $V = W$ if and only if $I(V) = I(W)$.

Proof: i) Suppose $V \subseteq W$. Then any polynomial vanishing on W must vanish on V.

Hence $I(V) \supseteq I(W)$.

To show the converse, assume that $I(V) \supseteq I(W)$.

Since W is the variety defined by some polynomials

$g_1, g_2, ..., g_t \in K[x_1, x_2, ..., x_n]$.

$\Rightarrow g_1, g_2, ..., g_t \in I(W) \subseteq I(V)$

Hence the g_i's vanish on V. Since W consists of all common zero of the g_i's. Thus, $V \subseteq W$.

ii) is an immediate consequence of (i).

CHAPTER TWO

2. THE IDEAL-VARIETY CORRESPONDENCE

In this chapter, we will explore the correspondence between ideals and varieties. Also we will prove the Nullstellensatz, a celebrated theorem which identifies exactly which ideals correspondence to varieties. This will allow us to construct a dictionary between geometry and algebra, where any statement about varieties can be translated into a statement about ideals (and conversely).

2.1 ORDERING ON THE MONOMIALS IN K[$x_1, x_2, \ldots, x_n$]

If we examine in detail the division algorithm in K[x], we see that a notion of **ordering of terms** in polynomials is a key ingredient. For example, in dividing $f(x) = x^5 - 3x^2 + 1$ by $g(x) = x^2 - 4x + 7$ by the standard method, we would:

- Write the terms in the polynomials in decreasing order by degree in x.
- At the first step, the leading term in f is $x^5 = x^3 \cdot x^2 = x^3 \cdot$(leading term in g). Thus, we would subtract $x^3 \cdot g(x)$ from f to cancel the leading term, leaving $4x^4 - 7x^3 - 3x^2 + 1$.
- Then, we would repeat the same process on $f(x) - x^3 g(x)$,etc., until we obtain a polynomial of degree less than 2.

  For the division algorithm on polynomials in one variable, then, we are dealing with the degree ordering on the one-variable:

(1) $\cdots > x^{m+1} > x^m > \ldots > x^2 > x > 1.$

The success of the algorithm depends on working systematically with the leading terms in f and g, and not removing terms "at random" from f using arbitrary terms from g. With these considerations in mind, we make the following definition.

Definition 2.1.1: A **monomial ordering** on $K[x_1,...,x_n]$ is an ordering > on $Z^n_{\geq 0}$ such that:

- > is a total (or linear) ordering on $Z^n_{\geq 0}$.
- Given $x^\alpha, x^\beta, x^\gamma$, that $x^\alpha > x^\beta \Rightarrow x^\alpha x^\gamma > x^\beta x^\gamma$.
- > is well-ordering on $Z^n_{\geq 0}$. This means that every nonempty subset of $Z^n_{\geq 0}$ has a smallest element under >.

A simple example of a monomial order is the usual numerical order

. . . > m+1 > m> . . .> 2> 1> 0

on the element of $Z_{\geq 0}$, since it satisfy the three condition of monomial ordering, hence the degree ordering (1) on the monomials in K[x] is a monomial ordering. Our example of an ordering on n-tuples will be lexicographic order (or lex order).

Definition 2.1.2: (**Lexicographic order**). Let $\alpha = (\alpha_1, \alpha_2,..., \alpha_n)$ and $\beta = (\beta_1, \beta_2,..., \beta_n) \in Z^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in Z^n$, the left-most nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Example 1: a) $(2, 3, 1) >_{lex} (1, 4, 2)$ since $\alpha - \beta = (1,-1,-1)$.

b) $(6, 4, 8) >_{lex} (6, 4, 2)$ since $\alpha - \beta = (0,0,6)$.

c) The variables $x_1, x_2,..., x_n$ are ordered in the usual way by the lex ordering

$$(1, 0, 0,\ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \ldots >_{lex} (0, 0, 0, \ldots, 1).$$

So $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

We will end this section with a discussion of how a monomial ordering can be applied to polynomials.

If $f = \sum_{\alpha} a_\alpha x^\alpha$ is a polynomial in $K[x_1, x_2, \ldots, x_n]$ and we have selected a monomial ordering >, then we can order the monomial of f in an unambiguous way with respect to >.

For example, $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$. Then, with respect to the lex order, we would reorder the terms of f in decreasing order as $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$.

Proposition 2.1.3: The lex order on $Z_{\geq 0}^n$ is a monomial ordering.

Proof: i) The relation $>_{lex}$ is a total ordering. Since from the definition and the fact that the usual numerical order on $Z_{\geq 0}$ is a total ordering.

ii) Let $\alpha >_{lex} \beta$. The left-most nonzero entry in $\alpha - \beta$, say $\alpha_k - \beta_k$ is positive. But $x^\alpha x^\delta = x^{\alpha+\delta}$ and $x^\beta x^\delta = x^{\beta+\delta}$, then in $(\alpha + \delta) - (\beta + \delta) = \alpha - \beta$.

$\Rightarrow$ The left-most nonzero entry is again $\alpha_k - \beta_k > 0$.

iii) Suppose that $>_{lex}$ were not a well-ordering.

$\Rightarrow$ There is $\phi \neq S \subseteq Z_{\geq 0}^n$ has no least element.

Now pick $\alpha(1) \in S$. Since $\alpha(1)$ is not the least element, then we can find $\alpha(1) >_{lex} \alpha(2)$ in S. Thus, $\alpha(2)$ is also not the least element, so that there is $\alpha(2) >_{lex} \alpha(3)$ in S. Continuing this way, we obtain an infinite strictly decreasing sequence $\alpha(1) >_{lex} \alpha(2) >_{lex} \ldots$ of elements of $Z_{\geq 0}^n$.

