On Bezout's Theorem

A thesis submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

Thesis Supervisor: Rabeya Basu

by
Anuj Kumar More
April, 2012

Indian Institute of Science Education and Research Pune
Sai Trinity Building, Pashan, Pune India 411021

This is to certify that this thesis entitled "On Bezout's Theorem" submitted towards the partial fulfillment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research Pune, represents work carried out by Anuj Kumar More under the supervision of Rabeya Basu.

Anuj Kumar More

Thesis committee:
Rabeya Basu

A. Raghuram
Coordinator of Mathematics

Acknowledgments

I express my deep gratitude to my supervisor Dr. Rabeya Basu for her guidance and moral support through out the project. I would like to thank Professor S. M. Bhatwadekar for his invaluable time and effort. His series of lectures on Bezout's Theorem and personal discussions on basic commutative algebra were very helpful for me in understanding the subject. My sincere appreciation also goes to Professor Raja Sridharan for inspiring me to pursue this area of mathematics. I thank all faculties of IISER Pune for the excellent course work given by them during first four years. I would like to thank my seniors and batchmates especially Manvendra Sharma for being with me all the time when I needed them through these five years of my life. Words cannot express my gratitude to my parents and brother, who have fulfilled all my needs.

Abstract

On Bezout's Theorem

by Anuj Kumar More

The aim of the project is to understand Bezout's Theorem for curves from algebraic and geometric point of view. The Theorem states that in complex projective plane, the number of points in which any two curves (with no common factors) intersect, counting with multiplicity, is the product of the degrees of the curves. We follow the proof given in the book "Algebraic Curves" by William Fulton. In the appendix, we have included solutions of few problems from the book. Basics of commutative algebra are learnt along with for understanding the subject.

Contents

Chapter 1

Introduction

Algebraic geometry originated with the study of solutions of system of polynomial equations. It was observed long back that conic sections can be described as the set of solution of a particular polynomial in two variables. In this thesis I have studied one of the most fundamental theorem of algebraic geometry viz. Bezout's Theorem, which has enormous applications in algebraic geometry.
To give some motivation let us consider the affine plane $\mathbb{A}^2$. A **curve** in $\mathbb{R}^2$ is the graph of a polynomial equation in two variables x and y. It is finite sum of terms of the form ex^iy^j, where the coefficient e is a real number and the exponents i and j are nonnegative integers. We will look at the points where a curve intersect another curve. Point to note is that it can intersect the curve multiple times. For example, we consider the equation

$$(x^2 + y^2)^2 - 2xy = 0$$

(as in figure 1.1). It intersects the curve $y =\ 0$ and $x = 0$ (x and y axis) twice at the origin.

Geometrically, it is not always possible to look at the graphs of f and g and find the

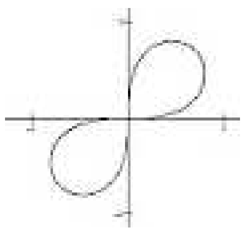

Figure 1.1:

number of times they intersect at some point. To overcome this problem we study so called projective space over complex plane $\mathbb{C}^2$. We consider the curve in $\mathbb{P}^2$ instead of $\mathbb{A}^2$. In affine plane we have the concept of parallel lines. So, they never intersect each other. For example, we have two parallel lines $X + Y = 0$ and $X + Y - 1 = 0$ in $\mathbb{A}^2$. On the other hand in $\mathbb{P}^2$, there are no parallel lines, since any two distinct lines $aX+bY+cZ = 0$ and $\alpha X+\beta Y+\gamma Z = 0$ meet at the point $(b\gamma-c\beta, c\alpha-a\gamma, a\beta-b\alpha)$. Infact, any two curves in $\mathbb{P}^2$ intersect each other.

Statement of Bezout's Theorem:

Any two distinct curves, f and g, on the projective plane, of degree m and n respectively, will meet in exactly mn points, counting multiplicities.

Etienne Bezout proved this result in his Ph.D. thesis in 1779 in Paris. According to historical notes, the earlier version of the result originated in the remarks of Newton and MacLaurin and was already proved by Euler in 1748 and Cramer in 1750.

In this thesis we give a proof of the result following the book "Algebraic Curves" by William Fulton. We use the concept of "Intersection Theory". At the beginning we provide some basic concepts of commutative algebra and algebraic geometry to keep it self content. Then in the consecutive sections we study Lemmas and Propositions which are ingredients for the proof of the Theorem. At the end of the thesis we include some solutions of problems in Fulton's book.

Chapter 2

Preliminary

2.1 Basic Commutative Algebra

Definition 1. A *ring* R is a set with two binary operations (addition $+$ and multiplication .) such that R is an abelian group with respect to addition and multiplication is associative and distributive over addition.

Through out this thesis we will be considering R to be commutative ring ($xy = yx$ for all $x, y \in R$) with identity ($\exists!\ 1 \in R$ such that $x1 = 1x = x\ \forall x \in R$). A ring R is called **integral domain** if $ab = 0 \Rightarrow a = 0$ or $b = 0$ $a, b \in R$. The characteristic of R, denoted by $char(R)$, is the smallest integer p such that $1 + \cdots + 1$ (p times) $= 0$, If such a p exists we say R has characteristic p; otherwise $char(R) = 0$. $Char(R)$ is a prime number or 0.

Just like the concept of vector spaces over field, we have analogue concept of **modules** over rings. A left R-Module M is an abelian group together with a map $f : R \times M \to M$ given by $(a, x) \to a \cdot x$, satisfying (1) $a \cdot (x + y) = a \cdot x + a \cdot y$, (2) $(a + b) \cdot x = a \cdot x + b \cdot x$, (3) $a(b \cdot x) = (ab) \cdot x$ and (4) $1 \cdot x = x$ for all $a, b \in R$ and $x, y \in M$.
Any vector space V over a field k can be considered as k-module V. Any abelian group G is a $\mathbb{Z}$-module.

Definition 2. An *ideal* I of a ring R is an additive subgroup of R such that $RI \subseteq I$.

Definition 3. A mapping $\phi : R \to S$ is called **ring homomorphism** from a ring R to a ring S if and only if $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ $(a, b \in R)$. If

ϕ is $1-1$ and onto, then it is called **ring isomorphism**.

The set of elements mapped to $0 \in S$ is called **kernel** of ϕ denoted as $Ker(\phi)$ and it is an ideal of R.

Definition 4. Quotient Ring: If I is an ideal of ring R, then the collection of cosets $\{x+I \mid x \in A\}$ form a ring under the induced operation from A, i.e. $((x+I)+(y+I) = (x+y)+I$ and $(x+I).(y+I) = (x.y+I))$. This ring is quotient ring (also called **factor ring** or **residue class ring**) denoted by R/I and element $(x+I)$ (called I-residue of x) is denoted as $\bar{x}$.

The classes R/I forms a ring in such a way that the mapping $\pi : R \to R/I$ taking x to I-residue of x is ring homomorphism.
R/I is characterized by the following property: If $\phi : R \to S$ is a ring homomorphism to a ring S and $\phi(I) = 0$, then there is a unique ring homomorphism $\bar{\phi} : R/I \to S$ such that $\phi = \bar{\phi} \circ \pi$.

Definition 5. An ideal I in A is ***prime*** if and only if $I \neq (1)$ and $xy \in I \implies x \in I \text{ or } y \in I$.

I is a prime ideal of A if and only if A/I is an integral domain. The set of all prime ideals of A is denoted by $\mathrm{Spec}(A)$.

Definition 6. An ideal I in A is ***maximal*** if and only if $I \neq A$ and there is no ideal J such that $I \subset J \subset A$.

I is a maximal ideal of A if and only if A/I is a field. The set of all maximal ideals of A is denoted by $Max(A)$ and it is a subset of $\mathrm{Spec}(A)$.
Two ideal I and J are said to be ***comaximal*** if $I + J = R$

Definition 7. A ring is said to be **local** if it has a unique maximal ideal and **semilocal** if it has finitely many maximal ideals.

Definition 8. I be an ideal of A. The set $I = \{x \in A \mid \exists n \in \mathbb{N} \ s.t. \ x^n \in I\}$ is an ideal of A and is called as *radical* of I denoted by $\sqrt{I}$.

The ideal $\sqrt{0}$ is called the **nilradical** of A.

Proposition 2.1.1. *The nilradical of A is the intersection of all prime ideals of A.*

Definition 9. The ***jacobson radical*** of A is the intersection of all the maximal ideals of A denoted by $Jac(A)$.

Lemma 2.1.2. Prime Avoidance Lemma : *Let A be a ring and $I \subset A$ an ideal. Suppose $I \subset \cup_{i=1}^{n} P_i$, where $P_i \in \operatorname{Spec}(A)$. Then $I \subset P_i$ for some i, $1 \leq i \leq n$.*

Proof. Use induction on n. Trivially true for $n = 1$. We assume the statement to be true for $n-1$, i.e. $I \subset \cup_{i=1}^{n-1} P_i \Rightarrow I \subset P_i$ for some i $(1 \leq i \leq n-1)$. We assume $I \subset \cup_{i=1}^{n} P_i$. If I is contained in union of any $(n-1)$ prime ideals, we can use induction hypothesis. If not, $I \not\subseteq \cup_{j\neq i} P_j$ for all i, i.e. $\exists\ a_i \in I$ such that $a_i \notin \cup_{j\neq i} P_j$ for all i $(1 \leq i \leq n)$. If for some i, $a_i \notin P_i$,then $I \not\subseteq \cup_{i=1}^{n} P_i$. So we assume that $a_i \in P_i$ for all i. Then the element

$$a = \sum_{i=1}^{n} a_1 \ldots a_{i-1} \cdot a_{i+1} \ldots a_n$$

is an element of I not in $\cup_{i=1}^{n} P_i$. Contradiction. □

Lemma 2.1.3. Nakayama Lemma : *A ring, M a finitely generated A-module and I be an ideal of A. Then $IM = M \implies \exists\ a \in I$ such that $(1 + a)M = 0$.*

Proof. Let M be generated by $\{x_1, \ldots, x_n\}$. $IM = M \Rightarrow x_i = \sum_{j=1}^{n} a_{ij} x_j$, $a_{ij} \in I \Rightarrow \sum_{j=1}^{n} (\delta_{ij} - a_{ij}) x_j = 0$, where $\delta_{ij} = 1$ if $i = j$ and 0 if $i \neq j$. This implies that

$$\begin{pmatrix} 1-a_{11} & -a_{12} & -a_{1n} \\ -a_{21} & 1-a_{22} & -a_{2n} \\ -a_{n1} & \cdots & 1-a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

If Δ is the determinant of the matrix $(\delta_{ij} - a_{ij})$, then by multiplying by its adjoint on the left, we get $\Delta x_i = 0$, $1 \leq i \leq n$. Thus, $\Delta M = 0$. Also $\Delta = 1 + a$, for some $a \in I$. Thus, $(1 + a)M = 0$. □

If I is a maximal ideal of A then $IM = M \implies M = 0$.

Definition 10. ***Polynomial rings***: Let A be a ring. The ring $A[X_1, \ldots, X_n]$ denotes the polynomial ring in n variables $X_1, \ldots, X_n$ over R and consists of elements of the type

$$f = \sum_{i=1}^{n} \lambda_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

where $\lambda_{i_1 \dots i_n} \in A$ and $\{i_1, \dots, i_n\} \in \mathbb{Z}_+^n$.

Element f of the polynomial ring is called a **polynomial**, which is finite $A-$linear combination of $X_1^{i_1} \dots X_n^{i_n}$ (called **monomials**). Degree of a monomial is the sum of powers of each X_i's, i.e. $i_1 + \dots + i_n$. A polynomial which is A-linear combination of monomials of degree d is called **homogeneous polynomial** of degree d. Any polynomial can be written as sum of finitely many homogeneous polynomials. The **degree** of a polynomial is define to be the maximum of the degree of its homogeneous components.

