Integrated Science Education and Research Centre

Visva Bharati University

Project Report

Introduction to Algebraic Geometry

Amal M

Roll No: M.Sc.FY(Sem-X)-03

supervised by,

Dr. Swapan Kumar Pandit
Integrated Science Education and Research Centre, Visva Bharati University

Dr. S.N. Ojha
Integrated Science Education and Research Centre, Visva Bharati University

August 24, 2021

Abstract

We introduce the basic properties of affine and projective varieties including dimension of varieties, regular maps and morphism as well three proofs of Hilbert's Nullstellensatz.

Contents

Chapter 1

Introduction

1.1 Affine Spaces

Definition 1.1.1. Let A be a set and denote by $\vec{V}$ a vector space such that the additive group of the vector space $\vec{V}$ acts transitively and freely on the set A. Such a pair $(A, \vec{V})$ is known as an *affine space*.

Choose an element $a \in A$. Denote by $\alpha_a : \vec{A} \to A$ a map which takes $\vec{v} \mapsto a + \vec{v}$ where $\vec{v} \in \vec{V}$ and the $+$ denotes group action. The transitive property of group action means that the map α_a is surjective and the free action means α_a is injective. So $\vec{v} \mapsto a + \vec{v}$ is a bijective mapping.

Let $a, b \in A$. Since α_a is bijective we have a unique vector $\vec{v} \in \vec{A}$ such that $a + \vec{v} = b$. Denote by the subtraction $b - a$ such a unique vector $\vec{v}$.

Definition 1.1.2. An *affine subspace* B of A is a subset of A of the form $a + \vec{V} = \{a + \vec{w} : \vec{w} \in \vec{V}\}$ where $\vec{V}$ is a linear subspace of the vector space $\vec{V}$.

Definition 1.1.3. An *affine mapping or homomorphism* from the affine space A to another affine space B is the map

$$f : A \to B$$

along with a well-defined linear map

$$\vec{f} : \vec{A} \to \vec{B}$$

of their respective vector spaces such that $b - a \mapsto f(a) - f(b)$.

A bijective affine homomorphism is an affine isomorphism.

Theorem 1.1.4. *Let A and B be two affine spaces over the same vector space $\vec{A}$. The choice of any $a \in A$ defines a unique isomorphism $f : A \to B$ where $\vec{f} : \vec{V} \to \vec{V}$ is the identity map of $\vec{V}$. [2]*

Thus we see that up to affine isomorphism there is only one affine space associated with a vector space $\vec{V}$. Since for vector space $\vec{V}$, the set V of itself is an affine space $(v, \vec{V})$with $\vec{V}$ as an associated vector space, we can consider $\vec{V}$ itself as the affine space. For any other affine space A of $\vec{V}$, choose $a \in A$ and let the isomorphism map be $f : a \mapsto 0$. In this way we think of the affine space $\vec{V}$ as *forgetting* the position of the origin.

1.2 Projective Spaces

Let V be a vector space over a field k. We define an equivalence relation on $V \setminus \{0\}$ as,

$$x \sim y \text{ if there is a non zero element } \lambda \in k \text{ such that } x = \lambda y$$

Definition 1.2.1. The projective space $\mathbb{P}(V)$ is the set of equivalence classes of the vector space V excluding the origin.

Over the vector space k^{n+1} we have the projective space of n dimensions over k, $\mathbb{P}_n^k$. Every point P in $\mathbb{P}_n^k$ has the projective coordinates $[x_0 : \cdots : x_n]$ which is any element of the corresponding equivalence class. If $[x_0 : \cdots : x_n]$ is the projective coordinates for a point then $[\lambda x_0 : \cdots : \lambda x_n]$ is another coordinate as well for any nonzero $\lambda \in k$.

The projective space $\mathbb{P}_n^k$ can be thought of as the space obtained by adjoining the points at infinity to k^n. The advantage of using a projective space is that we don't have to constantly keep talking of two kinds of points, ie points at infinity and points in the vector space. We can treat them as the same in the projective space.

1.3 Noetherian Topological Spaces

Definition 1.3.1. A topological space is caled *noetherian* if it satisfies the *descending chain condition* for closed subsets: for any sequence $Y_1 \supseteq Y_2 \supseteq \cdots$ of closed sets, there is an integer r such that $Y_r = Y_{r+1} = \cdots$. Example, $\mathbb{A}^n$ is a noetherian topological space.

Definition 1.3.2. If X is a topological space, we define the dimension of X (denoted as dim X) to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$, where Z_i are irreducible closed sets.

Proposition 1.3.3. *In a noetherian topological space X, every nonempty closed subset Y can be expressed as a finite union $Y = Y_1 \cup \cdots Y_r$ of irreducible closed subsets Y_i. If we require that $Y_i \not\supseteq Y_j$ for $i \neq j$, then the Y_i are uniquely determined. They are called the irreducible components of Y.*

Corollary 1.3.4. *Every algebraic set in A^n can be expressed uniquely as a union of varieties, no one containing another.*

1.4 Irreducible Topological Spaces

Definition 1.4.1. A topological space X is irreducible if it is not the union of two proper closed subsets in Y.

Proposition 1.4.2. *Any non empty open subset of an irreducible topological space is dense and irreducible. If Y is a subset of a topological space X, which is irreducible in its induced topology, then the closure $\bar{Y}$ is also irreducible.*

Proposition 1.4.3. *The following conditions are equivalent for a topological space X:*

1. *X is noetherian*
2. *every nonempty family of closed subsets has a minimal element*
3. *X satisfies the ascending chain condition for open subsets*
4. *every nonempy family of open subsets has a maximal element.*

Proposition 1.4.4. *A noetherian topological space is* quasi-compact*, i.e, every open cover has a finite subcover. Any subset of a noetherian topological space is noetherian in its induced topology.*

1.5 Commutative Algebra, Reprise

Definition 1.5.1. A ring A is said to be *Noetherian* if it satisfies the following equivalent conditions:

1. Every non-empty set of ideals in A has a maximal element.
2. Every ascending chain of ideals in A is stationary.
3. Every ideal in A is finitely generated.