We claim that this leads to a contradiction.

Consider the first entries of the vectors $\alpha(i) \in Z_{\geq 0}^{n}$, and then by the definition of lex order, these first entries form a non increasing sequence of nonnegative integers. Since $Z_{\geq 0}$ is well-ordering, the first entries of the $\alpha(i)$ must stabilize eventually. That is, there exist k, such that all the first components of the $\alpha(i)$ with $i \geq k$ are equal.

Beginning at $\alpha(k)$, the second entries of $\alpha(k), \alpha(k+1),...$ form a non increasing sequence. By the same reasoning as before, the second entries stabilize eventually as well.

Continuing in the same way, the $\alpha(l), \alpha(l+1),...$ all are equal for some l. This contradict with the fact that $\alpha(l) >_{lex} \alpha(l+1)$.

Definition 2.1.4: Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a nonzero polynomial in $K[x_1, x_2, ..., x_n]$

where $x^{\alpha_m} > x^{\alpha_{m-1}} > \cdots > x^{\alpha_1}$, then:

- The **leading monomial** of f, written $LM(f)$ is $LM(f) = x^{\alpha_m}$
- The **multidegree** of f is the degree of the leading monomial. Written $multi\deg(f) = \alpha_m$.
- The **leading coefficient** is $LC(f) = a_m$
- The **leading term** is $LT(f) = a_m x^{\alpha_m} LC(f).LM(f)$.

Example 2: Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ and let > denote the lex order. Then,

$multi\deg(f) = (3,0,0)$

$LC(f) = -5$

$LM(f) = x^3$

$LT(f) = -5x^3$.

2.2 MONOMIAL IDEALS AND DICKSON'S LEMMA

In this section, we will consider the ideal description problem for the special case of monomial ideals. To start, we define monomial ideals in $K[x_1, x_2, ..., x_n]$.

Definition 2.2.1: A **monomial ideal** is an ideal $I \subseteq K[x_1, x_2, ..., x_n]$ such that there is a subset $A \subseteq Z_{\geq 0}^n$ (possibly infinite) such that each $f \in I$ can be written as $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in K[x_1, x_2, ..., x_n]$, and every function of this form is in I. we write this as

$$I = < x^\alpha : \alpha \in A > .$$

Example 1: $I = < x^4 y^2, x^3 y^4, x^2 y^5 > \subseteq K[x, y]$ is a monomial ideal.

Lemma 2.2.2: Let $I = < x^\alpha : \alpha \in A >$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.

Proof: ($\Leftarrow$) Let x^β is divisible by x^α for some $\alpha \in A$.

$\Rightarrow x^\beta$ is a multiple of x^α, $x^\beta \in I$ by the definition of ideal.

($\Rightarrow$) If $x^\beta \in I$, then by definition

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} \text{ , where } h_i \in K[x_1, x_2, ..., x_n] \text{ and } \alpha(i) \in A \ .$$

If we expand each h_i as a linear combination of monomials, then every term on the right side of the equation is divisible by some $x^{\alpha(i)}$. Hence, x^β is divisible by x^α for some $\alpha \in A$.

Let us next show that whether a given polynomial f lies in a monomial ideal can be determined by looking at the monomials of f.

Lemma 2.2.3: Let I be a monomial ideal and let $f \in K[x_1, x_2, ..., x_n]$. Then the following are equivalent:

(i) $f \in I$

(ii) Every term of f lies in I.

(iii) f is a K-linear combination of the monomials in I.

Proof: (iii) $\Rightarrow$ (ii). Suppose f is a K-linear combination of the monomials in I.

Since I is an ideal then every term of f lies in I.

Next, to show (ii) $\Rightarrow$ (i), assume every term of f lies in I, then f lies in I, because I is an ideal.

Finally, the proof of (i) $\Rightarrow$ (iii) is similar to what we did in Lemma 2.2.2.

Corollary 2.2.4: Two monomial ideals are the same if and only if they contain the same monomials.

The main result of this section is that all monomial ideals of $K[x_1, x_2, ..., x_n]$ are finitely generated.

Theorem 2.2.5: (Dickson's Lemma). A monomial ideal

$$I = < x^\alpha : \alpha \in A > \subseteq K[x_1, ..., x_n]$$

can be written down in the form $I = < x^{\alpha(1)}, ..., x^{\alpha(s)} >$, where $\alpha(1), ..., \alpha(s) \in A$.

In particular, I has a finite basis.

Proof: By induction on n.

If n = 1, then I is generated by the monomials x_1^α where $\alpha \in A \subseteq Z_{\geq 0}$.

Let β be the smallest element of $A \subseteq Z_{\geq 0}$. Then $\beta \leq \alpha$ for all $\alpha \in A$, so that x_1^β divides all other generators x_1^α.

$\Rightarrow$ $I = < x_1^\beta >$.

Now assume that n > 1 and that the theorem is true for n-1. We will write the variables as $x_1, ..., x_{n-1}, y$, so that monomials in $K[x_1, ..., x_{n-1}, y]$ can be written as $x^\alpha y^m$, where $\alpha = (\alpha_1, ..., \alpha_{n-1}) \in Z_{\geq 0}^{n-1}$ and $m \in Z_{\geq 0}$.

Suppose that $I \subseteq K[x_1, ..., x_{n-1}, y]$ is a monomial ideal. We need to find the generators for I. Let J be the ideal in $K[x_1, ..., x_{n-1}]$ generated by the monomials x^α for which $x^\alpha y^m \in I$ for some $m \geq 0$. Since J is a monomial ideal in $K[x_1, ..., x_{n-1}]$. By our inductive hypothesis,

$\Rightarrow$ finitely many of the x^{α}'s generate J, say $J =< x^{\alpha(1)},...,x^{\alpha(s)} >$.