Definition 11. Let A be a ring. An A-module M is called **Noetherian** if it satisfies one of the following conditions (all are equivalent):

1. Any non empty collection of submodules of M has a maximal element.
2. Any ascending chain of submodules of M has a maximal element.
3. Every submodule of M is finitely generated.

A ring A is said to be *Noetherian* if A is Noetherian as an A-module. Fields and PIDs are Noetherian.

Proposition 2.1.4. *A ring, M an A-module, and N an A-submodule of M. Then M is Noetherian if and only if N and M/N are Noetherian.*

Definition 12. A nonzero element a of an integral domain R with unity is called an **irreducible** element if (1) it is not a unit, and (2) for any factorization $a = bc$, $b, c \in R$, either b or c is a unit.

Definition 13. A nonzero element p of an integral domain R is called a prime element if (1) it is not a unit and (2) if $p|ab$, then $p|a$ or $p|b$. $(a, b \in R)$.

A set S of elements of a ring R **generates** an ideal $I = \{\sum a_i s_i \mid s_i \in S,\ a_i \in R\}$. I is said to be **finitely generated** if S is a finite set and is said to be **principal** if S is singleton set.

Definition 14. A domain in which every ideal is principal is called Principal Ideal Domain.

Example of PIDs are $\mathbb{Z}$ and $k[X]$, where k is a field.

Definition 15. A commutative integral domain R with unity is called **unique factorization domain** (UFD) if every nonzero element in R can be factored uniquely, up to units and the ordering of the factors, into irreducible factors.

Example of UFDs are $\mathbb{Z}$, polynomial ring $R[X_1, \ldots, X_n]$, where R itself is a UFD. Every PID is a UFD but converse is not true ($k[X, Y]$ is not a PID as $I = (x, y)$ is not generated by single element).

Definition 16. Let R be a ring. The **quotient field** (or Field of fractions) K of the ring R is the field consisting of all elements of the form a/b, where $a, b \in R$ and $b \neq 0$.

The quotient field of polynomial ring $k[X_1, \ldots, X_n]$ is written as $k(x_1, \ldots, x_n)$ and is called **field of rational functions** in n variables over the field k.

Lemma 2.1.5. ***Gauss's Lemma:*** *Let R be a UFD with field of fractions F, then any irreducible element $F \in R[X]$ remains irreducible when considered in $K[X]$.*

Proof. Let $F \in K[X]$ be reducible element, i.e. $F = GH$, where G, H are in $k[X]$. Multiplying by a common denominator we can obtain $dF = G'H'$, where G', H' are elements in $R[X]$ and d is a nonzero element in R. If d is unit, then $F = (d^{-1}G')(H')$ is reducible. If d is not a unit, then $d = p_1 \ldots p_n$ (product of irreducibles). Now, p_1 is irreducible, then ideal (p_1) is prime (true for PIDs). Thus, $(R/p_1R)[X]$ is integral domain. Taking modulo p_1, we get $dF = G'H'$ modulo $p_1 \Rightarrow \bar{0} = \bar{H}'\bar{G}' \Rightarrow \bar{H}' = \bar{0}$ or $\bar{G}' = \bar{0}$. This means all the coefficients of H' or G' are divisible by p_1. So, we can cancel p_1 from both sides of $dF = G'H'$. But now the factor d has fewer irreducible factors. Preceding in the same fashion with each of the remaining factors of d, we can cancel all of the factors of d into two polynomials on the right hand side, leaving the equation $F = G'H'$ with $G', H' \in R[X] \Rightarrow F$ is reducible. $\square$

If R is a ring, $a \in R$, $F \in R[X]$. Then a is called ***root*** of F if $F = (x - a)G$ for a unique $G \in R[X]$.

Definition 17. A field k is **algebraically closed field** if any non constant $F \in k[X]$ has a root.

$\mathbb{C}$ is an algebraically closed field. Any polynomial of degree d in algebraically closed field k has d roots in k, counting multiplicities.

Definition 18. The **derivative** of a polynomial $F = \sum a_i X^i \in R[X]$ is defined to be $\sum i a_i X^{i-1}$ and is denoted by $\frac{\partial F}{\partial X}$ or F_X.

If $F \in R[X_1, \ldots, X_n]$, $\frac{\partial F}{\partial X_i} = F_{X_i}$ is defined by considering F as a polynomial in X_i with coefficients in $R[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.

2.2 Chinese Remainder Theorem

Theorem 2.2.1. *Let $I_1, \ldots, I_k$ be pairwise comaximal ideals in ring R. The map*

$$R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

$$r \to (r + I_1, r + I_2, \ldots, r + A_k)$$

is a surjective ring homomorphism with kernel $\bigcap_{k=1}^{n} I_k = I_1 I_2 \ldots I_n$.

Proof. We first prove for $n = 2$. We consider the natural projection map $\phi : R \to R/I_1 \times R/I_2$ defined by $\phi(r) = (r + I_1, r + I_2)$. This is a ring homomorphism. Kernel of ϕ consists of all elements of R that are in $I_1 \cap I_2$. Since $I_1 + I_2 = R$, there exist elements $x \in I_1$ and $y \in I_2$ such that $x + y = 1$. This equation shows that $\phi(x) = (0, 1)$ and $\phi(y) = (1, 0)$ (0 and 1 are elements of R/I_1 and R/I_2). Now, if $(r_1 + I_1, r_2 + I_2)$ is an arbitrary element in $R/I_1 \times R/I_2$, then element $r_2 x + r_1 y$ maps to this element as

$$\begin{aligned}
\phi(r_2 x + r_1 y) &= \phi(r_2)\phi(x) + \phi(r_1)\phi(y) \\
&= (r_2 + A, r_2 + B)(0, 1) + (r_1 + A, r_1 + B)(1, 0) \\
&= (0, r_2 + B) + (r_1 + A, 0) \\
&= (r_1 + A, r_2 + B)
\end{aligned}$$

Thus ϕ is surjective.
We claim that $I_1 I_2 = I_1 \cap I_2$. $I_1 I_2 \subset I_1 \cap I_2$. Also, for any $c \in I_1 \cap I_2$, $c = c \cdot 1 = cx + cy \in I_1 I_2$ (x and y are as above). Thus, $I_1 \cap I_2 \subset I_1 I_2$ implying $I_1 \cap I_2 = I_1 I_2$.
The general case follows by induction. We assume the statement to be true up to $(k-1)$ ideals. Take ideal $A = I_1$ and $B = I_2 I_3 \ldots I_k$. Claim is that A and B are comaximal. Given that $\forall\ i \in \{2, 3, \ldots, k\}$, there are elements $x_i \in I_1$ and $y_i \in I_i$ such that $x_i + y_i = 1$. Now, $1 = (x_2 + y_2) \ldots (x_k + y_k) \in A + B$. Thus, A and B are

comaximal. Now, we can apply the case for $n = 2$, i.e. $A \cap B = AB = \prod_{i}^{n} I_i$ to get the result. $\square$

2.3 Hilbert Basis Theorem

Theorem 2.3.1. Hilbert Basis Theorem : *Let R be a Noetherian ring. Then $R[X_1, \ldots, X_n]$ is Noetherian.*

Proof. Since $R[X_1, \ldots, X_n]$ is isomorphic to $R[X_1, \ldots, X_{n-1}][X_n]$, we can use mathematical induction. So problem suffices to: If R is Noetherian then $R[X]$ is Noetherian.

Let $I \subset R[X]$ be an ideal. To show that I is finitely generated. Let us choose $f_1(X) \in I$ of smallest degree. If $I = \langle f_1(X) \rangle$, then done. If not, choose $f_2(X) \in I$ such that $f_2(X)$ is not in $\langle f_1(X) \rangle$ and is of smallest degree w.r.t. that property. Proceeding this way, we can choose $f_i(X)$ for $i > 0$. Let a_i be leading coefficient of $f_i(X)$. Since R is Noetherian, the chain

$$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \ldots \subset \langle a_1, \ldots, a_r \rangle \subset \ldots$$

terminate for some $n \in \mathbb{N}$.

We claim $I = \langle f_1, \ldots, f_n \rangle$. If not, then $f_{n+1} \notin (f_1, \ldots, f_n)$. Let $a_{n+1} = \sum_{i=1}^{n} \lambda_i a_i$. We consider $g(X) = f_{n+1}(X) - \sum_{i+1}^{n} \lambda_i f_i(X) X^{\deg(f_{n+1}) - \deg(f_i)}$. $g(X)$ has degree less than degree of $f_{n+1}(X)$ and is not generated by $f_1, \ldots, f_n$. Thus contradiction. $\square$

2.4 Discrete Valuation Ring

Definition 19. Let Δ be an ordered group. A *valuation* ν on k (field) with values in Δ is a mapping $\nu : k^* \to \Delta$ satisfying the conditions:

1. $\nu(ab) = \nu(a) + \nu(b)$
2. $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$

It is sometimes convenient to adjoin an element ∞ to Δ and extend the operations.

Example 1. *Let $K = k(X)$ be the field of rational functions in X over k and $p(X)$ an irreducible polynomial in $k[X]$. Any non-zero element of K can be uniquely written* *as*

$$\theta(X) = p(X)^r \frac{f(X)}{g(X)}$$

$r \in \mathbb{Z}$ and $p(X)$ does not divide $f(X)$ or $g(X)$. Then the map $\nu : K \to \mathbb{Z}$ given by $\nu(\theta(X)) = r$ is a valuation on $k(X)$. This valuation is called $p(X)$-adic valuation. More generally, R be a PID with quotient field k and $p \in R$ an irreducible element. If $\alpha \in k$, write $\alpha = p^r b/c$, $(p, b) = 1$, $(p, c) = 1$, $r \in \mathbb{Z}$. $\nu : k \to \mathbb{Z}$ defined by $\nu(\alpha) = r$ is a valuation on k called p-adic valuation on k.

The valuation ring corresponding to the valuation ν is given by

$$\nu = \{a \in k \mid \nu(a) \geq 0\}$$

Definition 20. A *discrete valuation* is a surjective valuation $\nu : k^* \to \mathbb{Z}$. The corresponding valuation ring is called *discrete valuation ring* (DVR).

Both the examples given above of the valuation are discrete valuation.

Theorem 2.4.1. *Let R be a domain that is not a field. Then the following are equivalent:*

1. *R is Noetherian and local, and the maximal ideal is principal.*

2. *R is a DVR.*

Proof. ($\Rightarrow$) We will show that every nonzero element $z \in R$ can be written uniquely as $z = ut^n$, u unit in R, n a non negative integer and $t \in R$ is an irreducible element. Then we can define the valuation as $\nu(z) = n$.
Let $\mathfrak{m} = (t)$ be the maximal ideal. Suppose t is generator of $\mathfrak{m}$. Suppose $ut^n = vt^m$, u, v units, $n \geq m$. Then $ut^{n-m} = v$ is a unit. So $n = m$ and $u = v$. Thus, the expression $z = ut^n$ is unique. Now, let z not a unit (if it is, then we can take $z = ut^0$), so $z \in \mathfrak{m}$, i.e. $z = z_1 t$, $z_1 \in R$. If z_1 is a unit we are done, if not $\exists$ $z_2 \in R$ such that $z_1 = z_2 t$. Continuing, we can find an infinite sequence $z_1, z_2, \ldots$, with $z_i = z_{i+1} t$. Since R is Noetherian, the chain of ideals $(z_1) \subset (z_2) \cdots$ must have a maximal member. So $(z_n) = (z_{n+1})$ for some n. Then $z_{n+1} = vz_n$ for some $v \in R$, so $z_n = tvz_n \Rightarrow vt = 1 \Rightarrow t$ is a unit. Contradiction. So, there exists some z_i which can be written as ut, where u is unit, thus expressing $z = ut^i$, i unit.
($\Leftarrow$) R is a DVR. Claim is that every nonzero ideal is unique of the type $\mathfrak{m}^n (n \geq 1)$.