Proposition 1.5.2. *The following are equivalent, for a graded ring A:*

1. *A is a Noetherian ring.*
2. *A_0 is Noetherian and A is finitely generated as an A_0-algebra.*

Theorem 1.5.3. *(Hilbert's Basis Theorem) If R is a noetherian ring, so is $R[x]$.*

Proof. Consider the polynomials in $I \subseteq R[x]$ of degree n and let $I_n = (a_n^{(i)})_{i \in I}$, the ideal generated by $a_n^{(i)} \in R$, which are the leading coefficients of degree n polynomials over R. Then, $I_n \subset I_{n+1}$ (since we can multiply any polynomial of degree n by x to obtain a degree $n+1$ polynomial with the same leading coefficient). This gives an ascending chain of ideals in R that must stabilize since R is Noetherian:

$$I_0 \subset I_1 \subset \cdots \subset I_N = I_{N+1} = \cdots = I_\infty$$

Each I_j is finitely generated and thus we can pick a finite list of generators $g_i^{(j)}$ and we can choose a finite list of polynomials $p_i^{(j)}$ which have degree j with leading coefficient $g_i^{(j)}$. We now show that the finite list $\{p_i^{(j)}\}_{j=1}^N$ generates $I \subset R[x]$, by constructing and algorithm to express every polynomial in I as a linear combination of $p_i^{(j)}$s. Let $f \in I$ be some polynomial of degree n, so

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

Now a_n is in I_n, because it is a leading coefficient, so it can be expressed as a combination of $g_i^{(n)}$. Thus the combination of the corresponding $p_i^{(n)}$ gives us a polynomial g of degree n, which has the same leading coefficient as f. By construction, g and f are both in I, so $f - g$ is in I. But note that $f - g$ has a smaller degree than f, so repeating the argument above and using induction, we see that $f - g$ is generated by $p_i^{(j)}$s , so f is also generated by the $p_i^{(j)}$s. As a result, I is finitely generated, so $R[x]$ is Noetherian. [4] (Theorem 9.1). $\square$

Definition 1.5.4. A valuation ring is an integral domain D such that for every element x of its field of fractions F, at least one of x or x^{-1} belongs to D. Every valuation ring is a local ring

Definition 1.5.5. An artinian ring is a ring that satisfies the descending chain conditon on ideals. that is, there is no infinte descending sequence of ideals.

Definition 1.5.6. A proper ideal Q of a ring A is said to be primary if whenever $xy \in Q$ then x of y^n is in Q for some $n > 0$.

Definition 1.5.7. If Q is a primary ideal, then the radical of Q is necessarily a prime ideal P, and this ideal is called the associated prime ideal of Q. Q is then said to be P-primary.

Definition 1.5.8. Let M be a module over some ring R. Given a chain of submodules of M of the form

$$M_o \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

we say that n is the length of the chain. The length of M is defined to be the largest length of any of its chains. If no such largest length exists, we say that M has infinite length.

Definition 1.5.9. A ring R is said to have a finite length as a ring if it has finite length as a left R-module. Commonly length is denoted by ℓ. That is length of M is $\ell(M)$.

Definition 1.5.10. In a ring A, the height of a prime ideal $\mathfrak{p}$ is the supremum of all integers n such that there exists a chain $\mathfrak{p_o} \subset \mathfrak{p_1} \subset \cdots \subset \mathfrak{p_n} = \mathfrak{p}$ of distinct prime ideals. We define the dimension (or Krull dimension) of A to be the supremum of the heights of all prime ideals.

We say that a chain of prime ideals of the form $\mathfrak{p_0} \subsetneq \mathfrak{p_1} \subsetneq \cdots \subsetneq \mathfrak{p_n}$ has length n. The length is the number of strict inclusions.

Definition 1.5.11. The *Krull dimension* of a ring R is the supremum of the lengths of all chains of prime ideals in R.

Definition 1.5.12. Given a prime $\mathfrak{p}$ in R, we define the height of $\mathfrak{p}$, written $\mathrm{ht}(\mathfrak{p})$ to be the supremum of the length of all chains of prime ideals contained in $\mathfrak{p}$, that is

$$\mathfrak{p_0} \subsetneq \mathfrak{P_1} \subsetneq \cdots \subsetneq \mathfrak{p_n} = \mathfrak{p}$$

Definition 1.5.13. Alternatively, the height of $\mathfrak{p}$ is the Krull dimension of the localization of R at $\mathfrak{p}$.

Proposition 1.5.14. *A prime ideal has height zero if and only if it is a minimal prime idea.*

Proposition 1.5.15. *In a noetherian ring every prime ideal has a finite height.*

But there exists Noetherian rings of infinite Krull dimension.

Ex. A field k has a krull dimension 0. $k[x_1, \cdots, x_n]$ has dimension n. A PID has dim 1. A local ring has dim 0 if and only if every element of its maximal ideal is nilpotent.

Definition 1.5.16. A *graded ring* is a ring A together with a family $(A_n)_{n\geq 0}$ of subgroups of the additive group of A, such that $A = \bigoplus_{n=0}^{\infty} A_n$ and $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$. Thus A_0 is a subring of A (since $A_0 A_0 \subseteq A_0$), and each A_n is an A_0-module (since $A_0 A_n \subseteq A_n$). Eg. $A = k[x_1, \cdots, x_r], A_n =$ set of all homogeneous polynomials of degree n.

Think of every element of A_i as a *homogeneous element* of degree i. The condition $A_n A_m \subseteq A_{m+n}$ says that the product of two homogeneous elements of degree m and n is a homogeneous element of degree $m+n$. So we see that graded rings generalise the concept of homogenity over arbitary rings. (See Aluffi)

If A is a graded ring, a graded A-module is an A-module M together with a family $(M_n)_{n\geq 0}$ of subgroups of M such that $M = \bigoplus_{n=0}^{\infty} M_n$ and $A_m M_n \subseteq M_{m+n}$ for all $m, n \geq 0$. Thus each M_n is an A_0-module.