The ideal J can be understood as the projection of I into $K[x_1,...,x_{n-1}]$.

The definition of J tells us for each $1 \le i \le s$, $x^{\alpha(i)}y^{m_i} \in I$ for some $m_i \ge 0$.

Let m be the largest of the m_i. Then, for each k between 0 and m-1, consider the ideal $J_k \subseteq K[x_1,...,x_{n-1}]$ generated by monomials x^{β} such that $x^{\beta}y^k \in I$. One can think of J_k as the slice of I generated by monomials containing y exactly to the k^{th} power. Then, J_k has a finite generating set of monomials, say $J_k =< x^{\alpha_k(1)},...,x^{\alpha_k(s_k)} >$, (using our inductive hypothesis).

We claim that I is generated by the monomials in the following list:

from J: $x^{\alpha(1)}y^m,...,x^{\alpha(s)}y^m$,

from J_0: $x^{\alpha_0(1)},...,x^{\alpha_0(s_0)}$,

from J_1: $x^{\alpha_1(1)}y,...,x^{\alpha_1(s_1)}y$,

$\vdots$

from J_{m-1}: $x^{\alpha_{m-1}(1)}y^{m-1},...,x^{\alpha_{m-1}(s_{m-1})}y^{m-1}$

First note that every monomial in I is divisible by one on the list. To see why, Let $x^{\alpha}y^{p} \in I$. If $p \ge m$, then $x^{\alpha}y^{p}$ is divisible by some $x^{\alpha(i)}y^{m}$ by the construction of J.

On the other hand, if $p \le m-1$, and then $x^{\alpha}y^{p}$ is divisible by some $x^{\alpha_p(j)}y^{p}$ by the construction of J_p.

$\Rightarrow$ By Lemma 2.2.2, the above monomials generate an ideal having the same monomials as I. By corollary 2.2.4, our claim is proved.

Finally, let $I =< x^{\alpha} : \alpha \in A >\subseteq K[x_1,...,x_n]$.

We need to show that I is generated by finitely many of the x^{α}'s, where $\alpha \in A$.

By the above induction, since $I =< x^{\beta(1)},...,x^{\beta(s)} >$ for some monomials $x^{\beta(i)}$ in I

and also $x^{\beta(i)} \in I =< x^{\alpha} : \alpha \in A >$

$\Rightarrow x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ for some $\alpha(i) \in A$.

$\Rightarrow x^{\beta(i)} = x^{\alpha(i)} x^{\gamma(i)}$ for some monomial $\gamma(i) \in K[x_1,...,x_n]$ by lemma 2.2.2.

$\Rightarrow x^{\beta(i)}$ and $x^{\alpha(i)}$ generate the same ideal.

Then, I = $<x^{\alpha(1)},...,x^{\alpha(s)}>$. This completes the theorem.

2.3 THE HILBERT BASIS THEOREM

In this section, we will give a solution of the ideal description problem, that is, can every ideal $I \subseteq K[x_1, x_2,..., x_n]$ be written as $< f_1, f_2,..., f_s >$ for some $f_1, f_2,..., f_s \in K[x_1, x_2,..., x_n]$? The key idea we will use is a monomial ordering, each f$\in K[x_1, x_2,..., x_n]$ has a unique leading term LT(f). Then for any ideal I we can define its ideal of leading terms as follow:

Definition 2.3.1: Let $I \subseteq K[x_1, x_2,..., x_n]$ be an ideal other than $\{0\}$.

i) We denote by LT(I) the set of leading terms of elements of I. Thus,

$LT(I) = \{cx^{\alpha} : \text{there exist } f \in I \text{ with } LT(f) = x^{\alpha}\}$.

ii) We denote by <LT(I)> the ideal generated by the elements of LT(I).

If we are given a finite generating set for I, say I =$< f_1, f_2,..., f_s >$, then $< LT(f_1),..., LT(f_s) >$ and <LT (I)> may be different ideals.

From the definition since LT(f_i) $\in LT(I) \subseteq < LT(I) >$

$\Rightarrow < LT(f_1),..., LT(f_s) > \subseteq <$ LT (I) >.

However, <LT(I)> can be strictly larger. To see this, consider the next example.

Example 1: Let I =$< f_1, f_2 >$, where $f_1 = x^3$-2xy and $f_2 = x^2$y+x-2 y^2. Using lex ordering on monomials in K[x, y]. We have,

x(x^2y+x-2 y^2)-y (x^3-2xy) =x^2. So that $x^2 \in I$.

$\Rightarrow x^2 = LT(x^2) \in < LT(I) >$. However, x^2 is not divisible by LT(f_1) = x^3 or LT(f_2) = x^{2}y, then by lemma 2.2.6, x$^2 \notin < LT(f_1), LT(f_2) >$.

Proposition 2.3.2: Let I $\subseteq K[x_1, x_2, ..., x_n]$ be an ideal

i) <LT(I)> is a monomial ideal.

ii) There are $g_1, g_2, ..., g_t \in I$ such that

<LT(I)> = $< LT(g_1), LT(g_2), ..., LT(g_t) >$.

Proof: i) The leading monomials LM(g) of elements g$\in I - \{0\}$ generate the monomial ideal <LM(g): g$\in I - \{0\}$>. Since LM(g) and LT(g) differ by a nonzero constant, then <LT(g): g$\in I - \{0\}$> =<LT(I)>.