Let I be a nonzero ideal in R. Since, discrete valuation is surjective map, $\exists\ t \in R$ such that $\nu(t) = 1$. Choose $a \in I$ such that $\nu(a) = n$, n least non negative integer. Then $\nu(at^{-n}) = 0$, so that at^{-n} is a unit, i.e. $a = ut^n$. Hence $(t^n) \subset I$. If $b \in I$, with $\nu(b) = k \geq n$, then $\nu(bt^{-k}) = 0$, i.e. $b = vt^k$, v unit and $b \in (t^n)$. Hence, $I = (t^n) = \mathfrak{m}^n$ and n is unique. $\square$

The maximal ideal corresponding to a valuation ring R is given by

$$\mathfrak{m} = \{a \in k \mid \nu(a) > 0\}$$

An element with $t \in k$ is called a *uniformizing parameter* for ν if $\nu(t) = 1$. This is the generator of the maximal ideal.

Chapter 3

Affine Geometry

3.1 Algebraic sets and Ideals of Set of Points

Notation 1. *We assume k to be any algebraically closed field through out this thesis if otherwise mentioned.*

1. *$\mathbb{A}^n(k)$ or simply $\mathbb{A}^n$ (if k is understood) is the set of n-tuples of elements of k and is called Affine n-space over k. Its element are called points. $\mathbb{A}^1(k)$ is the Affine line and $\mathbb{A}^2(k)$ is the Affine space.*

2. *If $F \in k[X_1, \ldots, X_n]$, a point $P = (a_1, \ldots, a_n)$ in $\mathbb{A}^n(k)$ is called a zero of F if $F(P) = F(a_1, \ldots, a_n) = 0$.*

3. *If F is not a constant polynomial, the set of zeroes of F is called hypersurface defined by F, and is denoted by $V(F)$. An hypersurface in $\mathbb{A}^2(k)$ is called an Affine plane curve. If F is a polynomial of degree 1, $V(F)$ is called hyperplane in $\mathbb{A}^n(k)$. For $n = 2$, we call it a line.*

4. *If S is any set of polynomials in $k[X_1, \ldots, X_n]$, we have $V(S) = \{P \in \mathbb{A}^n(k) \mid F(P) = 0$ for all $F \in S\}$, $V(S) = \cap_{F \in S} V(F)$. A subset $X \subset \mathbb{A}^n(k)$ is an Affine algebraic set or simply algebraic set, if $X = V(S)$ for some S.*

5. *For any subset X of $\mathbb{A}^n(k)$, the Ideal of X is defined as those polynomials in $k[X_1, \ldots, X_n]$ that vanish on X, i.e. $I(X) = \{F \in k[X_1, \ldots, X_n] \mid F(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in X\}$. It is an ideal in $k[X_1, \ldots, X_n]$.*

Example 2. *$A = \{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$ is an algebraic set as $A = V(X - Y^2, Y^2 - Z^3)$. Similarly, the circle $C = \{(\cos(t), \sin(t)) \in \mathbb{A}^2(\mathbb{R}) \mid t \in \mathbb{R}\}$ is also an algebraic set as $C = V(X^2 + Y^2 - 1)$.*
However, $\{(\cos(t), \sin(t), t) \in \mathbb{A}^3(\mathbb{R}) \mid t \in \mathbb{R}\}$ is not an algebraic set. (cf. appendix problem 7.1.11 and problem 7.1.13)

Facts on Algebraic sets

1. If I is an ideal in $k[X_1, \dots, X_n]$ generated by S, then $V(S) = V(I)$. So, every algebraic set is equal to $V(I)$ for some ideal I.

2. If $\{I_\alpha\}$ is any collection of ideals in $k[X_1, \dots, X_n]$, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$. So, intersection of algebraic sets is an algebraic set.

3. If $I \subset J$, then $V(I) \supset V(J)$ (I, J are ideals in $k[X_1, \dots, X_n]$); If $X \subset Y$, then $I(X) \supset I(Y)$.

4. $V(FG) = V(F) \cup V(G)$ for any polynomial F, G. So, any finite union of algebraic sets is an algebraic set.

5. (i) $V(0) = \mathbb{A}^n(k)$

   (ii) $V(k[X_1, X_2, \dots, X_n]) = V(1) = \Phi$

   (iii) $V(X_1 - a_1, \dots, X_n - a_n) = \{(a_1, \dots, a_n)\}$

   for $a_i \in k$. So, any finite subset of $\mathbb{A}^n(k)$ is an algebraic set.

6. (i) $I(\Phi) = k[X_1, \dots, X_n]$

   (ii) $I(\mathbb{A}^n(k)) = (0)$ if k is an infinite field

   (iii) $I(\{(a_1, \dots, a_n)\}) = (X_1 - a_1, \dots, X_n - a_n)$ for $a_1, \dots, a_n \in k$.

7. $I(V(S)) \supset S$ for any set S of polynomials and if S is an algebraic set, then equality holds true; $V(I(X)) \supset X$ for any set X of points and if I is an an ideal of algebraic set then equality holds true. In general, $V(I(V(S))) = V(S)$ and $I(V(I(X))) = I(X)$.

8. $I(X)$ is a radical ideal for any $X \subset \mathbb{A}^n(k)$ (Radical of I, written $\sqrt{I}$, is $\{a \in R \mid a^n \in I$ for some integer $n > 0\}$. $\sqrt{I}$ is itself an ideal and an ideal I is called a radical ideal if $I = \sqrt{I}$).

Definition 21. An algebraic set V is **reducible** if $V = V_1 \cup V_2$, where V_1, V_2 are algebraic sets in $\mathbb{A}^n$, and $V_i \neq V$, $i = 1, 2$. Otherwise we say V is irreducible. An irreducible affine algebraic set is called an **affine variety**.

Theorem 3.1.1. *An algebraic set V is irreducible if and only if $I(V)$ is prime.*

Proof. ($\Rightarrow$:) If $I(V)$ is not prime, suppose $F_1F_2 \in I(V)$, $F_i \notin I(V)$. Then $V \subset V(F_1F_2) = V(F_1) \cup V(F_2) \Rightarrow V = (V \cap V(F_1)) \cup (V \cap V(F_2))$, and $V \cap V(F_i) \neq V$, so V is irreducible.
($\Leftarrow$:) If $V = V_1 \cup V_2$, $V_i \subsetneq V$, then $I(V_i) \supsetneq I(V)$; Let $F_i \in I(V_i)$, $F_i \notin I(V)$. Then $F_1F_2 \in I(V)$, so $I(V)$ is not prime. $\square$

In particular, $\mathbb{A}^n$ is irreducible.

Theorem 3.1.2. *Every algebraic set is the intersection of a finite number of hypersurfaces*

Proof. Let the algebraic set be $V(I)$ for some ideal $I \subset k[X_1, \ldots, X_n]$. Since, $k[X_1, \ldots, X_n]$ is a Noetherian ring, $I = (F_1, \ldots, F_r)$ (by Hilbert Basis Theorem), then $V(I) = V(F_1) \cap \cdots \cap V(F_r)$, where F_i's are irreducible. $\square$

Lemma 3.1.3. *Let ζ be any nonempty collection of ideals in a Noetherian ring R. Then ζ has a maximal member, i.e. there exists an ideal I in ζ that is not contained in any other ideal of ζ.*

Proof. Choose an ideal from each subset of ζ. let I_0 be the chosen ideal for ζ itself. Let $\zeta_1 = \{I \in \zeta \mid I \supsetneq I_0\}$, and let I_1 be the chosen ideal of ζ_1. Let $\zeta_2 = \{I \in \zeta \mid I \supsetneq I_1\}$, and so on.
Claim: ζ_n is empty. If not, let $I = \bigcup_{n=0}^{\infty} I_n$. Let $F_1, \ldots, F_r$ generate I (as I is an ideal of Noetherian ring R), each $F_i \in I_n$ if n is chosen sufficiently large. But then $I_n = I$, so $I_{n+1} = I_n$, a contradiction. $\square$

Lemma 3.1.4. *Any collection of algebraic sets in $\mathbb{A}^n(k)$ has a minimal member.*

Proof. If $\{V_\alpha\}$ is such a collection, take a maximal member $I(V_{\alpha_0})$ from $\{I(V_\alpha)\}$ (by above Lemma it exists). Then V_{α_0} is the minimal in the collection. $\square$

Theorem 3.1.5. *Let V be an algebraic set in $\mathbb{A}^n(k)$. Then there are unique irreducible algebraic sets $V_1, \ldots, V_m$ such that $V = V_1 \cup \cdots \cup V_m$ and $V_i \nsubseteq V_j$ for all $i \neq j$.*

Proof. Let $\zeta = \{$algebraic sets $V \subset \mathbb{A}^n(k) \mid V$ is not the union of a finite number of irreducible algebraic sets $\}$.
Claim: ζ is empty. If not, let V be a minimal member of ζ (by above Lemma it exists). Since $V \in \zeta$, V is not irreducible, so $V = V_1 \cup V_2, V_i \subsetneq V$. Then $V_i \notin \zeta$, so $V_i = V_{i1} \cup \cdots \cup V_{im_i}$, V_{ij} irreducible. But then $V = \cup_{i,j} V_{ij}$, a contradiction. Thus, any algebraic set can be written as $V = V_1, \ldots, V_m$, V_i irreducible. If $V_i \subset V_j$ for some i, j, remove V_i to get the condition $V_i \not\subset V_j$ for all $i \neq j$.
(*Uniqueness*:) Let $V = W_1 \cup \cdots \cup W_l$ be another such decomposition. Then $V_i = \bigcup\limits_j (W_j \cap V_i)$. Since, V_i's are irreducible, $V_i \subset W_{j(i)}$ for some $j(i)$. Similarly, $W_{j(i)} \subset V_k$ for some k. This imply that $V_i \subset V_k \Rightarrow i = k$. So, $V_i = W_{j(i)}$ and $W_j = V_{i(j)}$. □

The irreducible algebraic sets in the Theorem are called as **irreducible components** of V and $\cup_{i=1}^m V_i$ is called the **decomposition** of V into irreducible components.

3.2 Zariski Topology

Definition 22. Let R be a ring. For an ideal I of R

$$V(I) = \{P \mid P \in \mathrm{Spec}(R)\ I \subset P\}$$

is called algebraic subset of ring R.

It satisfies the following properties:

1. $V(R) = \Phi$
2. $V(0) = \mathrm{Spec}(R)$
3. $V(I) = V(\sqrt{I})$
4. $V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$ (can be extended to finite union)
5. $\bigcap\limits_{\alpha \in \Delta} V(I_\alpha) = V(\sum\limits_{\alpha \in \Delta} I_\alpha)$ (Δ is indexing set)
6. $I \subset J \Rightarrow V(J) \subset V(I)$

Definition 23. A subset C of $\mathrm{Spec}(R)$ is said to be closed if $C = V(I)$ for some ideal I of R.

Definition 24. ***Zariski topology*** *is defined by the closed sets satisfying above properties (1), (2), (4) and (5).*

Let $U = \bigcup_{\alpha\in\Delta} V(I_\alpha)$, then $\bar{U} = V(\bigcap_{\alpha\in\Delta} I_\alpha)$, i.e. $\bar{U}$ is smallest closed set containing U.

Definition 25. For $f \in R$, $D(f) = \mathrm{Spec}(R) - V(f)$, $D(f)$ are the basic open sets of the Zariski Topology.

One can identify $D(f)$ with $\mathrm{Spec}(R[\frac{1}{f}])$.
If U is open in $\mathrm{Spec}(R)$, then there exists an ideal $J \in R$ such that $U = \mathrm{Spec}(R) - V(J)$ and $U = \bigcup_{f\in J} D(F)$.

3.3 Affine Varieties

Let $V \subset \mathbb{A}^n$ be a nonempty variety.

Definition 26. A function $f : V \to k$ is called a **polynomial function** on V if f is the restriction to V of a polynomial function on $\mathbb{A}^n$, i.e. $F \in k[X_1, \ldots, X_n]$ such that $f(x) = F(x)$, $\forall x \in V$.

The map that associates to each $F \in k[X_1, \ldots, X_n]$ a polynomial function on V is a ring homomorphism whose kernel is $I(V)$ (cf. appendix problem 7.2.1).