If $A = A_0$ that is the grading of the ring is concentrated in degree 0, then the compatibility condition says that each subgroup M_i is an A-module.

Definition 1.5.17. An element x of M is homogeneous if $x \in M_n$ for some n ($n =$ degree of x). Any element $y \in M$ can be written uniquely as a finite sum $\sum_n y_n$ where $y_n \in M_n$ for all $n \geq 0$, and all but a finite number of the y_n are 0. The non-zero components y_n are called the homogeneous components of y.

Definition 1.5.18. If M, N are graded A-modules, a homomorphism of graded A-modules is an A-module homomorphism $f : M \to N$ such that $f(M_n) \subseteq N_n$

for all $n > 0$. If A is a graded ring, let $A_+ = \bigoplus_{n>0} A_n$. Then A_+ is an ideal of A.

Definition 1.5.19. An ideal I of a graded ring $S = \oplus_i S_i$ is homogeneous if $I = \oplus_i (I \cap S_i)$

Lemma 1.5.20. *Let $S = \bigoplus_i S_i$ be a graded ring, and let $I \subseteq S$ be an ideal of S. Then the following are equivalent:*

1. *I is homogeneous;*
2. *If $s \in S$, and $s = \sum_i s_i$ is the decomposition of s into homogeneous elements $s_i \in S_i$, then $s \in I \Leftrightarrow s_i \in I$ for all i;*
3. *I admits a generating set consisting of homogeneous elements;*
4. *I is the kernel of a graded homomorphism*

A graded homomorphism $\varphi : S \to T$ induces a homormorphism of abelian groups $\varphi_i : S_i \to T_i$ for each i. The ideal ker φ is then the direct sum of all ker φ_i.

1.5.1 Associated Graded Ring

Definition 1.5.21. An infinite chain $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$ where the M_n are submodules of of M is called a filtration of M and is denoted by (M_n).

Definition 1.5.22. A filtration is an $\mathfrak{a}$-filtration if $\mathfrak{a}M_n \subseteq M_{n+1}$ for all n. It is called a stable $\mathfrak{a}-$filtration if $\mathfrak{a}M_n = M_{n+1}$ for all sufficiently large n. Thus $(\mathfrak{a}^n M)$ is a stable a-filtration.

Definition 1.5.23. Let A be a ring and $\mathfrak{a}$ an ideal of A. Define

$$G(A)\,(= G_{\mathfrak{a}}(A)) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}, \text{ where } (\mathfrak{a}^{\mathfrak{o}} = A)$$

this is a graded ring in which the multiplication is defined as follows: For each $x_n \in \mathfrak{a}^{\mathfrak{n}}$, let $\bar{x}_n$ denote the image of x_n in $\mathfrak{a}^{\mathfrak{n}}/\mathfrak{a}^{\mathfrak{n+1}}$; define $\bar{x}_m\bar{x}_n$ to be $\overline{x_m x_n}$, i.e., the image of $x_m x_n$ in $\mathfrak{a}^{\mathfrak{m+n}}/\mathfrak{a}^{\mathfrak{m+n+1}}$. $\bar{x}_m\bar{x}_n$ does not depend on the particular representative chosen.

Definition 1.5.24. Similarily, if M is an A-module and (M_n) is an $\mathfrak{a}$-filtration of M, define

$$G(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$$

which is a graded $G(A)$-module in a natural way. Let $G_n(M)$ denote M_n/M_{n+1}.

1.6 Ideals, Zero Sets and Varieties

Definition 1.6.1. Let $A = k[x_1, \cdots, x_n]$ be the polynomial ring in n variables over k. Let S be any subset of A. By the zero set of S we define

$$Z(S) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in S\}$$

If $\mathfrak{a}$ is an ideal generated by S, then $Z(S) = Z(\mathfrak{a})$.

By the Hilbert basis theorem, A is a noetherian ring which means that every ideal of A is finitely generated by say the elements $f_1, \cdots, f_r$. Therefore $Z(T) = Z(f_1, \cdots, f_r)$.

Definition 1.6.2. A subset Y of $\mathbb{A}^n$ is an algebraic set if there exists a subset $S \subseteq A$ such that $Y = Z(S)$.

Definition 1.6.3. *The Zariski Topology* on $\mathbb{A}^n$ is defined by taking as open sets, the compliments of algebraic sets.

Proposition 1.6.4. *The union of two algebraic sets is an algebraic set. The intersection of any family of algebraic sets is an algebraic set. The empty set and the whole space are algebraic sets.*

Using this result we can show that the Zariski Topology is indeed defined the way we say it is.

Definition 1.6.5. An *affine algebraic variety* is an irreducible closed subset of $\mathbb{A}^n$. An open subset of an affine variety is called a *quasi-affine variety.*

Definition 1.6.6. Analogous to the zero set, given an algebraic set Y we form the ideal of Y

$$I(Y) = \{f \in A : f(P) = 0 \text{ for all } P \in Y\}$$

Proposition 1.6.7.

1. *If $T_1 \subseteq T_2$ are subsets of A, then $Z(T_1) \supseteq Z(T_2)$.*
2. *If $Y_1 \subseteq Y_2$ are subsets of $\mathbb{A}^n$, then $I(Y_1) \supseteq I(Y_2)$.*
3. *For any two subsets Y_1, Y_2 of $\mathbb{A}^n$, we have $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.*
4. *For any ideal $\mathfrak{a} \subseteq A, I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$, the radical of $\mathfrak{a}$.*
5. *For any subset $Y \subseteq \mathbb{A}^n, Z(I(Y)) = \bar{Y}$, the closure of Y.*

Corollary 1.6.8. *There is a 1-1 inclusion-reversing correspondence between algebraic sets in $\mathbb{A}^n$ and radical ideals in A, given by $Y \mapsto I(Y)$ and $\mathfrak{a} \mapsto Z(\mathfrak{a})$. Furthermore an algebraic set is irreducible if and only if its ideal is prime.*

Proof. If Y is irreducible, we show that $I(Y)$ is prime. If $fg \in I(Y)$, then $Y \subseteq Z(fg) = Z(f) \cup Z(g)$. Thus $Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$, both being closed subsets of Y. Since Y is irreducible, we have either $Y = Y \cap Z(f)$, in which case $Y \subseteq Z(f)$, or $Y \subseteq Z(g)$. Hence either $f \in I(Y)$ or $g \in I(Y)$.