Therefore, <LT(I)> is a monomial ideal.

ii) Since <LT(I)> is generated by the monomials LM(g) for g$\in I - \{0\}$. Since all monomials of $K[x_1, x_2, ..., x_n]$ are finitely generated, by Dickson's Lemma:

$\Rightarrow$ <LT(I)> = $<LT(g_1), LT(g_2), ..., LT(g_t) >$ for finitely many $g_1, g_2, ..., g_t \in I$. Since LM(g_i) differs from LT(g_i) by a nonzero constant. Hence, <LT(I)> = $<LT(g_1), LT(g_2), ..., LT(g_t) >$.

Theorem 2.3.3: (Hilbert Basis Theorem). Every ideal $I \subseteq K[x_1, x_2, ..., x_n]$ has a finite generating set. That is, $< I = < g_1, g_2, ..., g_t >$ for some $g_1, g_2, ..., g_t \in I$.

Proof: If I = {0}, we take our generating set to be {0}. This is certainly finite.

If I contain some nonzero polynomial, then a generating set $g_1, g_2, ..., g_t$ for I can be constructed as follows.

By the above proposition, there are $g_1, g_2, ..., g_t \in I$ such that

<LT(I)> = $<LT(g_1), LT(g_2), ..., LT(g_t) >$.We claim that I =$< g_1, g_2, ..., g_t >$. Now since each $g_i \in$ I, then $< g_1, g_2, ..., g_t > \subseteq I$.

To see the other way, let f$\in I$ be arbitrary polynomial. To divide f by $< g_1, g_2, ..., g_t >$ apply the division algorithm, then we get

$$f = a_1 g_1 + a_2 g_2 + ... + a_t g_t + r$$

Where no term of r is divisible by any of $LT(g_1), LT(g_2),..., LT(g_t)$. We claim that r = 0. To see this, note that $r = f - a_1g_1 - ... - a_tg_t \in I$. If $r \neq 0$, then $LT(r) \in <LT(I)> = <LT(g_1), LT(g_2),..., LT(g_t)>$. Which implies that, LT(r) must be divisible by some $LT(g_t)$ contradict with the assumption (i.e., no term of r is divisible by any of $LT(g_1), LT(g_2),..., LT(g_t)$). Hence, r must be zero. Thus, $f = a_1g_1 + a_2g_2 + ... + a_tg_t + 0 \in <g_1, g_2,..., g_t>$.

Then, $I \subseteq <g_1, g_2,..., g_t>$. Therefore $I = <g_1, g_2,..., g_t>$.

Our second consequence of the Hilbert Basis Theorem will be geometric. Up to this point, we have considered affine varieties as the set of solutions of specific finite sets of polynomial equations:

$$V(f_1, f_2,..., f_s) = \{(a_1, a_2,..., a_n) \in K^n : f_i(a_1,..., a_n) = 0 \text{ for all i}\}.$$

The Hilbert Basis Theorem shows that, in fact, it also makes sense to speak of the affine variety defined by an ideal $I \subseteq K[x_1, x_2,..., x_n]$.

Definition 2.3.4: Let $I \subseteq K[x_1, x_2,..., x_n]$ be an ideal. We will denote by V(I) the set $V(I) = (a_1, a_2,..., a_n) \in K^n : f(a_1,..., a_n) = 0$ for all $f \in I\}$.

Even though a nonzero ideal I always contains infinitely many different polynomials the set V(I) can still be defined by a finite set of polynomial equations.

Proposition 2.3.5: V(I) is an affine variety. In particular, if $I = < f_1, f_2,..., f_s >$, then $V(I) = V(f_1, f_2,..., f_s)$.

Proof: By the Hilbert Basis Theorem, $I = < f_1, f_2,..., f_s >$ for some finite generating set. We claim that, V(I) = V $(f_1, f_2,..., f_s)$.

First, since $f_i \in$ I, if f $(a_1, a_2,..., a_n) = 0$ for all $f \in I$ so $V(I) \subseteq V(f_1, f_2,..., f_s)$. On the other hand, let $f \in$ I since $I = < f_1, f_2,..., f_s >$, then

$$f = \sum_{i=1}^{s} h_i f_i \quad \text{for some } h_i \in K[x_1, x_2,..., x_n]$$

But then, $f(a_1,...,a_n) = \sum_{i=1}^{s} h_i(a_1,...,a_n) f_i(a_1,...,a_n)$

$$= \sum_{i=1}^{s} h_i(a_1,...,a_n).0 = 0$$

Thus, $V(f_1, f_2,..., f_s) \subseteq V(I)$ and hence, $V(I) = V(f_1, f_2,..., f_s)$.

2.4 RADICAL IDEALS AND THE IDEAL-VARIETY CORRESPONDENCE

In the previous chapter, we saw that

$$I(V) = \{f \in K[x_1,...,x_n] : f(x) = 0 \text{ for all } x \in V\}.$$

A variety $V \subseteq K^n$ can be studied by passing to the ideal of all polynomials vanishing on V. That is, we have a map

$$\begin{array}{ccc} \text{affine varieties} & \xrightarrow{I} & \text{ideals} \\ V & & I(V). \end{array}$$

Conversely, for all ideal $I \subseteq K[x_1, x_2,..., x_n]$, we can define the set

$$V(I) = \{x \in K^n : f(x) = 0 \text{ for all } f \in I\}.$$

By Hilbert Basis Theorem, there exist a finite set of polynomials $f_1,..., f_s \in I$ such that $I = < f_1,..., f_s >$. Since V(I) is the set of common roots of these polynomials. Thus, we have a map

$$\begin{array}{ccc} \text{ideals} & \xrightarrow{V} & \text{affine varieties} \\ I & & V(I) \end{array}$$

These two maps give us a correspondence between ideals and varieties. But the map V is not one-to-one because two different ideals can give the same variety. For example, < x > and $< x^2 >$ are different ideals in K[x] which have the same variety $V(x) = V(x^2) = \{0\}$.