Definition 27. The set of all polynomial functions on V is a k-algebra (for point wise addition and multiplication of functions), called **coordinate ring** of V and is denoted by $\Gamma(V)$.

Proposition 3.3.1. *The coordinate ring $\Gamma(V)$ of V is naturally isomorphic to the quotient ring $k[X_1, \ldots, X_n]/I(V)$.*

Proof. We consider the natural map $k[X_1, \ldots, X_n] \to k[V]$, $F \mapsto f = F|_V$ which is surjective homomorphism of rings. Its kernel is $I(V)$. □

V is irreducible, implies $I(V)$ is a prime ideal in $k[X_1, \ldots, X_n]$. So $\Gamma(V)$ is a domain.

Definition 28. The quotient field of $\Gamma(V)$ is called the **field of rational functions** on V and is denoted by $k(V)$. An element of $k(V)$ is the rational function on V.

Let $\Gamma(V)$ be a UFD. If f is a rational function on V and $P \in V$, we say that f is defined at P if and only if for some $a, b \in \Gamma(V)$, $f = a/b$, and $b(P) \neq 0$. The set of rational functions on V that are defined at P is represented by $\mathscr{O}_P(V)$. $\mathscr{O}_P(V)$ forms a subring of $k(V)$ containing $\Gamma(V)$ and is called **local ring** of V at P. The ideal $\mathfrak{m}_P(V) = \{f \in \mathscr{O}_P(V) | f(P) = 0\}$ is the maximal ideal of V at P as it is the kernel of the evaluation homomorphism $f \to f(P)$ of $\mathscr{O}_P(V)$ onto k, so $\mathscr{O}_P(V)/\mathfrak{m}_P(V)$ is isomorphic to k.

Proposition 3.3.2. *$\mathscr{O}_P(V)$ is a Noetherian local domain.*

Proof. Since $k[X_1, \ldots, X_n]$ is Noetherian ring, $\Gamma(V)$ is Noetherian. Choose generators $f_1, \ldots, f_r$ for the ideal $I \cap \Gamma(V)$ of $\Gamma(V)$. Let $f \in I \subset \mathscr{O}_P(V)$, then there exists $b \in \Gamma(V)$ with $b(P) \neq 0$ such that

$$bf \in \Gamma(V) \Rightarrow bf \in \Gamma(V) \cap I \Rightarrow bf = \sum a_i f_i \; a_i \in \Gamma(V)$$

□

3.4 Hilbert's Nullstellensatz Theorem

Lemma 3.4.1. *Let A be a commutative ring and $I = (a_1, a_2, \ldots, a_n)$ be an ideal of A. Suppose that $P_1, P_2, \ldots, P_r$ are prime ideals of A and $I \nsubseteq P_i, 1 \leq i \leq r$. Then we can find $b_2, \ldots, b_n \in A$ such that $a_1 + b_2 a_2 + \cdots + b_n a_n \notin \bigcup_{i=1}^{r} P_i$.*

Proof. Without loss of generality, we can assume that $P_i \nsubseteq P_j$ for $i \neq j$. Applying induction on r. Trivially true for $r = 1$ case. Suppose by induction we have chosen $c_2, \ldots, c_n \in A$ such that $d_1 = a_1 + c_2 a_2 + \cdots + c_n a_n \notin \cup_{i=1}^{r-1} P_i$. If $d_1 \notin P_r$, then we are done by taking $b_i = c_i, 2 \leq i \leq n$. So, we assume $d_1 \in P_r$. If $a_2, \ldots, a_n$ all belong to P_r, then $d_1 - \sum_{i=2}^{n} a_i c_i = a_1 \in P_r$. But, this will imply that $I \subset P_r$. Thus, at least one of the $a_i \notin P_r, 2 \leq i \leq n$. Let it be $a_2 \notin P_r$. Since $P_i \nsubseteq P_j$ for $i \neq j$, we can choose $x \in \bigcap_{i=1}^{r-1} P_i$ such that $x \notin P_r$. Then $c = d_1 + x a_2 = a_1 + a_2 b_2 + \ldots + a_n b_n \notin \bigcup_{i=1}^{r} P_1$. (This Lemma can also be proved using Prime Avoidance Lemma) □

Lemma 3.4.2. ***Change of variables:*** *Let k be any field (not necessarily algebraically closed), $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ be a non constant polynomial. Then there exist $c_1, \ldots, c_{n-1} \in \mathbb{N}$ such that if ϕ is the ring automorphism of $k[X_1, \ldots, X_n]$,* *given by $\phi\mid_k = Id$, $\phi(X_i) = X_i + X_n^{c_i}$ for $1 \leq i \leq n-1$ and $\phi(X_n) = X_n$, then $\phi(f(X_1, \ldots, X_n))$ is monic in X_n (after multiplying an element of k^*).*

Proof. We have

$$\begin{aligned}\phi(X_1^{\alpha_1} \ldots X_n^{\alpha_n}) &= (X_1 + X_n^{c_1})^{\alpha_1}(X_2 + X_n^{c_2})^{\alpha_2} \ldots (X_{n-1} + X_n^{c_{n-1}})^{\alpha_{n-1}}(X_n)^{\alpha_n} \\ &= X_n^{c_1\alpha_1 + \cdots + c_{n-1}\alpha_{n-1} + \alpha_n} + \textit{ terms involving a lower power of } X_n\end{aligned}$$

Let $X_1^{\gamma_1} \ldots X_n^{\gamma_n}$ and $X_1^{\beta_1} \ldots X_n^{\beta_n}$ be any two distinct monomials in the polynomial $f(X_1, \ldots, X_n)$. We want to choose integers $c_1, \ldots, c_{n-1}$ such that

$$c_1\beta_1 + \cdots + c_{n-1}\beta_{n-1} + \beta_n \neq c_1\gamma_1 + \cdots + c_{n-1}\gamma_{n-1} + \gamma_n$$

Let $t > max(\gamma_i, \beta_j)$ for all $1 \leq i, j \leq n$. Let $c_1 = t^{n-1}, c_2 = t^{n-2}, \ldots, c_{n-1} = t$. These c_i's works by considering t-adic expansions. Thus, by suitably choosing t, $\phi(f(X_1, \ldots, X_n))$ is monic. $\square$

Lemma 3.4.3. ***Extension Lemma:*** *Let A be Noetherian ring and $I \subset A[X]$ be an ideal containing a monic polynomial. Let J be an ideal of A satisfying $I + JA[X] = A[X]$. Then $I \cap A + J = A$.*

Proof. Let $I \cap A + J \neq A$, then $I \cap A + J \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of A. Then, $I + \mathfrak{m}A[X] = A[X]$ and $I \cap A + \mathfrak{m} = \mathfrak{m}$. Hence, if we show that the Lemma is valid when J is a maximal ideal, we are through. $\square$

Lemma 3.4.4. *Let A be Noetherian ring and $\mathfrak{m} \subset A$ be a maximal ideal. Suppose $I \subset A[X]$ is an ideal containing a polynomial $f(x)$ of the form $c_nX^n + c_{n-1}X^{n-1} + \cdots + c_0$, with $c_n \notin \mathfrak{m}$. Suppose $I + A[X] = A[X]$. Then $I \cap A + \mathfrak{m} = A$.*

Proof. Suppose to the contrary that $I \cap A + \mathfrak{m} \neq A$, then $I \cap A \subset \mathfrak{m}$. We consider the set S of polynomials in I which have the property that their leading coefficients do not belong to $\mathfrak{m}$. Since $f(X) \in S$, S is not empty. We prove that there is a polynomial of degree 0 in S thus contradicting the fact that $I \cap A \subset \mathfrak{m}$.
Let $f_1(X)$ be the polynomial of least degree in S. If deg $f_1(X) = 0$, we are through. We assume deg$f_1(X) > 0$.
Since A is Noetherian, we can choose $f_1(X), \ldots, f_r(X) \in I$ s.t. $I = (f_1(X), \ldots, f_r(X))$. Take reduction modulo $\mathfrak{m}[X]$ (representing the elements by bar). Since $A + \mathfrak{m}A[X] = A[X]$, we have $\overline{I} = (\overline{f_1(X)}, \ldots, \overline{f_r(X)}) = \overline{A}[X]$. Let $\overline{Q}_1, \ldots, \overline{Q}_s$ be the maximal ideals

of $A/\mathfrak{m}[X]$ containing $f_1(X)$. Since $\overline{I} = \overline{A}[X]$, it follows that $(\overline{f_2(X)}, \dots, \overline{f_r(X)}) \nsubseteq Q_i$ for every $i, 1 \leq i \leq s$. Then by Lemma 3.4.1, we can find $\overline{\lambda_3(X)}, \overline{\lambda_4(X)}, \dots, \overline{\lambda_r(X)} \in \overline{A}[X]$ such that the polynomial

$$\overline{g_1(X)} = \overline{f_2(X)} + \overline{\lambda_3(X) f_3(X)} + \cdots + \overline{\lambda_r(X) f_r(X)} \notin Q_i \ \forall 1 \leq i \leq s$$

This implies that $(\overline{g_1(X)}, \overline{f_1(X)}) = \overline{A}[X]$. Thus,

$$(f_1(X), g_1(X)) + \mathfrak{m}A[X] = A[X]$$

Let $f_1(X) = a_t X^t + a_{t-1} X^{t-1} + \cdots + a_0$ $(a_t \notin \mathfrak{m})$ and $g_1(X) = b_l X^l + b_{l-1} X^{l-1} + \cdots + b_0$
Let $\deg(g_1(X)) \geq \deg(f_1(X))$
Since $(f_1(X), g_1(X)) + \mathfrak{m}A[X] = A[X]$ and $a_t \notin \mathfrak{m}$, any prime ideal containing $(f_1(X), a_t g_1(X)) + \mathfrak{m}A[X]$ has to be equal to $A[X]$. Hence

$$(f_1(X), a_t g_1(X)) + \mathfrak{m}A[X] = A[X]$$

Now, if $h_1(X) = a_t g_1(X) - b_l X^{\deg(g_1) - \deg(f_1)} f_1(X)$, then $(f_1(X), h_1(X)) + \mathfrak{m}A[X] = A[X]$ and $\deg(h_1) < \deg(g_1)$. Proceeding like this, we can reduce the case where $\deg(g_1) < \deg(f_1)$.
Let $f_1(X) = a_t X^t + a_{t-1} X^{t-1} + \cdots + a_0$ $(a_t \notin \mathfrak{m})$ and $g_1(X) = b_l X^l + b_{l-1} X^{l-1} + \cdots + b_0$ as before and $(f_1(X), g_1(X)) + \mathfrak{m}A[X] = A[X]$ and $\deg(g_1) < \deg(f_1)$. Since, $f_1(X) = a_t X^t + a_{t-1} X^{t-1} + \cdots + a_0$ and $a_t \notin \mathfrak{m}$, we see that $g_1(X) \notin \mathfrak{m}A[X]$ and hence $b_i \notin \mathfrak{m}$ for some $i \leq l$. If $b_l \notin \mathfrak{m} \Rightarrow g_1(X) \in S$. Since $\deg(g_1) < \deg(f_1)$ and $f_1(X)$ is the element of least degree in S, we get a contradiction. Hence $b_l \in \mathfrak{m}$.
It follows that $b_i \notin \mathfrak{m}$ for some $i < l$. We assume for simplicity $b_{l-1} \notin \mathfrak{m}$. Then the polynomial $a_t X^{\deg(f_1) - \deg(g_1)} g_1(X) - b_l f_1(X)$ has leading coefficients $a_t b_{l-1}$ modulo $\mathfrak{m}$ and has lesser degree than f_1. Since $a_t \in \mathfrak{m}$ and $b_{l-1} \notin \mathfrak{m}$, $a_t b_{l-1} \notin \mathfrak{m}$ and this contradicts the choice of f_1. Thus $b_{l-1} \in \mathfrak{m}$ and $b_i \notin \mathfrak{m}$ for some $i < l-1$, we can proceed in a similar manner to get the contradiction for any l. Thus $\deg(f_1) = 0$. $\square$