Conversely, let $\mathfrak{p}$ be a prime ideal, and suppose that $Z(\mathfrak{p}) = Y_1 \cup Y_2$. Then $\mathfrak{p} = I(Y_1) \cap I(Y_2)$, so eithr $\mathfrak{p} = I(Y_1) or \mathfrak{p} = I(Y_2)$. Thus $Z(\mathfrak{p}) = Y_1$ or Y_2, hence it is irreducible. [3] (Corollary 1.4) □

Definition 1.6.9. If $Y \subseteq \mathbb{A}^n$ is an affine algebraic set, we define the affine coordinate ring $A(Y)$ of Y to be $A/I(Y)$.

Proposition 1.6.10. *If Y is an affine variety, then $A(Y)$ is an integral domain. Furthermore, $A(Y)$ is a finitely generated k-algebra. Conversely any finitely generated k-algebra which is a domain is the affine cooridnate ring of some affine variety. Write B as the quotient of a polynomial ring $A = k[x_1, \cdots, x_n]$ by an ideal $\mathfrak{a}$ and let $Y = Z(\mathfrak{a})$.*

Let $S = k[x_0, \cdots, x_n]$ be a polynomial ring. We can consider S to be a graded ring by taking the elements of degree d as the set of all linear cominbations of monomial terms of total degree d. We generally cannot use whatever polynomial we please in the projective space. A homogeneous polynomials that vanishes at a point $P = (a_0, \cdots, a_n) \in \mathbb{A}^{n+1}$ vanishes at all points on that particualar equivalence class. Hence we can talk about the zero set of homogeneous polynomials, $Z(f) = \{P \in \mathbb{P}^n : f(P) = 0, f \in S\}$.

Definition 1.6.11. If T is any set of homogeneous polynomials of S then the zero set is defined as

$$Z(T) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in T\}$$

.

If $\mathfrak{a}$ is a homogeneous ideal of S, we define $Z(\mathfrak{a}) = Z(T)$, where T is the set of all homogeneous elements in $\mathfrak{a}$. Since S is a noetherian ring, any set of homogeneous elements T has a finite subset $f_1, \cdots, f_r$ such that $Z(T) = Z(f_1, \cdots, f_r)$.

Definition 1.6.12. A subset Y of $\mathbb{P}^n$i is an *algebraic set* if there exists a set T of homogeneous elements of S such that $Y = Z(T)$.

Definition 1.6.13. *The Zariski Topology* on $\mathbb{P}^n$ is defined by taking all the open sets to be the complements of algebraic sets.

Proposition 1.6.14. *The union of two algebraic sets is an algebraic set. The intersection of any family of algebraic sets is an algebraic set. The empty set and the whole space are algebraic sets.*

Definition 1.6.15. A *projective algebraic variety* is an irreducible algebraic set in $\mathbb{P}^n$ with the induced topology. An open subset of a projective variety is a *quasi-projective variety.* The dimension of a projective variety is defined as the dimension of a toplological space.

Definition 1.6.16. If Y is any subset of $\mathbb{P}^n$, define the homogeneous ideal of Y in S, denoted by $I(Y)$ as the ideal generated by $\{f \in S : f$ is homogeneous and $f(P) = 0$ for all $P \in Y\}$.

Definition 1.6.17. If Y is an algebraic set, define the homogeneous cooridnate ring of Y to be $S(Y) = S/I(Y)$.

Chapter 2

Affine Varieties

2.1 Regular Functions

First we consider the affine case.

Definition 2.1.1. Let Y be a quasi-affine variety. A function $f : Y \to k$ is said to be regular at a point x if it can be written as g/h in an open subset U of Y containing x where g, h are polynomials in $A = k[x_1, \cdots, x_n]$ such that h does not vanish on U. The function is said to be a *regular function* if it is regular on every such point x of Y.

That is a regular function is defined locally as a regular function (of polynomials).

Lemma 2.1.2. *A subset Z of a topological space Y is closed if and only if Y can be covered by open subsets U such that $Z \cap U$ is closed in U.*

Proof. Let U be an open subset in Y and assume that Z is closed. U can be divided by Z into two mutually exclusive subsets, $U \cap Z$ and $U \cap (Y - Z)$.

$U \cap (Y - Z)$ is the union of two open sets, hence is open in Y and therefore is open in U itself. Therefore it's compliment in U, $U \cap Z$ is closed in U.

Conversely, let U be an open set in Y and let U divide Z as before. Assume tht $U \cap Z$ is closed in U.

Therefore $U \cap (Y - Z)$ is open in U and therefore is open in Y as well. Let the open subsets U_i cover Y. Then the subsets $U_i \cap (Y - Z)$ which are open cover $Y - Z$ exactly. Which means as their union, $Y - Z$ is open and therefore we have that Z is closed. □

Proposition 2.1.3. *Regular functions on a quasi-affine variety are continuous if we identify k with $\mathbb{A}^1_k$.*

Proof. We will show that f^{-1} takes closed sets to closed sets. The affine line $\mathbb{A}^1_k$ has the Zariski Topology. Hence every closed set must necessarily be the zero set of some set of polynomials in one dimension over the field k. Therefore all closed sets in the Affine line are set of finite points. Hence we need only show that $f^{-1}(a)$ is closed when $a \in k$. We use the lemma 2.1.2. $\square$

Let U be an open set in Y and suppose $f = \frac{g}{h}$ on U.

$$f^{-1}(a) \cap U = \{x \in U : \text{where} \frac{g(x)}{h(x)} = a\}$$

Now this set is the same as the zero set of $g - ah)(x)$ on U. That is, $Z(g - ah) \cap U$. Hence it is closed in U itself satisfying the condition of 2.1.2. Therefore $f^{-1}(a)$ is closed and hence the regular function f is continuous.

Now we consider the case of quasi-projective varieties.