Theorem 2.4.1: (The Weak Nullstellensatz). Let K be an algebraically closed field and let $I \subseteq K[x_1, x_2, ..., x_n]$ be an ideal satisfying $V(I) = \phi$. Then, $I = K[x_1, x_2, ..., x_n]$.

Proof: Suppose I $\subseteq K[x_1, x_2, ..., x_n]$ be an ideal with V(I) $= \phi$. We claim that, I $= K[x_1, x_2, ..., x_n]$.

By induction on n, if n = 1 and I $\subseteq K[x]$ satisfies $V(I) = \phi$. We will show that, I=K[x]. Since K is a field, then every ideal of K[x] can be written in the form $< f >$ for some $f \in K$, that is, $I =< f >$. Then V(I) is the set of roots of f . i.e., the set $a \in K$ *suchthat* $f(a) = 0$. But since K is algebraically closed, then every non constant polynomial has a root. Hence, $V(I) = \phi$ only if f is nonzero constant. This implies that, $\frac{1}{f} \in K$. Thus, $1=\left(\frac{1}{f}\right) f \in I$. Hence, I =K[x].

Now assume the condition is true for the polynomial ring in n-1 variables, we write as $K[x_2, ..., x_n]$. Consider I $=< f_1, ..., f_s > \subseteq K[x_1, x_2, ..., x_n]$ for which $V(I) = \phi$. Assume f_1 is not a constant and has total degree $N \geq 1$.

Consider the linear change of coordinates

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2 \tilde{x}_1, \\ &\vdots \\ x_n &= \tilde{x}_n + a_n \tilde{x}_1. \end{aligned}$$

Where a_i's are as yet to be determined constants in K. Then,

$f_1(x_1, ..., x_n) = f_1(\tilde{x}_1, \tilde{x}_2 + a_2\tilde{x}_1, ..., \tilde{x}_n + a_n\tilde{x}_1) = c(a_2, ..., a_n)\tilde{x}_1^{\,N}$ + terms in which $\tilde{x}_1$ has degree < N.

Since c($a_1, ..., a_n$) is a nonzero polynomial expression in $a_2, ..., a_n$ and K is infinite. Thus, we can choose ($a_2, ..., a_n$) and c($a_1, ..., a_n$) $\neq 0$.

Then every polynomial $f \in K[x_1,\ldots,x_n]$ goes over to a polynomial $\tilde{f} \in K[\tilde{x}_1,\ldots,\tilde{x}_n]$, $\tilde{I} = \{\tilde{f} : f \in I\}$ is an ideal in $K[\tilde{x}_1,\ldots,\tilde{x}_n]$ and we have $V(\tilde{I}) = \phi$. Our claim is, $1 \in \tilde{I}$. To see this, $f_1 \in I$ transforms to $\tilde{f}_1 \in \tilde{I}$ with $\tilde{f}_1(\tilde{x}_1,\ldots,\tilde{x}_n) = c(a_2,\ldots,a_n)\tilde{x}_1^{\,N}$ + terms in which $\tilde{x}_1$ has degree < N, where $c(a_2,\ldots,a_n) \neq 0$. Let $\pi_1 : K^n \to K^{n-1}$ be the projection mapping onto the last n-1 components. If we set $\tilde{I}_1 = \tilde{I} \cap K[\tilde{x}_2,\ldots,\tilde{x}_n]$ as usual, then the partial solutions in K^{n-1} always extend, that is, $V(\tilde{I}_1) = \pi_1(V(\tilde{I}))$. This implies that, $V(\tilde{I}_1) = \pi_1(V(\tilde{I})) = \pi_1(\phi) = \phi$. Thus, $\tilde{I}_1 = K[\tilde{x}_2,\ldots,\tilde{x}_n]$ by the inductive hypothesis. Then, $1 \in \tilde{I}_1 \subseteq \tilde{I}$. Hence, $1 \in I$ and the proof is complete.

The Weak Nullstellensatz Theorem tells us the correspondence between ideals and varieties is one-to-one provided only that one restricts to algebraically closed field.

Theorem 2.4.2: (Hilbert's Nullstellensatz). Let K be an algebraically closed field. If $f_1, f_2,\ldots, f_s \in K[x_1,\ldots,x_n]$ are such that $f \in I(V(f_1,\ldots,f_s))$, then there exists an integer $m \geq 1$ such that

$$f^m \in < f_1,\ldots,f_s >$$ (and conversely).

Proof: Let $f \in I(V(f_1,\ldots,f_s))$. Then f vanishes at every common zero of the polynomials $f_1,\ldots,f_s$. We claim that, there exist $m \geq 1$ and polynomials $A_1,\ldots,A_s$ such that $f^m = \sum_{i=1}^{s} A_i f_i$.

Consider the ideal, $\tilde{I} = < f_1,\ldots,f_s, 1 - yf > \subseteq K[x_1,\ldots x_n, y]$. We have to show that, $V(\tilde{I}) = \phi$. To see this let $(a_1,\ldots,a_n,a_{n+1}) \in K^{n+1}$, either $(a_1,\ldots,a_n)$ is a common zero of $f_1, f_2,\ldots, f_s$ or $(a_1,\ldots,a_n)$ is not a common zero of $f_1, f_2,\ldots, f_s$.

i) Since f vanishes at any common zero of $f_1, f_2, ..., f_s$. Thus, 1-yf takes the value $1 - a_{n+1} f(a_1, ..., a_n) = 1 \neq 0$ at $(a_1, ..., a_n, a_{n+1})$. In particular $(a_1, ..., a_n, a_{n+1}) \notin V(\tilde{I})$.

ii) For some i, $1 \leq i \leq s$, we must have $f_i(a_1, ..., a_n) \neq 0$. Let f_i be a function of n+1 variable which does not depend on the last variable, then $f_i(a_1, ..., a_n, a_{n+1}) \neq 0$. In particular we again conclude that $(a_1, ..., a_n, a_{n+1}) \notin V(\tilde{I})$. Since $(a_1, ..., a_n, a_{n+1}) \in K^{n+1}$ was arbitrary, therefore, $V(\tilde{I}) = \phi$.