Theorem 3.4.5. ***Weak Hilbert's Nullstellensatz Theorem:*** *Let I be a proper ideal in $k[X_1, \dots, X_n]$. Then $V(I) \neq \Phi$.*

Proof. Let $A = k[X_1, X_2, \dots, X_{n-1}]$. By Lemma 3.4.2, change of variables, I contains a monic polynomial in X_n, that is a polynomial of the form $X_n^t + b_{n-1} X_n^{t-1} + \cdots + b_0$, with $b_i \in A$. By induction, we choose $a_1, a_2, \ldots, a_{n-1} \in k$ such that

$$g(a_1, a_2, \ldots, a_{n-1}) = 0, \ \forall g \in I \cap A$$

Let $I = (f_1(X_1, \ldots, X_n), \ldots, f_m(X_1, \ldots, X_n))$ (As $k[X_1, X_2, \ldots, X_n]$ is Noetherian ring).
Claim: Ideal $(f_1(a_1, \ldots, a_{n-1}, X_n), \ldots, f_m(a_1, \ldots, a_{n-1}, X_n))$ of $k[X_n]$ is a proper ideal. As, if this is the case, since k is algebraically closed, choose $a_n \in k$ such that $f_i(a_1, \ldots, a_n) = 0, 1 \leq i \leq m$. Thus $(a_1, \ldots, a_n)$ is the common zero of every polynomial in $I \Rightarrow V(I) \neq \Phi$.
If claim is false, then

$$(f_1(a_1, \ldots, a_{n-1}, X_n), \ldots, f_m(a_1, \ldots, a_{n-1}, X_n)) = k[X_n]$$

It follows that $I + JA[X_n] = A[X_n]$, where J is the ideal $(X_1 - a_1, \ldots, X_{n-1} - a_{n-1})$ of A. It follows from the extension Lemma

$$I \cap A + J = A$$

Therefore, $1 = h + j$, where $h \in I \cap A$ and $j \in J$. Setting $X_1 = a_1, X_2 = a_2, \ldots, X_{n-1} = a_{n-1}$, we obtain $0 = 1$ contradiction. □

Lemma 3.4.6. *For any ideal I in $k[X_1, \ldots, X_n]$, $V(I) = V(\sqrt{I})$ and $\sqrt{I} \subset I(V(I))$.*

Proof. Since $I \subset \sqrt{I} \Rightarrow V(\sqrt{I}) \subset V(I)$.
Let $P \in V(I)$ and g$\in \sqrt{I}$. Then there exists $m \in \mathbb{N}$ such that $g^m \in I$. Thus,

$$g^m(P) = 0 \Rightarrow g(P) = 0 \Rightarrow P \in \sqrt{I} \Rightarrow V(I) \subset V(\sqrt{I})$$

Thus, $V(I) = V(\sqrt{I})$. Since, $\sqrt{I} \subset I(V(\sqrt{I}))$ (true for any subset of $k[X_1, \ldots, X_n] \Rightarrow \sqrt{I} \subset I(V(I)))$ □

Theorem 3.4.7. ***Hilbert's Nullstellensatz Theorem:*** *Let I be a proper ideal in $k[X_1, \ldots, X_n]$. Then $I(V(I)) = \sqrt{I}$*

Proof. $\sqrt{I} \subset I(V(I))$ follows from the above Lemma.
Suppose that $I = (f_1, f_2, \ldots, f_r), f_i \in k[X_1, \ldots, X_n]$. Suppose g is in the ideal $I(V(I))$. Let $J = (f_1, \ldots, f_r, X_{n+1}g - 1) \subset k[X_1, \ldots, X_n, X_{n+1}]$. g vanishes where

ever f_i's are zero. This implies that $V(J)$ is empty. Applying Weak Hilbert's Nullstellensatz Theorem, $J = k[X_1, \dots, X_n, X_{n+1}]$. So, $1 \in J$. So there is an equation $1 = \sum A_i(X_i, \dots, X_{n+1})f_i + B(X_1, \dots, X_{n+1})(X_{n+1}g - 1)$. Let $Y = 1/X_{n+1}$, and multiply the equation by a higher power of Y, so that an equation $Y^N = \sum C_i(X_1, \dots, X_n, Y)f_i + D(X_1, \dots, X_n, Y)(g-Y)$ in $k[X_1, \dots, X_n, Y]$ results. Taking $Y = g$, we get g^N as linear combination of $f_i's$ in $k[X_1, \dots, X_n]$. Thus, $g \in \sqrt{I} \Rightarrow I(V(I)) \subset \sqrt{I}$. □

Corollary 3.4.8. *There is one to one correspondence between the following:*

1. *Algebraic subsets of $\mathbb{A}^n$ and radical ideals of $k[X_1, \dots, X_n]$.*
2. *Non empty irreducible algebraic subsets of $\mathbb{A}^n$ and prime ideals of $k[X_1, \dots, X_n]$.*
3. *Points in $\mathbb{A}^n$ and maximal ideals in $k[X_1, \dots, X_n]$.*

Corollary 3.4.9. *Let I be an ideal in $k[X_1, \dots, X_n]$. Then $V(I)$ is a finite set if and only if $k[X_1, \dots, X_n]/I$ is a finite dimensional vector space over k. If this occurs, the number of points in $V(I)$ is at most $\dim_k(k[X_1, \dots, X_n]/I)$.*

Corollary 3.4.10. *Let F ($\notin k$) be a polynomial in $k[X_1, \dots, X_n]$, $F = F_1^{n_1} \dots F_r^{n_r}$ the decomposition of F into irreducible factors. Then $V(F) = V(F_1) \cup \dots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components, and $I(V(F)) = (F_1, \dots, F_r)$*

Proof. By property 4, $V(F) = V(F_1) \cup \dots \cup V(F_r)$ and irreducibility follows as F_i's are distinct irreducible factors. Now,

$$I(\cup_i V(F_i)) = \cap_i I(V(F_i)) = \cap_i (F_i)$$

as $I(V(F_i)) = \sqrt{F_i} = (F_i)$ by Hilbert's Nullstellensatz Theorem and (F_i) is a prime (implies radical) ideal as (F_i) is irreducible. □

Chapter 4

Multiplicity and Intersection Numbers in Plane Curves

Affine plane curve is a non constant polynomial $F \in k[X,Y]$, where F is determined up to multiplication by a non zero $\lambda \in k$ (i.e. F, G in $K[X,Y]$ represent the same curve or we say they are *equivalent* if $F = \lambda G$).

Definition 29. The point $P = (a,b)$ in $V(F)$ is called a **simple point** of F if either derivative $F_X(P) \neq 0$ or $F_Y(P) \neq 0$ and the line

$$F_X(P)(X-a) + F_Y(P)(Y-b) = 0$$

is called a **tangent line** to F at P.

A point that is not simple is called **multiple** or **singular**. A curve with only non-singular points is called a **non-singular curve**.

Definition 30. Let F be any curve of degree n and $P = (0,0)$. Let $F = F_m + F_{m+1} + \cdots + F_n$, where F_i's are form of degree i and $F_m \neq 0$ $(m \leq i \leq n)$. Then, F_m is called **initial form** of F and m as **multiplicity** of F at P (denoted by $m_p(F)$).
Since F_m is a form in two variables, we can write $F_m = \prod L_i^{r_i}$, where L_i's are distinct lines called as **tangent** lines to F at P and r_i as **multiplicity** of the tangent. If F has m distinct tangents then P is an **ordinary multiple point** of F.

For any arbitrary point $P = (a,b)$, let $T(x,y) = (x+a, y+b)$ be a translation. Then

$$F^T = F(X+a, X+b) = G_m + G_{m+1} + \cdots + G_n$$

G_i's are forms and $G_m \neq 0$. Therefore, $m_p(F) = m_0(F^T)$ and if $G_m = \prod L_i^{r_i}$, $L_i = \alpha_i X + \beta_i Y$, the lines $\alpha_i(X-a) + \beta_i(Y-b)$ are the tangent lines to F at P.

If $F = \prod F_i^{e_i}$ be the decomposition of F into irreducible components, then $m_P(F) = \sum e_i m_P(F_i)$ and if L is the tangent line to F_i with multiplicity r_i, then L is the tangent to F with multiplicity $\sum e_i r_i$ as the lowest degree terms of F is the product of lowest degree terms of its factors.

From now on, $\Gamma(V(F)), k(V(F))$ *and* $\mathscr{O}_P(V(F))$ *are represented as* $\Gamma(F), k(F)$ *and* $\mathscr{O}_P(F)$.

Definition 31. A mapping $T : V \to W$ is called a **polynomial map** if there are polynomials $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ such that

$$T(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n)) \;\; \forall \; (a_1, \ldots, a_n) \in V$$

Any polynomial map $T : V \to W$ induces a homomorphism between $\tilde{T} : \Gamma(W) \to \Gamma(V)$ by setting $\tilde{T}(f) = f \circ T$.

Definition 32. An **affine change of coordinates** on $\mathbb{A}^n$ is a polynomial map $T = (T_1, \ldots, T_n) : \mathbb{A}^n \to \mathbb{A}^n$ such that each T_i is a polynomial of degree 1, and such that T is one-to-one and onto.

Any such map T has the form $T_i = \sum_{j=1}^{n} a_{ij} X_j + a_{i0}$, then $T = T'' \circ T'$, where T' is a linear map ($T' = \sum a_{ij} X_j$) and T'' is translation ($T'' = X_i + a_{i0}$). Since any translation has a inverse, it follows that T is one-to-one and onto if and only if T' is invertible. Thus, T is an isomorphism of the variety $\mathbb{A}^n$ with itself. If T and U are affine change of coordinates on $\mathbb{A}^n$, then so are $T \circ U$ and T^{-1}.

Notation 2. *Let* F *be a polynomial in* $k[X_1, \ldots, X_n]$*. We define* $F^T = \tilde{T}(F) = F(T_1, \ldots, T_m)$*. For ideals* I *and algebraic set* V *in* $\mathbb{A}^m$*,* I^T *will denote the ideal in* $k[X_1, \ldots, X_n]$ *generated by* $\{F^T | F \in I\}$ *and* V^T *will denote algebraic set* $T^{-1}(V) = V(I^T)$*, where* $I = I(V)$*.*

Lemma 4.0.11. *Let* $\phi : V \to W$ *be a polynomial map of affine varieties,* $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$ *the induced map on coordinate rings. Suppose* $P \in V, \phi(P) = Q$*. Show that* $\tilde{\phi}$ *extends to a ring homomorphism (also written* $\tilde{\phi}$*) from* $\mathscr{O}_Q(W)$ *to* $\mathscr{O}_P(V)$*. Show that* $\tilde{\phi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$*.*

Proof. We consider

$$\tilde{\phi} : \mathscr{O}_Q(W) \to \mathscr{O}_P(V)$$

$$f/g \to \tilde{\phi}(f)/\tilde{\phi}(g) = (f \circ \phi)/(g \circ \phi)$$

As g is defined at Q, $g \circ \phi$ is defined at P. Thus, the ring homomorphism is well defined.
Since $f/g \in \mathfrak{m}_Q(W)$, $f(Q) = 0 \Rightarrow \tilde{\phi}(f)(P) = f(\phi(P)) = f(Q) = 0 \Rightarrow \tilde{\phi}(f/g) \in \mathfrak{m}_P(V) \Rightarrow \tilde{\phi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$. □

Proposition 4.0.12. *Let F, G be non-constant polynomials in $k[X, Y]$ such that F and G have no common component. Then $V(F, G) = V(F) \cap V(G)$ is a finite set of points.*