Let $h, g \in S = k[x_0, \cdots, x_n]$ are homogeneous polynomials of same degree. Then the rational function $\frac{g}{h}$ is defined on the projective space $\mathbb{P}^n$ when h does not vanish (See 2.1.4). Analogous to how we defined a rational function in the affine space we now consider the case of a quasi-projective variety Y.

Lemma 2.1.4. *If g, h are homogeneous polynomials of same degree in $k[x_0, \cdots, x_n]$ then the function $\frac{g}{h}$ is defined on $\mathbb{P}^n$ when $h \neq 0$.*

Proof. A homogeneous polynomial of degree d is a polynomial g such that $g(a\vec{x}) = a^d g(\vec{x})$ where $\vec{x} = (x_0, \cdots, x_n)$. Put $\vec{x'} = (x_0/x_n, \cdots, 1)$ in g and we get $g(\vec{x'}) = g(1/x^n \vec{x}) = \frac{1}{x_n^d} g(\vec{x})$, that is

$$g(\vec{x}) = x_n^d g(\vec{x'})$$

If h is another such homogeneous polynomial of degree d then

$$\frac{g(\vec{x})}{f(\vec{x})} = \frac{g(\vec{x'})}{h(\vec{x'})}$$

If we have that $\vec{x} \in \mathbb{P}^n$ then $\frac{g}{h}$ is defined on $\mathbb{P}^n$. $\square$

Definition 2.1.5. Let Y be a quasi-projective variety. A map $f : Y \to k$ is a rational function at a point $x \in Y$ if there exists an open subset U of Y which contains x and on U, $f = \frac{g}{h}$ such that h does not vanish on U. Furthermore, f is a *regular function* on Y if f is regular at each point x.

2.1.1 Morphisms

Let k be a fixed algebraic closed field. By a variety over k we mean any affine, quasi-affine, projective or quasi-projective variety.

Definition 2.1.6. A map $\varphi : X \to Y$ is a morphism from the variety X to Y when for each open subset $V \subseteq Y$ and every regular function $f : V \to k$ on V, the regular function formed by the composition of the two maps, $f \circ \varphi : \varphi^{-1}(V) \to k$ is a regular function.

Proposition 2.1.7. *Let X, Y and Z be three varieties with the morphisms $\varphi : X \to Y$ and $\phi : Y \to Z$ between them. We claim that the composition $\phi \circ \varphi : X \to Z$ is a morphism as well.*

Proof. To show that $\phi \circ \varphi$ is a morphism we have to show that for every open subset $V \subseteq Z$ and every regular function $f : V \to k$ the function $f \circ \phi \circ \varphi$ is a regular function. That is, $(\phi \circ \varphi)^{-1}(V) \to k$ is regular or $\varphi^{-1}(\phi^{-1}(V)) \to k$ is regular.

Since φ is a morphism, and say $g : \phi^{-1}(V) \to k$ is regular then $g \circ \varphi : \varphi^{-1}(\phi^{-1}(V)) \to k$ is regular. We ned $g : \phi^{-1}(V) \to k$ to be regular. So we look at ϕ which is a morphism. Hence our required g is $f \circ \phi : \phi^{-1}(V) \to k$. So we are done. $\square$

Now we are in a possition to define the category of varieties since we have morphisms which commute. We also have an isomorphims of varieties which are morphisms of variety $\varphi : X \to Y$ which admit an inverse morphims $\psi : Y \to X$ such that

$$\psi \circ \varphi = id_X$$

$$\varphi \circ \psi = id_Y$$

Such an isomorphims is both bijective and bicontinously, ie, the inverse map is continuous as well.

The affine charts $U_i \subseteq \mathbb{P}^n$ are open sets defined by the equation $x_i \neq 0$. The maps $\varphi_i : U_i \to \mathbb{A}^n$ is an isomorphism of varieties. Hence we can cover the projective space using affine spaces and study it that way.

2.1.2 Ring of Regular Functions

Definition 2.1.8. Given a variety Y by $\mathcal{O}(Y)$ we denote the ring of all regular functions on Y.

Consider a point $P \in Y$ and let U be any open subset of Y containing P let f be a regular function on U. We denote the pair of open subset and regular function on it as $\langle U, f \rangle$. For a fixed point P and two open subsets U and V on it, we can consruct an equivalence class by setting the condition that $\langle U, f \rangle \sim \langle V, g \rangle$ if and only if $f = g$ on $U \cap V$. Every such equivalence class is called a *germ*.

Lemma 2.1.9. *The condition that $\langle U, f \rangle \sim \langle V, g \rangle$ if and only if $f = g$ on $U \cap V$ defines an equivalence class.*

Definition 2.1.10. $\mathcal{O}_{P,Y}$ (also $\mathcal{O}_P$) is the ring of germs of all regular functions at P.

Proposition 2.1.11. *$\mathcal{O}_P$ is a local ring. And the residue field is $\mathcal{O}_P/\mathfrak{m} \cong k$*

Proof. The only maximal ideal of the ring $\mathcal{O}_P$ is $\mathfrak{m} = \{$ set of germs that vanish precisely at P $\}$. Since if $f(P) \neq 0, 1/f$ is regular in some neighborhood of P. $\square$

2.1.3 Function Field

Let Y be a variety and let U, V be open subsets of Y. Let f, g be regular functions on U and V respectively. If we let the equivalence relation be $\langle U, f\rangle \sim \langle V, f\rangle$ if and only if $f = g$ on $U \cap V$ then the set of equivalence classes forms a field which is called a function field.

Definition 2.1.12. $K(Y)$ is the *function field*. It is the set of equivalence classes given by this equivalence relation.

Lemma 2.1.13. *$K(Y)$ is a field.*

Upto isomorphism between varieties, the ring of regular functions $\mathcal{O}(Y)$, the local ring at a point P of Y, $\mathcal{O}_P$ and the function field $K(Y)$ are all invariants.