Now apply the Weak Nullstellensatz to conclude that $1 \in \tilde{I}$, that is,

$1 = \sum_{i=1}^{s} p_i(x_1, ..., x_n, y) f_i + q(x_1, ..., x_n, y)(1 - yf)$ for some $p_i, q \in K[x_1, ..., x_n, y]$.

Now set y =1/ f $(x_1, ..., x_n)$. Then, $1 = \sum_{i=1}^{s} p_i(x_1, ..., x_n, 1/f) f_i$.

Multiply both sides by f^m, where m is chosen sufficiently large to clear all the denominators. Thus, $f^m = \sum_{i=1}^{s} A_i f_i$ *for some* $A_i \in K[x_1, ..., x_n]$.

Lemma 2.4.3: Let V be a variety. If $f^m \in I(V)$, then $f \in I(V)$.

Proof: Let x∈ V. If $f^m \in I(V)$, then $(f(x))^m = 0$. But this can happen only if f(x) = 0. Since x∈ V was arbitrary, f∈ I(V).

Definition 2.4.4: An ideal I is **radical** if $f^m \in I$ for some $m \geq 1$ implies that $f \in I$.

Corollary 2.4.5: I(V) is a radical Ideal.

On the other hand, Hilbert's Nullstellensatz tells us that the only way on arbitrary idea I can fail to be the ideal of all polynomials vanishing on V(I) is for I to contain powers f^m of polynomials f which are not in I.

In other words, for I to fail to be a radical ideal. This suggests that there is a one-to-one correspondence between affine varieties and radical ideals.

Definition 2.4.6: Let $I \subseteq K[x_1, x_2, ..., x_n]$ be an ideal. The **radical** of I, denoted $\sqrt{I}$, is the set

$$\{f : f^m \in I \text{ for some integer } m \geq 1\}.$$

Lemma 2.4.7: An ideal I is radical if and only if $I = \sqrt{I}$.

Proof: First, to show $I \subseteq \sqrt{I}$. Since $f \in I$. Which implies that, $f^1 \in I$. Then $f \in \sqrt{I}$. Thus, $I \subseteq \sqrt{I}$. To see the converse inclusion, let $f \in \sqrt{I}$. Then by the definition, $f^m \in I$ for some $m \geq 1$. Since I is a radical ideal, then $f \in I$. Thus, $\sqrt{I} \subseteq I$. Therefore, $I = \sqrt{I}$. Next, assume that $I = \sqrt{I}$, then $I = \{ f \subseteq K[x_1, ..., x_n] : f^m \in I \text{ for some integer } m \geq 1 \}$. Then by the definition, I is radical.

Lemma 2.4.8: If I is an ideal in $K[x_1, x_2, ..., x_n]$, then $\sqrt{I}$ is an ideal in $K[x_1, x_2, ..., x_n]$ containing I. Furthermore, $\sqrt{I}$ is a radical ideal.

Proof: i) We always have $I \subseteq \sqrt{I}$. To show $\sqrt{I}$ is an ideal first, $0 \in \sqrt{I}$ since $0 \in I$. Next, let $f, g \in \sqrt{I}$, then there are positive integers m and l such that $f^m, g^l \in I$. Using binomial expansion of $(f+g)^{m+l-1}$ every term has a factor $f^i g^j$ with $i + j = m + l - 1$. Since either $i \geq m$ or $j \geq l$, then either f^i or g^j is in I, whence $f^i g^j \in$ I and every term in the binomial expansion is in I. Hence, $(f+g)^{m+l-1} \in I$. Therefore, $f + g \in \sqrt{I}$.

Finally, let $f \in \sqrt{I}$ and $h \in K[x_1, x_2, ..., x_n]$, then $f^m \in$ I for some $m \geq 1$. Since I is an ideal, $(hf)^m = h^m f^m \in I$. Hence, hf $\in \sqrt{I}$. This shows that $\sqrt{I}$ is an ideal.

ii) To show $\sqrt{I}$ is a radical ideal, let $f^m \in \sqrt{I}$ for some integer $m \geq 1$. Then, by the definition of radical ideal $(f^m)^n \in I$ for some integer $n \geq 1$. This implies that, $f^{mn} \in I$ for some mn ≥ 1. By definition, we have $f \in \sqrt{I}$.

Therefore, $\sqrt{I}$ is a radical ideal.

Example 1: Consider $J < x^2, y^3 > \subseteq K[x, y]$. We will show that the radical of an ideal J is an ideal.

Solution: First, since x, y $\notin$ J, but x, y $\in \sqrt{J}$. Since $x^2 \in J$, then $(xy)^2 = x^2y^2 \in J$. Thus, $xy \in \sqrt{J}$. Secondly, $(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \in J$, because $x^4, 4x^3y, 6x^2y^2 \in J$ (all are multiples of x^2) and $4xy^3, y^4 \in J$ (they are multiples of y^3). Thus, $x + y \in \sqrt{J}$. But xy, x+y $\notin J$.

Theorem 2.4.9: (The strong Nullstellensatz). Let K be an algebraically closed field. If I is an ideal in $K[x_1, x_2, ..., x_n]$, then $I(V(I)) = \sqrt{I}$.