Proof. By assumption, F and G have no common factors in $k[X, Y]$. By Gauss's lemma, they have no common factor in $k(X)[Y]$ (ring of polynomials in one variable over field $k(X)$). It is a PID. Hence, we can find $H, K \in k(X)[Y]$ satisfying $HF + KG = 1$. Now, we have $H = \frac{H_1}{H_2}$ and $K = \frac{K_1}{K_2}$ for some $H_1, K_1 \in k[X, Y]$ and $H_2, K_2 \in k[X]$, $H_2 \neq 0$, $K_2 \neq 0$. Therefore, $H_1K_2F + H_2K_1G = H_2K_2 \in k[X]$. Since, $H_2K_2 \neq 0$, H_2K_2 has finitely many zeroes in k. Let $S_1 = \{a_1, \dots, a_r\}$ be all the zeroes of H_2K_2. Now, H_2K_2 vanishes whenever F and G vanishes together. So if $(a, b) \in V(F, G)$ then $a \in S_1$. Similarly, we can find $S_2 = \{b_1, \dots, b_t\}$ so that if $(a, b) \in V(F, G)$ then $b \in S_2$. Thus, $V(F, G) \subset S_1 \times S_2$. Hence, $V(F) \cap V(G)$ is a finite set. □

Proposition 4.0.13. *Let I be an ideal in $k[X_1, \dots, X_n]$. If $V(I) = \{P_1, \dots, P_s\}$ is a finite set. Let $\mathscr{O}_{P_i}(\mathbb{A}^n) = \mathscr{O}_i$. Then there exists a k-algebra isomorphism between $k[X_1, \dots, X_n]/I$ and $\prod_{i=1}^{s} \mathscr{O}_i/I\mathscr{O}_i$. Moreover,*

$$\dim_k(k[X_1, \dots, X_n]/I) = \sum_{i=1}^{m} \dim_k \mathscr{O}_i/I\mathscr{O}_i$$

Proof. Let $I_i = I(\{P_i\})$ be the maximal ideal in $k[X_1, \dots, X_n]$ corresponding to the point P_i in $V(I)$. Let $\mathfrak{m}_i$ be the maximal ideal in $k[X_1, \dots, X_n]/I$, corresponding to the point P_i, which is of the form I_i/I for every $i = 1, 2, \dots, s$. By Hilbert's Nullstellensatz Theorem, we have $\sqrt{I} = I(V(I)) = I_1 \cap I_2 \dots \cap I_s$ in $k[X_1, \dots, X_n]$. So, in $k[X_1, \dots, X_n]/I$, $\sqrt{0} = I_1/I \cap \dots \cap I_s/I = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_s$. Therefore, there exists some $N \in \mathbb{N}$ such that $(\cap_{i=1}^{s} \mathfrak{m}_i)^N = 0$. Moreover, $(\cap_{i=1}^{s} \mathfrak{m}_i)^N = \mathfrak{m}_1^N \dots \mathfrak{m}_s^N$

(as $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ are comaximal and so $\mathfrak{m}_1^N, \dots, \mathfrak{m}_s^N$ are comaximal). Let $J_i = \mathfrak{m}_i^N$ for $i = 1, \dots, s$ and $R = k[X_1, \dots, X_n]/I$. Applying Chinese Remainder Theorem, we get a surjective homomorphism

$$\phi : R/I \to R/J_1 \times \cdots \times R/J_s$$

with kernel $\cap_{i=1}^s J_i = \cap_{k=1}^s \mathfrak{m}_k^N = 0$. Hence ϕ is an isomorphism.
Claim 1: $\mathscr{O}_i/I\mathscr{O}_i = R_{\mathfrak{m}_i}$.

$$R_{\mathfrak{m}_i} = (k[X_1, \dots, X_n]/I)_{I_i/I} = k[X_1, \dots, X_n]_{I_i}/Ik[X_1, \dots, X_n]_{I_i}$$

Also, $\mathscr{O}_i = k[X_1, \dots, X_n]_{I_i}$. Hence the claim.
Claim 2: $R_{\mathfrak{m}_1} = R/\mathfrak{m}_1^N$. We have, $R_{\mathfrak{m}_1} = R_{\mathfrak{m}_1}/(\mathfrak{m}_1^N \dots \mathfrak{m}_s^N)R_{\mathfrak{m}_1}$. For $j \geq 2$, $\mathfrak{m}_j$ is not contained in $\mathfrak{m}_1$ and hence $\mathfrak{m}_j^N R_{\mathfrak{m}_1} = R_{\mathfrak{m}_1}$. Therefore, $R_{\mathfrak{m}_1} = R_{\mathfrak{m}_1}/\mathfrak{m}_1^N R_{\mathfrak{m}_1} = (R/\mathfrak{m}_1^N)_{\mathfrak{m}_1} = (R/\mathfrak{m}_1^N)$. This proves the claim. Similarly for all $i = 2, \dots, s$. We get,

$$R/J_i = R/\mathfrak{m}_i^N = R_{\mathfrak{m}_i} = \mathscr{O}_i/I\mathscr{O}_i$$

Hence, follows the Theorem. $\square$

Corollary 4.0.14. *If $V(I) = \{P\}$, then $k[X, Y]/I \cong \mathscr{O}_P(\mathbb{A}^2)/I\mathscr{O}_P(\mathbb{A}^2)$.*

Lemma 4.0.15. *Let V be a variety in $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \dots, X_n]$, $P \in V$, and let J be an ideal of $k[X_1, \dots, X_n]$ that contains I. Let J' be the image of J in $\Gamma(V)$. Then there is a natural isomorphism φ from $\mathscr{O}_P(\mathbb{A}^n)/J\mathscr{O}_P(\mathbb{A}^n)$ to $\mathscr{O}_P(V)/I\mathscr{O}_P(V)$. In particular, $\mathscr{O}_P(\mathbb{A}^n)/I\mathscr{O}_P(\mathbb{A}^n)$ is isomorphic to $\mathscr{O}_P(V)$.*

Proof. We consider the map

$$\phi : \mathscr{O}_P(\mathbb{A}^n)/J\mathscr{O}_P(\mathbb{A}^n) \to \mathscr{O}_P(V)/J'\mathscr{O}_P(\mathbb{A}^n)$$

$$f/g + J\mathscr{O}_P(\mathbb{A}^n) \to (f + I)(g + I) + J'\mathscr{O}_P(V)$$

where $f, g \in k[X_1, \dots, X_n]$
Well defineness: We consider $a/b \in J\mathscr{O}_P(\mathbb{A}^n)$. Then a/b has the form

$$\frac{a}{b} = \sum_i f_i(\frac{g_i}{h_i}) = \frac{\sum_{i=1}^n (a_i g_i \prod_{j \neq i} h_j)}{\prod_i h_i}$$

where $f_i \in J$ and $g_i, h_i \in k[X_1, \ldots, X_n]$. Since $h_i(P) \neq 0 \ \forall i \Rightarrow \prod_i h_i(P) \neq 0$ and $\sum_{i=1}^{n} (a_i g_i \prod_{j \neq i} h_j) \in J$. Thus, every element $a/b \in \mathscr{O}_P(\mathbb{A}^n)$ has the form g/h, where $g \in J$ and $h \in k[X_1, \ldots, X_n]$. It is easy to check that ϕ is ring homomorphism and surjective. For injectivity: Let $(f + I)(g + I) \in J'\mathscr{O}_P(V)$. We can assume that $(f + I) \in J'$ and $1/(g + I) \in \mathscr{O}_P(V) \Rightarrow f \in J$ and $1/g \in \mathscr{O}_P(\mathbb{A}^n)$. Thus $f/g \in J\mathscr{O}_P(\mathbb{A}^n)$. Thus, ϕ is isomorphic. In particular, $\mathscr{O}_P(\mathbb{A}^n)/I\mathscr{O}_P(\mathbb{A}^n)$ is isomorphic to $\mathscr{O}_P(V)$. □

Theorem 4.0.16. *Let P be a point on an irreducible curve F. Then there exists n_0 such that*

$$\mathfrak{m}_P(F) = \dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}) \ \forall n \geq n_0$$

Dimension above means the dimension as a vector space over field k.

Proof. We consider the exact sequence:

$$0 \longrightarrow \mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1} \longrightarrow \mathscr{O}_P(F)/\mathfrak{m}_P(F)^{n+1} \longrightarrow \mathscr{O}_P(F)/\mathfrak{m}_P(F)^n \longrightarrow 0$$

By rank nullity theorem (first isomorphism theorem for vector spaces), we have

$$\dim_k(\mathscr{O}_P(F)/\mathfrak{m}_P(F)^{n+1}) = \dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}) + \dim_k(\mathscr{O}_P(F)/\mathfrak{m}_P(F)^n)$$

Thus, it is enough to show that $\dim_k(\mathscr{O}_P(F)/\mathfrak{m}_P(F)^n) = nm_P(F) + s$, for some constant s, and for all $n \geq m_P(F)$.
We assume $P = (0, 0)$. So, $\mathfrak{m}_P(F) = I\mathscr{O}_P(F) \Rightarrow \mathfrak{m}_P(F)^n = I^n\mathscr{O}_P(F)$, where $I = (X, Y) \subset k[X, Y]$. Since $V(I^n) = \{P\}$ and $F(P) = 0$, we have $V(I^n, F) = \{P\}$. By Corollary 4.0.14, $k[X, Y]/(I^n, F) \cong \mathscr{O}_P(\mathbb{A}^2)/(I^n, F)\mathscr{O}_P(\mathbb{A}^2)$. And by lemma 4.0.15, $\mathscr{O}_P(\mathbb{A}^2)/(I^n, F)\mathscr{O}_P(\mathbb{A}^2) \cong \mathscr{O}_P(F)/I^n\mathscr{O}_P(F)$. Thus, we have

$$k[X, Y]/(I^n, F) \cong \mathscr{O}_P(F)/I^n\mathscr{O}_P(F) = \mathscr{O}_P(F)/\mathfrak{m}_P(F)^n$$

Now we have to calculate the dimension of $k[X, Y]/(I^n, F)$. Let $m = m_P(F)$. Then $FG \in I^n$ whenever $G \in I^{n-m}$. There exists a natural homomorphism

$$\phi : k[X, Y]/I^n \to k[X, Y]/(I^n, F)$$

$$\phi(h + I^n) = h + (I^n, F)$$

Also, there exists a k-linear map ψ from $k[X,Y]/I^{n-m}$ to $k[X,Y]/I^n$ given by $\psi(\overline{G}) = \overline{FG}$. We consider the sequence

$$0 \to k[X,Y]/I^{n-m} \to k[X,Y]/I^n \to k[X,Y]/(I^n, F) \to 0$$

This is an exact sequence. Also, $k[X,Y]/I^n$ consists of all monomials of degree less than n. Therefore,

$$\dim_k(k[X,Y]/I^n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Hence,

$$\dim_k(k[X,Y]/(I^n, F)) = nm - \frac{m(m-1)}{2} = nm_p(F) + s$$

for all $n \geq m$ and $s = -\frac{m(m-1}{2}$ is fixed constant as $m = m_P(F)$ is fixed. □

Theorem 4.0.17. *P is a simple point of F if and only if $\mathscr{O}_P(F)$ is a discrete valuation ring (i.e. $\mathscr{O}_P(F)$ is Noetherian local domain and the maximal ideal is principal).*

Proof. Suppose P is a simple point on F and L is the line through P, not tangent to F at P. By making affine change of coordinates (cf. appendix problem 7.2.2), we may assume that $P = (0,0)$, $L = X$ and $Y = 0$ is the tangent line.
By Proposition 3.3.2, $\mathscr{O}_P(F)$ is Noetherian local domain. We have to only show that its maximal ideal is principal.
Since, $\mathfrak{m}_P(F)$ consist of all rational functions that vanish at $P = (0,0)$, $\mathfrak{m}_P(F) = (\overline{X}, \overline{Y})$. Also $F = Y +$ *higher degree terms*, as Y is assumed to be the tangent line of F. Taking terms of Y together, we have $F = YG - X^2H$, where $G = 1 +$ *higher degree terms* and $H \in k[X]$. Then $\overline{YG} = \overline{X^2H} \in \Gamma(F)$. So, $\overline{Y} = \overline{X^2HG^{-1}} \in (\overline{X})$ (as $G(P) \neq 0$). Thus, $\mathfrak{m}_P(F) = (\overline{X})$.
If $\mathscr{O}_P(F)$ is Discrete Valuation Ring, then $\mathfrak{m}_P(F)$ is principal. Therefore by previous Theorem, $m_P(F) = 1$. Thus P is a simple point of F. □

Definition 33. Let $P \in \mathbb{A}^2$ and F, G be plane curves. F and G **intersect properly** at P if F and G have no common components that passes through P.