Proposition 2.1.14. *$\mathcal{O}(Y) \to \mathcal{O}_P \to K(Y)$, the maps are all injective.*

2.1.4 Regular functions and Coordinate Rings

Theorem 2.1.15. *[3] Let $Y \subseteq \mathbb{A}^n$ be an affine variety with affine coordinate ring $A(Y)$. Then*

1. *$\mathcal{O}(Y) \cong A(Y)$*
2. *for each point $P \in Y$, let $\mathfrak{m}_P \subseteq A(Y)$ be the ideal of functions vanishing at P. Then $P \mapsto \mathfrak{m}_P$ gives a one to one correspondence between the points of Y and the maximal ideals of $A(Y)$.*
3. *for each P, $\mathcal{O}_p \cong A(Y)_{\mathfrak{m}_P}$ and dim $\mathcal{O}_P =$ dim Y.*
4. *$K(Y)$ is isomorphic to the quotient field of $A(Y)$ and hence $K(Y)$ is a finitely generated extension field of k, of transcendence degree = dim Y.*

Proof. We will not give a proof for (4) right now.

The polynomial $f \in A = k[x_1, \cdots, x_n]$ defines a regular function on $\mathbb{A}^n$ and hence on Y. Therefore there is a homomorphism $A \to \mathcal{O}(Y)$ whose kernel is $I(Y)$. Therefore we get an injective homomorphism $\alpha : A(Y) = A/I(Y) \to \mathcal{O}(Y)$. Using (1.4) There is a 1-1 correspondence between points of Y that is minimal algebraic subsets of Y and maximals ideals of A containing $I(Y)$. α identifies elements of $A(Y)$ with regular functions on Y. Hence the maximal ideal corresponding to P is just $\mathfrak{m}_P = \{f \in A(Y) : f(P) = 0\}$. This proves (2).

For each P there is a natural map $A(Y)_{\mathfrak{m}_P} \to \mathcal{O}_P$. It is an injection because α is injective and it is surjective by definition of regular functions. Therefore $\mathcal{O}_P \cong A(Y)$

Now dim $\mathcal{O}_P =$ height $\mathfrak{m}_P$. Since $A(Y)/\mathfrak{m}_P \cong k$ we use (1.7) and (1.8A) to say that dim $\mathcal{O}_P =$ dim Y. This proves (3).

$\mathcal{O}(Y) \subseteq \bigcap_{P\in Y} \mathcal{O}_P$ where all our rings are regarded as subrings of $K(Y)$. Using (2) and (3) we have that

$$A(Y) \subseteq \mathcal{O}(Y) \subseteq \bigcap_{\mathfrak{m}} A(Y)_{\mathfrak{m}}$$

where $\mathfrak{m}$ runs over all maximal ideals of $A(Y)$.

Since if B is an integral domain, then B is equal to the intersection (inside its quotient field) of its localization at all maximal ideals.

The equality follows, hence (1) is proved.

$\square$

Chapter 3

Projective Varieties

Let S be a graded ring and $\mathfrak{p}$ be a homogeneous prime ideal in S. By $S_{(\mathfrak{p})}$ we denote the subring of elements of degree 0 the localisation of S with respect to the multiplicative subset T consisting of the homogeneous elements of S not in $\mathfrak{p}$. The ring of fractions $T^{-1}S$ has a natural grading $\deg(f/g) = \deg f - \deg g$ where f is homogeneous in S and $g \in T$. $S_{(\mathfrak{p})}$ is a local ring with maximal ideal $(\mathfrak{p} \cdot T^{-1}S) \cap S_{(\mathfrak{p})}$. If S is a domain, then for $\mathfrak{p} = (0)$ we obtain a field $S_{((0))}$. If $f \in S$ is a homogeneous element, we denote by $S_{(f)}$ the subring of elements of degree 0 in the localized ring S_f.

Theorem 3.0.1. *Let $Y \subseteq \mathbb{P}^n$ be a projective variety with homogeneous coordinate ring $S(Y)$. Then*

1. $\mathcal{O}(Y) = k$
2. *for any point $P \in Y$, let $\mathfrak{m}_P \subseteq S(Y)$ be the ideal generated by the set of homogeneous elements $f \in S(Y)$ such that $f(P) = 0$. Then $\mathcal{O}_P = S(Y)_{(\mathfrak{m}_P)}$.*
3. $K(Y) \cong S(Y)_{((0))}$

Proposition 3.0.2. *Let X be any variety and let Y be an affine variety. Then there is a natural bijective mapping of sets*

$$\alpha : Hom(X, Y) \xrightarrow{\sim} Hom(A(Y), \mathcal{O}(X))$$

where the left Hom means morphisms of varieties, and the right Hom means homomorphisms of k-algebras.

Corollary 3.0.3. *If X, Y are two affine varieties, then X and Y are isomorphic if and only if $A(X)$ and $A(Y)$ are isomorphic as k-algebras.*

In the language of categories,

Corollary 3.0.4. *The functor $X \mapsto A(X)$ induces an arrow-reversing equivalence of categories between the category of affine varieties over k and the category of finitely generated integral domains over k.*

Chapter 4

Proving Hilbert's Nullstellensatz

4.1 First Proof of the Nullstellensatz

In the theorem below (1) is *the* Nullstellensatz and (2) is generally considered to be the Weak Nullstellensatz.

Theorem 4.1.1. *Suppose k is algebraically closed field. The the following are both true and equivalent:*

1. *Given an ideal $J \subset \mathbb{A}_n^k$, we have $\sqrt{J} = I(V(J))$.*
2. *Given an ideal $J \subset \mathbb{A}_n^k$, we have the implication $(V(J)) = \emptyset \implies J = k[x_1, \cdots, x_n])$.*
3. *The maximal ideals of $k[x_1, \cdots, x_n]$ are exactly $J = (x_1 - a_1, \cdots, x_n - a_n), (a_1, \cdots, a_n) \in k^n$, with $k[x_1, \cdots, x_n]/J \cong k$.*

Proof. (1) $\implies$ (2). If $V(J) = \emptyset$, then (1) gives us $\sqrt{J} = I(V(J)) = I(\emptyset) = k[x_1, \cdots, x_n]$. However $1 \in \sqrt{J}$, and thus $1^n = 1 \in J$, or equivalently $J = k[x_1, \cdots, x_n]$.