Proof: Given I is an ideal in $K[x_1, x_2, ..., x_n]$. Let $f \in \sqrt{I}$, then by definition, $f^m \in$ I for some positive integer m. Hence, f^m vanishes on V(I), which implies that, f vanishes on V(I). Thus, $f \in$ I(V(I)). Conversely, let $f \in$ I(V(I)). Then, f vanishes on V(I). By Hilbert's Nullstellensatz, there exist $m \geq 1 \ni f^m \in I$. But this means that $f \in \sqrt{I}$. Since f was arbitrary, I(V(I)) $\subseteq \sqrt{I}$. Therefore, I(V(I)) $= \sqrt{I}$.

Theorem 2.4.10 :(The Ideal -Variety Correspondence). Let K be an arbitrary field.

i) The maps

affine varieties $\xrightarrow{I}$ ideals

and

ideals $\xrightarrow{V}$ affine varieties

are inclusion reversing, that is, if $I_1 \subseteq I_2$ are ideals, then $V(I_1) \supseteq V(I_2)$ and similarly, if $V_1 \subseteq V_2$ are varieties, then $I(V_1) \supseteq I(V_2)$. Furthermore, for any variety V, we have V(I(V)) =V. So that I always one- to- one.

ii) If K is algebraically closed, and if we restrict to radical ideals, then the maps

affine varieties $\xrightarrow{I}$ radical ideals

and

radical ideals $\xrightarrow{V}$ affine varieties

are inclusion-reversing bijections which are inverses of each other.

Proof: i) First suppose $I_1 \subseteq I_2$, we claim that the map V is inclusion reversing.

By Hilbert Basis Theorem there exists $f_1,\ldots,f_s \in I_1$ and $g_1,\ldots,g_t \in I_2$ such that $I_1 =< f_1,\ldots,f_s >$ and $I_2 =< g_1,\ldots,g_t >$. Since $V(I_2)$ is the set of common roots of $g_1,\ldots,g_t \in I_2$, then $V(I_2)$ is the set of common roots of $f_1,\ldots,f_s \in I_1$, because $I_1 \subseteq I_2$. Hence, $V(I_1) \supseteq V(I_2)$.

Next, assume $V_1 \subseteq V_2$. We will show that, $I(V_1) \supseteq I(V_2)$. Since $V_1 \subseteq V_2$, then any polynomial vanishing on V_2 must vanish on V_1. Hence, $I(V_2) \subseteq I(V_1)$.

Finally, to prove V(I(V)) =V. If V=$V(f_1,\ldots.f_s)$ is a subvariety of K^n. Since every $f \in I(V)$ vanishing on V, then by definition of V we have, $V \subseteq V(I(V))$.

To see the other way, let $f_1,\ldots,f_s \in$ I(V). Thus, $< f_1,\ldots,f_s > \subseteq$ I(V) because I(V) is an ideal. Since V is inclusion reversing, then $V(I(V)) \subseteq V(< f_1,\ldots,f_s >) = V$. Therefore, V=V(I(V)), and consequently, I is one-to-one since it has a left inverse.

ii) Since I(V) is radical, we can think of I as a function which takes varieties to radical ideals. Furthermore, V(I(V)) =V for any variety V. We claim that, I(V(I)) =I whenever I is a radical ideal.

By Nullstellensatz since I(V(I))= $\sqrt{I}$ and I being radical, then $\sqrt{I}$ = I.

Hence, I(V(I)) =I. Thus, V and I are inverse of each other. Therefore, define bisections between the set of radical ideals and affine varieties.

As a consequence of this theorem, any question about varieties can be rephrased as an algebraic question about radical ideals (and conversely), provided that we are working over an algebraically closed field. This ability to pass between algebra and geometry will give us considerable power.

2.5 IRREDUCIBLE VARIETIES AND PRIME IDEALS

Definition 2.5.1: An affine variety $V \subseteq K^n$ is **irreducible** if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V = V_1$ or $V = V_2$.

Definition 2.5.2: An ideal $I \subseteq K[x_1,...,x_n]$ is **prime** if whenever $f, g \in K[x_1,...,x_n]$ and $fg \in I$, then either $f \in I$ or $g \in I$.

Proposition 2.5.3 Let $V \subseteq K^n$ be an affine variety. Then V is irreducible if and only if I(V) is a prime ideal.

Proof: $\Rightarrow$ assume that V is irreducible. We need to show that I(V) is a prime ideal.

Let fg$\in$ I(V). Set $V_1 = V \cap V(f)$ and $V_2 = V \cap V(g)$; these are affine varieties because an intersection of affine varieties is a variety. Then fg$\in$ I(V).

$\Rightarrow V = V_1 \cup V_2$ Since V is irreducible.

$\Rightarrow$ either $V = V_1$ or $V = V_2$, say $V = V_1 = V \cap V(f)$

$\Rightarrow$ f vanishes on V

So that f$\in$ I(V). Thus, I(V) is prime.

Conversely, assume that I(V) is prime and let $V = V_1 \cup V_2$. Suppose that $V \neq V_1$. We claim that I(V)= $I(V_2)$. Since $V_2 \subseteq V$, then $I(V) \subseteq I(V_2)$.

For the reverse inclusion, since $V_1 \subset V$.

$\Rightarrow I(V) \subset I(V_1)$

Thus, we can pick $f \in I(V_1) - I(V)$. Now take any $g \in I(V_2)$. Since $V = V_1 \cup V_2$, it follows that fg vanishes on V, and, hence, $fg \in I(V)$. But I(V) is prime;

so that f or g lies in I(V). Since $f \notin I(V)$, thus, $g \in I(V)$. This proves $I(V) = I(V_2)$, whence $V = V_2$ because I is one-to-one. Thus, V is an irreducible variety.