To define the intersection number denoted by $I(P, F \cap G)$, we require following conditions to hold:

1. If F and G intersect properly at P, then $I(P, F \cap G)$ is a non negative integer, else $I(P, F \cap G) = \infty$.

2. $I(P, F \cap G) = 0$ if and only if $P \notin V(F) \cap V(G)$.

3. If T is the change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

4. $I(P, F \cap G) = I(P, G \cap F)$.

5. $I(P, F \cap G) \geq m_p(F) m_P(G)$, with equality occurring if and only if F and G have no tangent lines in common at P.

6. If $F = \prod F_i^{r_i}$ and $G = \prod G_j^{s_j}$, then $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F \cap G)$.

7. $I(P, F \cap G) = I(P, F \cap (G + AF))$ for any $A \in k[X, Y]$.

Now, we will show that this intersection number exists and is unique. We will first prove few lemmas needed to proof the existence part of intersection multiplicity.

Lemma 4.0.18. *Let $I = (X, Y)$ and $F, G \in k[X, Y]$ containing $P = (0, 0)$. We assume that F and G have no common components. Let m and n be multiplicities of f and g respectively. Let*

$$\psi : k[X, Y]/I^n \times k[X, Y]/I^m \longrightarrow k[X, Y]/I^{m+n}$$

$$\psi(\overline{A}, \overline{B}) = \overline{AF + BG}$$

Then

1. *If F and G have no common tangents at P, then $I^t \subset (F, G)\mathscr{O}_P(\mathbb{A}^2)$ for $t \geq m + n - 1$.*

2. *ψ is one-to-one if and only if F and G have distinct tangents at P.*

Proof. **(1):** Let $L_1, \ldots, L_m$ be the tangents to F at P, $M_1, \ldots, M_n$ be the tangents to G at P. Take $L_1 = L_m$ for $i > m$, $M_j = M_n$ if $j > n$ and $A_{ij} = L_1 \ldots L_i, M_1 \ldots M_j$ for all $i, j \geq 0$ ($A_{00} = 1$). Let V_t denote the vector space consisting of all forms of degree t in $k[X, Y]$. $B_t = \{A_{ij} \mid i + j = t\}$ forms a basis for V_t (as the set is linearly independent and the cardinality is $t + 1$). So, $I^t =< B_t >$. So it is enough to show that $B_t \subset (F, G)\mathscr{O}_P(\mathbb{A}^2)$ for $t \geq m + n - 1$. Now, if $i + j \geq m + n - 1$ then either $i \geq m$ or $j \geq n$. We assume, without loss of generality, that $i \geq m$. So, we have $A_{ij} = A_{m0} B$, where B is a form of degree of degree $i + j - m$. We can write

$F = A_{m0} + F'$, where all terms of F' are of degree $\geq m+1$. Then $A_{ij} = BF - BF'$, where each term of BF' has degree $\geq i+j+1$. Since, $BF \in (F,G)\mathscr{O}_P(\mathbb{A}^2)$, we need to show that $BF' \in (F,G)\mathscr{O}_P(\mathbb{A}^2)$ (As then repeating the process finitely many times we get the forms of higher and higher degree that should belong to $(F,G)\mathscr{O}_P(\mathbb{A}^2)$). Also, $BF' \in (B_{t+1})$. Therefore, it is enough to show that $B_{t+1} \subset (F,G)\mathscr{O}_P(\mathbb{A}^2)$, i.e. there exists some N such that $I^N \subset (F,G)\mathscr{O}_P(\mathbb{A}^2)$.
Let $V(F,G) = \{P, P_1, \ldots, P_s\}$. Let $P_i = (P_{i1}, P_{i2})$ with $P_{ij} \in k$ for every $i = 1, \ldots, s$ and $j = 1, 2$. We consider the polynomials:

$$H = \prod_{i=1}^{s} [(X - P_{i1}) + (Y - P_{i2})]$$

$H(P_i) = 0, \forall i = 1, \ldots, s$ and $H(P) \neq 0$. We have $HX, HY \in I(V(F,G))$. Therefore, by Hilbert's Nullstellensatz, there exists N such that $(HX)^N, (HY)^N \in (F,G) \subset k[X,Y]$. Since, $H(P) \neq 0 \Rightarrow H^N(P) \neq 0$, H^N is a unit in $\mathscr{O}_P(\mathbb{A}^2)$. Thus, X^N and Y^N are in $(F,G)\mathscr{O}_P(\mathbb{A}^2)$. Thus, $I^{2N} \subset (F,G)\mathscr{O}_P(\mathbb{A}^2)$ proving our claim.
Proof of (2): Suppose the tangents are distinct and $\psi(\overline{A}, \overline{B}) = \overline{AF + BG} = 0$. Then $Af + BG$ consists entirely of terms of degree $\geq m+n$. Let $A = A_r +$ higher terms $(r < m)$, $B = B_s +$ higher terms $(s < n)$. So, $AF + BG = A_rF_m + B_sG_n +$ higher terms. Then we must have $r + m = s + n$ and $A_rF_m = -B_sG_n$. Since, F and G have no common tangents at P, we can say that F_m divides B_s and G_n divides A_r. Therefore, $s \geq m, r \geq n$, so $(\overline{A}, \overline{B}) = (0,0)$.
Conversely, if L is a common tangent to F and G at P, we can write $F_m = LF'_{m-1}$ and $G_n = LG'_{n-1}$, where F'_{m-1}, G'_{n-1} are forms of degree $m-1$ and $n-1$. Then $\psi(\overline{G'_{n-1}}, -\overline{F'_{m-1}}) = 0$, so ψ is not one-to-one. $\square$

Theorem 4.0.19. *There exists a unique intersection number $I(P, F \cap G)$ defined for all plane curves F and G and all points $P \in \mathbb{A}^2$, satisfying properties* (1) *to* (7) *stated above. It is given by the formula*

$$I(P, F \cap G) = \dim_k(\mathscr{O}_P(\mathbb{A})^2)/(F,G)$$

Proof. (*Uniqueness*:) Without loss of generality we can assume $P = (0,0)$. Let F and G intersect properly at P so that the intersection number is unique. By property 2, the intersection number is 0 if the two curves do not intersect at P, i.e. $P \notin V(F) \cap V(G)$. So in both the cases, the intersection number is unique. We assume $I(P, F \cap G) = n$

and by induction hypothesis, we have already verified it for the $< n$ case (for $n = 0$, it is trivially true by property 2).
Suppose $F(X,0) = 0$. Then Y divides F. Hence, $F = YH$ for some $H \in k[X,Y]$. By property 6, $I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G)$. Note that $G(X,0) \neq 0$ as otherwise Y will be a common component of F and G contradicting the assumption. We have $I(P, Y \cap G) = I(P, Y \cap (G + AY))$ for any $A \in k[X,Y]$. By property 7, taking $a = \frac{G(X,0)-G}{Y}$ we get $I(P, Y \cap G) = I(P, Y \cap G(X,0))$. Therefore, if $G(X,0) = X^m(a_0 + a_1X + \cdots + a_tX^t)$, $a_0 \neq 0$ and $t > 0$, then

$$I(P, Y \cap G) = I(P, Y \cap G(X,0)) = I(P, Y \cap X^m(a_0 + a_1X + \cdots + a_tX^t)) = I(P, Y \cap X^m)$$

Last equality is due to property 2. Since, $I(P, Y \cap G) \neq 0$, $I(P, H \cap G) < n$. By induction hypothesis, it is unique.
If $F(X,0) \neq 0$ and $G(X,0) \neq 0$. Let r and s be degrees of F and G respectively and without loss of generality we assume that $r \leq s$. By multiplying F and G by suitable constants, we can assume that $F(X,0)$ and $G(X,0)$ are monic. We consider $H = G - X^{s-r}F$. Then, we have $I(P, F \cap G) = I(P, F \cap H)$ by property 7, and $\deg(H(X,0)) < s$. Repeating the process finite number of times, we get a pair of curves A and B such that $I(P, F \cap G) = I(P, A \cap B)$, and either $A(X,0) = 0$ or $B(X,0) = 0$. Thus, repeating the previous paragraph steps, we can say that $I(P, F \cap G)$ is unique in this case also.
Existence: We have to show that

$$I(P, F \cap G) = \dim_k(\mathscr{O}_P(k^2)/(F,G))$$

satisfy all seven properties defined above for intersection number.
By Proposition 4.0.12, $V(F,G)$ is finite if they do not have any common component. And by Proposition 4.0.13, $\dim_k(\mathscr{O}_P(k^2)/(F,G))$ is finite. In case F and G have common component say H, then $(F,G) \subset (H)$, there exists a homomorphism from $\mathscr{O}_P(k^2)/(F,G)$ to $\mathscr{O}_P(k^2)/(H)$. So, $I(P, F \cap G) \geq \dim_k(\mathscr{O}_P(k^2)/(H))$. But by Lemma 4.0.15, $\mathscr{O}_P(k^2)/(H)$ is isomorphic to $\mathscr{O}_P(H)$. Since, $\Gamma(H) \subset \mathscr{O}_P(H)$ and $\Gamma(H)$ is infinite dimensional, by Corollary 3.4.9, property 1 follows. Property 4 and 7 are easily satisfied as intersection number depends only on the ideal generated by F and G. Property 3 follows from Lemma 4.0.11 (As, affine change of coordinates give an isomorphism of local rings).is just the affine change of coordinates (cf. Appendix

problem 7.2.2).
To prove property 2, Suppose $I(P, F \cap G) = 0$, i.e. $\mathscr{O}_P(k^2) = (F, G)$. Now, if $P \in F \cap G$ then (F, G) is contained in $\mathfrak{m}_P(k^2)$ which is a contradiction. Hence, $P \notin F \cap G$. Conversely, if $P \in F \cap G$ then (F, G) is contained in the $\mathfrak{m}_P(k^2)$. So, $(F, G) \neq \mathscr{O}_P(k^2)$, hence, $I(P, F \cap G) \neq 0$ satisfying property 2.
To prove property 6, it is enough to show that

$$I(P, F \cap GH) = I(P, F \cap G) + I(P, F \cap H)$$

(By induction on the number of components, property 6 follows). We may assume that F and GH have no common components, else it is obvious. Let

$$\phi : \mathscr{O}_P(k^2)/(F, GH) \to \mathscr{O}_P(k^2)/(F, G)$$

be the natural homomorphism. It is surjective map. Define a k-linear map

$$\psi : \mathscr{O}_P(k^2)/(F, H) \to \mathscr{O}_P(k^2)/(F, GH)$$

$$\psi(\overline{Z}) = \overline{GZ}$$

where $Z \in \mathscr{O}_P(k^2)$. We are done if we show that the following sequence is exact.

$$0 \to \mathscr{O}_P(k^2)/(F, H) \xrightarrow{\psi} \mathscr{O}_P(k^2)/(F, GH) \xrightarrow{\phi} \mathscr{O}_P(k^2)/(F, G)$$