(2) $\implies$ (1). This is called the *Rabinowitz Trick*.

(2) $\implies$ (3). Suppose $\mathfrak{m}$ is a maximal ideal of $A = k[x_1, \cdots, x_n]$. If $V(\mathfrak{m}) = \emptyset$ then (2) gives us that $\mathfrak{m} = A$. This is not possible since $\mathfrak{m}$ is maximal. Thus we have $V(\mathfrak{m}) \neq \emptyset$.

If $(a_1, \cdots, a_m) \in V(\mathfrak{m})$, then $I(V(\mathfrak{m})) \subseteq I(a_1, \cdots, a_m) = (x-a_1, \cdots, x-a_m)$ because I and V are inclusion reversing operations. We also know that $\mathfrak{m} \subseteq I(V(\mathfrak{m}))$. Combining these gives us that $\mathfrak{m} = (x - a_1, \cdots, x - a_m)$. Finaly, we find $(x - a_1, \cdots, x - a_m)$ is always maximal because $k[x_1, \cdots, x_n]/(x_1 - a_1, \cdots, x_n - a_n) \cong k$.

(3) $\implies$ (2). Suppose $V(J) = \emptyset$. Now if $J \subseteq (x_1 - a_1, \cdots, x_m - a_m) \in V(J) = \emptyset$. As this is not possible we deduce that $J \not\subseteq (x_1 - a_1, \cdots, x_n - a_n)$ for

any a_i, which with (3) implies that J is not in any maximal ideal. Therefore, we conclude J is the entire ring $k[x_1, \cdots, x_n]$. [4] (Theorem 10.4). $\square$

Lemma 4.1.2. *Suppose $f, g \in k[x_1, \cdots, x_n]$ with $g \neq 0$. Consider*

$$k[x_1, \cdots, x_n, y]/(yg - 1) = k[x_1, \cdots, x_n][1/g]$$

If $\bar{f} = 0$ giving an injection

$$k[x_1, x_2, \cdots, x_n] \hookrightarrow k[x_1, \cdots, x_n][1/g] \subset k(x_1, \cdots, x_n)$$

Proof. Suppose $f \equiv 0(\mod yg - 1)$ in $k[x_1, \cdots, x_n, y]$. Then f is a multiple of $(yg - 1)$ by some polynomial $g \in k[x_1, \cdots, x_n, y]$. But the only way this multiple has no y's in the expression is if $g = 0$. Thus $f = 0$ in $k[x_1, \cdots, x_n, y]$, and hence $k[x_1, \cdots, x_n]$. [4] (Lemma 10.5). $\square$

Corollary 4.1.3. *(Rabinowitsch Trick) The Weak Nullstellensatz implies the Nullstellensatz, or*

$$(V(J) = \emptyset \implies J = k[x_1, \cdots, x_n]) \implies I(V(J)) = \sqrt{J}$$

.

Proof. Clearly $\sqrt{J} \subset I(V(J))$. Now suppose g is any element in the ideal $I(V(J))$, and consider the augmented ideal

$$\hat{J} = J + (yg - 1) \subset k[x_1, \cdots, x_n, y]$$

By construction, $V(\hat{J}) = \emptyset \subset \mathbb{A}^{n+1}$, since if a point $(x_1, \cdots, x_n, y) \in V(\hat{J})$, then $(x_1, \cdots, x_n) \in V(J)$ and hence $g(x_1, \cdots, x_n) = 0$, a contradiction to $yg - 1 = 0$. By the weak Nullstellensatz, it follows that $\hat{J} = k[x_1, \cdots, x_n, y]$.

Let $f_1, \cdots, f_r$ generate J; from $1 \in \hat{J}$ we have

$$1 = \sum_{j=1}^{r} a_j f_j + b(yg - 1)$$

for some $a_j, b \in k[x_1, \cdots, x_n, y]$. Mod out by $yg - 1$:

$$1 \equiv \sum_{j=1}^{r} a_j f_j (\mod yg - 1)$$

Multiplying both sides by a huge power of g and substituting in $gy = 1$ (where we have multiplied by a large enough power of g so that all y's are eliminated from the expression), we get:

$$g^N = \sum_{j=1}^{r} a_j(x_1, \cdots, x_{n+1}, g) f_j \in k[x_1, \cdots, x_n, y]/(yg - 1)$$

. By Lemma 4.1.2 we have

$$g^N = \sum_{j=1}^{r} a_j(x_1, \cdots, x_{n+1}, g) f_j \in k[x_1, \cdots, x_n]$$

so indeed $g \in sqrtJ$. [4] (Corollary 10.6). $\square$

4.2 Second Proof of the Nullstellensatz

Lemma 4.2.1. *(Zariski's Lemma) Suppose the field K is finitely generated as an algebra over the field k, then it is finitely generated as a module.*

We first prove the Weak Nullstellensatz for all algebraically closed fields.

Proposition 4.2.2. *(Weak Nullstellensatz) The maximal ideals of $k[x_1, \cdots, x_n]$ are exactly the ideals $(x_1 - a, \cdots, x_n - a)$*

Proof. Let k be an algebraically closed field and $\mathfrak{m}$ a maximal ideal. Then the field $k[x_1, \cdots, x_n]/\mathfrak{m}$ is finitely generated as a module over k by Zariski's Lemma 4.2.1. So it is k itself as k is algebraically closed. So each $x_i = a_i \mod m$ where $a_i \in k$. Hence $\mathfrak{m} \subseteq (x_1 - a_1, x_2 - a_2, \cdots)$. $\square$

Theorem 4.2.3. *(Strong Nullstellensatz) $I \subseteq k[x_1, \cdots, x_n]$ and V is the zero set. Then,*

$$f = 0 \text{ on } V \Leftrightarrow f^k \in I \text{ for some } k$$

Corollary 4.2.4. *If $f : A \to B$ is a homomorphism of finitely generated algebras (ie, f.g as algebras) over k. Then*

$$f^{-1}(\textit{maximal ideal}) = \textit{maximal}.$$

Proof. Let $A \to B$, let $\mathfrak{m}$ be a maximal ideal in B. We have the injective mapping

$$k \subseteq A/f^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$$

. $B/\mathfrak{m}$ is a finitely generated k-module by Zariski's Lemma 4.2.1 since it is a finitely generated k-algebra.