Corollary 2.5.4: When K is algebraically closed, the functions I and V induce a one-to-one correspondence between irreducible varieties in K^n and prime ideal in $K[x_1,...,x_n]$.

Definition 2.5.5: An ideal $I \subseteq K[x_1,...,x_n]$ is said to be **maximal** if $I \neq K[x_1,...,x_n]$ and any ideal J containing I is such that either J = I or $J = K[x_1,...,x_n]$.

Proposition 2.5.6: If K is any field, a maximal ideal in $K[x_1,...,x_n]$ is prime.

Proof: Suppose that I is a maximal ideal in $K[x_1,...,x_n]$ which is not prime.

$\Rightarrow$ there is $fg \in I$, where f$\notin$ I and $g \notin$ I

Consider the ideal <f> + I. Since $f \notin$ I, then $I \subset$ <f> + I. If 1 $\in$ <f> + I, then 1= cf +h for some $c \in K[x_1,...,x_n]$ and some $h \in$ I. Multiplying both sides by g, we get g = cfg+hg $\in$ I. This would contradict our choice of g.

Thus, I + <f> $\neq K[x_1,...,x_n]$

$\Rightarrow$ I is not maximal. Again this contradicts with our assumption.

Therefore, I is prime.

Theorem 2.5.7: If K is algebraically closed field, then every maximal ideal of $K[x_1,...,x_n]$ is of the form $< x_1 - a_1, x_2 - a_2,..., x_n - a_n >$ for some $a_1,...,a_n \in K$.

Proof: Let I$\subseteq K[x_1,...,x_n]$ be maximal. Since $I \neq K[x_1,...,x_n]$, $V(I) \neq \phi$ by the Weak Nullstellensatz.

$\Rightarrow$ there is some point $(a_1,...,a_n) \in$ V(I)

$\Rightarrow$ $f(a_1,...,a_n) = 0$ for every $f \in I$.

So that $f \in I(\{(a_1,...,a_n)\})$. Thus, $I \subseteq I(\{(a_1,...,a_n)\})$. We claim that $I(\{(a_1,...,a_n)\}) = < x_1 - a_1, x_2 - a_2,..., x_n - a_n >$.

Hence, if $I(\{(a_1,...,a_n)\})=< x_1-a_1, x_2-a_2,..., x_n-a_n >$, then

$I \subseteq < x_1-a_1, x_2-a_2,..., x_n-a_n >$. Hence, by the maximal condition I

$=< x_1-a_1, x_2-a_2,..., x_n-a_n >$

Let $f \in < x_1-a_1, x_2-a_2,..., x_n-a_n >$.

$\Rightarrow f = h_1(x_1-a_1)+...+h_n(x_n-a_n)$, for some $h_1,...,h_n \in K[x_1,...,x_n]$.

Thus, $f(a_1,...,a_n)=0$ where $(a_1,...,a_n) \in V(I)$.

$\Rightarrow f \in I(\{(a_1,...,a_n)\})$

$\Rightarrow < x_1-a_1, x_2-a_2,..., x_n-a_n > \subseteq I(\{(a_1,...,a_n)\})$.

To see the reverse inclusion assume that

$$I(\{(a_1,...,a_n)\}) \not\subset < x_1-a_1, x_2-a_2,..., x_n-a_n >$$

$\Rightarrow V(< x_1-a_1, x_2-a_2,..., x_n-a_n >) \not\subset V(I(\{(a_1,...,a_n)\}))$

$\Rightarrow (a_1,...,a_n) \not\subset (a_1,...,a_n)$ contradiction.

Thus, $I(\{(a_1,...,a_n)\}) \subseteq < x_1-a_1, x_2-a_2,..., x_n-a_n >$.

Therefore, $I(\{(a_1,...,a_n)\})=< x_1-a_1, x_2-a_2,..., x_n-a_n >$. We are finished.

Next, to show $< x_1-a_1, x_2-a_2,..., x_n-a_n >$ is maximal. Suppose that an ideal $J \supset I$. Then there exist $f \in J \ni f \notin I$. By the division algorithm $f = A_1(x_1-a_1)+...+A_n(x_n-a_n)+b$ for some $A_1,...,A_n \in K[x_1,...,x_n]$ and some $b \in K$. Since $A_1(x_1-a_1)+...+A_n(x_n-a_n) \in I$ and $f \notin J$, we must have $b \neq 0$. However, since $f \in J$ and since $A_1(x_1-a_1)+...+A_n(x_n-a_n) \in I \subseteq J$, we also have

$b = f-(A_1(x_1-a_1)+...+A_n(x_n-a_n)) \in J$.

Since $b \neq 0$, $\frac{1}{b} b \in J$, so $J = K[x_1,...,x_n]$.

Corollary 2.5.8: If K is an algebraically closed field, then there is a one- to-one correspondence between points of K^n and maximal ideals of $K[x_1,...,x_n]$.

Thus, we have extended our Algebra-Geometry dictionary. Over an algebraically closed field, every nonempty irreducible variety corresponds to a proper prime ideal and conversely. Every point corresponds to a maximal ideal, and conversely.

REFERENCES

[1] **David Cox, John Little, Donal O'Shea**. Ideal, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra, Second Edition, Springer Science+Business Media. Inc, 1997, 1992..

[2] **Jacob K**. Algebra, Goldhaber and Gertrude Ehrlich University of Maryland, the Macmillan Company 1970.

[3] **R.Y.Sharp.** Steps in commutative Algebra, Second Edition, London Mathematical Society Student Text 51, Cambridge University press 2000.