We use here the result that any subalgebra of a finite extension of a field k is also a field. Now $B/\mathfrak{m}$ is a finite extension of k and $A/f^{-1}(m)$ is contained in it. Hence $A/f^{-1}(\mathfrak{m})$ is a field. Therefore $f^{-1}(\mathfrak{m})$ is maximal.

$\square$

Theorem 4.2.5. *Weak Nullstellensatz $\implies$ Strong Nullstellensatz.*

Proof. Let $I \subseteq k[x_1, \cdots, x_n]$ be an ideal and let $f = 0$ on V, the zero set of I in k^n. We look at the polynomial ring $k[x_1, \cdots, x_n, f^{-1}]$. Notice that the maximal ideals of $k[x_1, \cdots, x_n]$ are contained in the maximal ideals of $k[x_1, \cdots, x_n]$ of the form $(x_1 - a_1, \cdots, x_n - a_n)$.

The maximal ideals of the localisation $k[x_1, \cdots, x_n, f^{-1}]$ are such that they are maximal ideals of $k[x_1, \cdots, x_n]$ but such that $f \notin$ maximal ideals which we think of informally as saying that "$f \neq 0$" at the maximal ideal. So $I[f^{-1}]$ which is an ideal of the localisation is not in any maximal ideal of $k[x_1, \cdots, x_n, f^{-1}]$ because the only maximal ideal $I[f^{-1}]$ can be contained in corresponds to points where f vanishes and f^{-1} can't be in the corresponding maximal ideal. So it is the whole ring, so $f \in I[f^{-1}]$ where $I[f^{-1}] = \{i/f^k, k \geq 1\}$. This is the same as saying that $f^k = i$ for some $i \in I$ implies $f^k \in I$ which is exactly the strong Nullstellensatz.

$\square$

4.3 Third Proof of the Nullstellensatz

The third proof of the Nullstellensatz uses Noether Normalization.

Theorem 4.3.1. *If k is a field then dim $k[x_1, \cdots, x_r] = r$*

Lemma 4.3.2. *Suppose that k is a field and that $f \in T = k[x_1, \cdots, x_r]$ is a non constant polynomial. There are elements $x'_1, \cdots, x'_{r-1} \in T$ such that T is a finitely generated module over the k-subalgebra generated by $x'_1, \cdots, x'_{r-1}$ and f. Also: (c) (Noether): If k is infinite then for some (in fact, for any sufficiently general) $a_i \in k$ we may choose $x'_i = x_i - a_i x_r$.*

Theorem 4.3.3. *(Noether Normalisation) Let R be an affine ring of dimension d over a field k. If $I_1 \subset \cdots \subset I_m$ is a chain of ideals of R with dim $I_j = d_j$ and $d_1 > d_2 > \cdots > d_m > 0$ then R contains a polynomial ring $S = k[x_1, \cdots, x_d]$ in such a way that k is finitely generated S-module and*

$$I_j \cap S = (x_{d_{j+1}}, \cdots, x_d), \text{ for } j = 1, \cdots, m$$

If the ideals I_i are homogeneous, then the x_i may be chosen to be homogeneous. In fact, if k is infinite, and R is generated over k by $y_1, \cdots, y_r$, then for $j \leq d_m$ the elements x_j may be chosen to be a k-linear continuation of the y_i.

Now we give the Nullstellensatz as a corollary of this theorem.

Corollary 4.3.4. *(Hilbert's Nullstellensatz) Let R be an affine ring over a field k and let $P \subset R$ be a prime.*

1. *If P is maximal, then R/P is a finite field extension of k.*
2. *P is the intersection of maximal ideals of R*

Proof.

1. By Theorem 4.3.3, the 0-dim affine ring R/P is a finitely generated module over the polynomial ring over k in $d = 0$ variables. This is, R/P is a finite dimensional vector space over k.
2. If $f \in R - P$, we must find a maximal ideal of R containing P but not containing f. Factoring out P, we may assume $P = 0$. Let $S = k[x_1, \cdots, x_d] \subset R$ be a polynomial ring satisfying Theorem 4.3.3 with $I_1 = (f)$. Since dim $R/(f) = d$, we have $(f) \cap S - (x_1)$. There exists a prime $\mathfrak{p}$ of R lying over the maximal ideal $\mathfrak{m} = (x_1 - 1, x_2, \cdots, x_d) \subset S$, and we claim that $\mathfrak{p}$ has the desired properties. Since $\mathfrak{m}$ is a maximal ideal, $\mathfrak{p}$ is maximal and $\mathfrak{p}$ cannot contain f, since $\mathfrak{m}$ would then contain x_1 and with it 1.

□

Acknowledgement

I would like to thank my mentor Dr. Swapan Kumar Pandit as well as Dr. Saurav Bhaumik (IIT-B) for their valuable guidance without which this project would have been impossible. Dr. Saurav Bhaumik acted informally as my advisor for this project. I would like to thank Dr. S.N. Ohja for agreeing to be my external advisor. Furthermore, I would like to thank Dr Mahasweta Nandi for her work behind the scenes organising the project presentation as well as managing the dessertation work for our batch.

Bibliography

[1] Affine space. Encyclopedia of Mathematics. URL: http://encyclopediaofmath.org/index.php?title=Affine_space&oldid=45147

[2] Affine space. Wikipedia. URL: https://en.wikipedia.org/wiki/Affine_space

[3] Algebraic Geometry. Robin Hartshorne.

[4] Math 145: Algebraic Geometry. Ravi Vakil.

[5] Introduction to Commutative Algebra. M. F. Atiyah, I. G. MacDonald

[6] Commutative Algebra Lectures. Richard Borcherds. URL: https://www.youtube.com/playlist?list=PL8yHsr3EFj53rSexSz7vsYt-3rpHPR3HB