Let $\psi(\overline{Z}) = 0$, i.e. $GZ = UF + VGH$, where $U, V \in \mathscr{O}_P(k^2)$. Choose $S \in k[X, Y]$ with $S(P) \neq 0$ and $SU = A$, $SV = B$ and $SZ = C$, where $A, B, C \in k[X, Y]$. Then $G(C - BH) = AF$. Since F and G have no common factor, F must divide $C - BH$, so that $C - BH = DF$. Then $Z = (B/S)H + (D/S)F$, hence $\overline{Z} = 0$, which implies ψ is injective. Let $\overline{Z} \in ker(\phi)$, i.e. $\phi(\overline{Z}) = \overline{0}$. Hence, $\phi(Z + (F, GH)) = Z + (F, G) = (F, G)$. So there exist $A, B \in \mathscr{O}_P(k^2)$ such that $Z = FA + GB$. Hence $\overline{Z} = GB + (F, GH) = \psi(B + (F, H))$. Thus $\overline{Z} \in image(\psi)$. Conversely, let $\overline{Z} \in image(\psi)$, then there exists $b \in \mathscr{O}_P(k^2)$ such that $\psi(B + (F, H)) = GB + (F, GH) = \overline{Z}$. We consider, $\phi(GB + (F, GH)) = GB + (F, G) = 0 + (F, G)$. Thus, $ker(\phi) = image(\psi)$. Hence, the sequence is exact.
To prove property 5, Let $m = m_P(F)$, $n = m_P(G)$ and $I = (X, Y)$. We consider the

sequence

$$k[X,Y]/I^n \times k[X,Y]/I^m \xrightarrow{\psi} k[X,Y]/I^{m+n} \xrightarrow{\phi} k[X,Y]/(I^{m+n}, F, G) \to 0$$

where $\psi(\overline{A}, \overline{B}) = \overline{AF + BG}$ and $\phi(\overline{A}) = \overline{A}$. We will show that this sequence is exact. Let $\overline{H} \in ker(\phi)$, then $H = A + CF + DG$, for some $A \in I^{m+n}$, $C, D \in k[X,Y]$. Thus, in $k[X,Y]/I^{m+n}$, $\overline{H} = \psi(\overline{C}, \overline{D}) \in image(\psi)$. Conversely, let $\overline{H} \in image(\psi)$. Then, there exist $\overline{C}, \overline{D} \in k[X,Y]$ such that $\psi(\overline{C}, \overline{D}) = \overline{H}$, i.e. $\overline{H} = \overline{FC + DG}$. Hence, $\overline{H} \in ker(\phi)$. Also, ϕ is surjective. Thus, the sequence is exact. Now we consider,

$$k[X,Y]/(I^{m+n}, F, G) \xrightarrow{\alpha} \mathscr{O}_P(k^2)/(I^{m+n}, F, G)$$

where $\alpha(\overline{a}) = \overline{a}/\overline{1}$. We have $V((I^{m+n}, F, G)) = \{P\}$. Therefore, by Proposition 4.0.13, α is an isomorphism. We consider the natural surjective map π,

$$\mathscr{O}_P(k^2)/(F,G) \xrightarrow{\pi} \mathscr{O}_P(k^2)/(I^{m+n}, F, G) \to 0$$

where $\pi(\alpha(a)) = \overline{a}$. π is onto map. From the above exact sequence, we have

$$\dim(k[X,Y]/I^n) + \dim(k[X,Y]/I^m) \geq \dim(ker(\alpha)) = \dim(image(\alpha))$$

Equality holds if ψ is one-one. Putting all these together, we get

$$\begin{aligned}
I(P, F \cap G) &= \dim(\mathscr{O}_P(k^2)/(F,G)) \\
&\geq \dim(\mathscr{O}_P(k^2)/(I^{m+n}, F, G)) \\
&= \dim(k[X,Y]/(I^{m+n}, F, G)) \\
&\geq \dim(k[X,Y]/I^{m+n}) - \dim(k[X,Y]/I^n) - \dim(k[X,Y]/I^m) \\
&= mn
\end{aligned}$$

This shows that $I(P, F \cap G) \geq mn$, and that $I(P, F \cap G) = mn$ if and only if both inequalities are equality, i.e. if and only if π is an isomorphism ($I^{m+n} \subset (F,G)\mathscr{O}_P(k^2)$) and ψ is one-one. Now, property 5 follows directly from Lemma 4.0.18. $\square$

Corollary 4.0.20. *If F and G have no common components, then*

$$\sum_P I(P, F \cap G) = \dim_k(k[X,Y]/(F,G))$$

Proof. This follows from Proposition 4.0.13 $\square$

Chapter 5

Projective Geometry

Suppose we want to study all points of intersection of two curves. In $\mathbb{R}^2$, it may not be always true that two curves intersect. For example, two parallel lines do not intersect in real plane. So, we want to extend our plane so as to include the points where any two curves intersect. This can be done by including the points at infinity in real plane. One way to achieve this is: We consider all lines in $\mathbb{R}^3$ passing through origin. Each point $(x, y) \in \mathbb{R}^2$ can be identified with the line passing through $(0, 0, 0)$ and $(x, y, 1)$ in $\mathbb{R}^3$. These includes all lines through origin except those lying in the plane $z = 0$ which can be thought of as "points at infinity". Following section will give the formal definition of projective geometry and projective varieties.

5.1 Introduction

Definition 34. The set of all one dimensional subspaces of the vector space k^{n+1} (set of all lines through origin in k^{n+1}) over a field k is called **projective n-space**. It is denoted by $\mathbb{P}^n$. Equivalently, $\mathbb{P}^n$ is the quotient of $k^{n+1} - (0, 0, 0)$ by the action: $(a_1, \ldots, a_{n+1}) \sim (b_1, \ldots, b_{n+1}) \in \mathbb{P}^n$ if and only if there exists some $\lambda \in k$, $\lambda \neq 0$ such that $(a_1, \ldots, a_{n+1}) = \lambda(b_1, \ldots, b_{n+1})$. The equivalence class $[a_1 : a_2 : \ldots : a_{n+1}] \in \mathbb{P}^n$ denotes the set containing $(a_1, a_2, \ldots, a_{n+1})$.

If a point $P \in \mathbb{P}^n$ is determined as above by some $(x_1, \ldots, x_n) \in \mathbb{A}^{n+1}$, we say that $(x_1, \ldots, x_{n+1})$ are **homogeneous coordinates** for P. We let

$$U_i = \{[x_1 : \ldots : x_{n+1}] \in \mathbb{P}^n | x_i \neq 0\}$$

Each $P \in U_i$ can be uniquely written in the form

$$P = [x_1 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_{n+1}]$$

The coordinates $(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_{n+1})$ are called **non-homogeneous coordinates** for P with respect to U_i. If we define $\phi_i : \mathbb{A}^n \to U_i$ by

$$\phi_i(a_1, \ldots, a_n) = [x_1 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_{n+1}]$$

then ϕ_i sets up one-to-one correspondence between the points of $\mathbb{A}^n$ and the points of U_i. Thus, $\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i$. Let

$$H_\infty = \mathbb{P}^n - U_{n+1} = \{[x_1 : \ldots : x_{n+1}] | x_{n+1} = 0\}$$

H_∞ is called **hyperplane at infinity**. The correspondence

$$[x_1 : \ldots : x_n : 0] \leftrightarrow [x_1 : \ldots : x_n]$$

shows that H_∞ can be identified with P^{n-1}. Thus **projective n-space can be identified as**

$$\mathbb{P}^n = U_{n+1} \cup H_\infty$$

the union of an affine n-space and a set that gives all directions in affine n-space. For convenience we usually concentrate on U_{n+1}.

In general $F \in k[X_1, \ldots, X_{n+1}]$ is not a well defined function on $\mathbb{P}^n$, as, if $[x_1 : \ldots : x_{n+1}]$ are homogeneous coordinates of P and $F(x_1, \ldots, x_{n+1}) = 0$, it may not be true that $F(\lambda x_1, \ldots, \lambda x_{n+1}) = 0$ for every $\lambda \in k - \{0\}$. To satisfy this, F must be a homogeneous function (i.e. each term in F must have same degree say d). Then, a point $P \in \mathbb{P}^n$ is said to be a zero of a homogeneous polynomial $F \in k[X_1, \ldots, X_{n+1}]$ if $F(x_1, \ldots, x_{n+1}) = 0$ for every choice of homogeneous coordinates $(x_1, \ldots, x_{n+1})$ for P, i.e. $F(P) = 0$.

For any set S of polynomials in $k[X_1, \ldots, X_{n+1}]$, we let

$$V(S) = \{P \in \mathbb{P}^n | P \textit{ is a zero of each } F \in S\}$$

If I is the ideal generated by S, $V(I) = V(S)$. If $I = (F^{(1)}, \ldots, F^{(r)})$, where $F^{(i)} =$

$\sum F_j^{(i)}$, then $V(S) = V(\{F_j^{(i)}\})$ is the set of forms of a finite number of forms. Such a set is called an **algebraic set** in $\mathbb{P}^n$ or **projective algebraic set**. An ideal I is called **homogeneous** if for every $F = \sum_{i=0}^{m} F_i \in I$, F_i a form of degree i and $F_i \in I$.

Proposition 5.1.1. *An ideal $I \subset k[X_1, \ldots, X_{n+1}]$ is homogeneous if and only if it is generated by a finite set of forms.*

Proof. If $I = (F^{(1)}, \ldots, F^{(r)})$ is homogeneous, then I is generated by $\{F_j^{(i)}\}$. Conversely, let $S = \{F^{(\alpha)}\}$ be a set of forms generating an ideal I, with $\deg(F^{(\alpha)}) = d_\alpha$, and suppose $F = F_m + \cdots + F_r \in I$, $\deg(F_i) = i$. It suffices to show that $F_m \in I$, for then $F - F_m \in I$ and an inductive argument finishes the proof. Write $F = \sum A^{(\alpha)} F^{(\alpha)}$. Comparing terms of the same degree, we can conclude that $F_m = \sum A^{(\alpha)} F^{(\alpha)}$, so $F_m \in I$. $\square$

Note. ***The concepts and idea are almost similar in case of projective algebraic sets to those of affine algebraic sets***.

Notation 3. *To avoid the confusion of notation in projective case and affine case, we will write V_P, I_P for the projective operations , V_a, I_a for the affine case*

An algebraic set $V \subset \mathbb{P}^n$ is **irreducible** if it is not the union of two algebraic sets. As in the affine case, V is irreducible if and only if $I(V)$ is prime. An irreducible algebraic set in $\mathbb{P}^n$ is called a **projective variety**. Any algebraic set can be uniquely written as a union of projective varieties.

Notation 4. *To avoid the confusion of notation in projective case and affine case, we will write V_P, I_P for the projective operations , V_a, I_a for the affine case*

If V is an algebraic set in $\mathbb{P}^n$, we define

$$C(V) = \{(x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1} | [x_1 : \ldots : x_{n+1}] \in V \text{ or } (x_1, \ldots, x_{n+1}) = (0, \ldots, 0)\}$$

to be the **cone** over V. If $V \neq \phi$, then $I_a(C(V)) = I_P(V)$ and if I is a homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$ such that $V_P(I) \neq \phi$, then $C(V_P(I)) = V_a(I)$. Now, we will see the projective analogue of Hilbert's Nullstellensatz Theorem.

Theorem 5.1.2. ***Projective Nullstellensatz:*** *Let I be a homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$. Then*

1. *$V_P(I) = \Phi$ if and only if there is an integer N such that I contains all forms of degree $\geq N$.*

2. *If $V_P(I) \neq \Phi$, then $I_P(V_P(I)) = \sqrt{I}$.*

Proof. Let $\pi : k^{n+1} - \{0\} \to \mathbb{P}^n$ be the map defining $\mathbb{P}^n$. For a homogeneous ideal $I \subset k[X_1, \ldots, X_{n+1}]$, we consider $V_a(I) \subset k^{n+1}$ and $V_P(I) = (V_a(I) - \{0\})/\sim \subset \mathbb{P}^n$. Then, $V_P(I) = \Phi$ if and only if $V(I) \subset \{0\}$ if and only if $(X_1, \ldots, X_{n+1}) \subset \sqrt{I}$ (By Hilbert's Nullstellensatz Theorem in affine case). Thus, there exists N such that I contains all forms of degree $\geq N$. Also, if $V_P(I) \neq \Phi$, then $I_P(V_P(I)) = I_a(C(V_P(I))) = I_a(V_a(I)) = \sqrt{I}$. $\square$

The usual corollaries of Hilbert's Nullstellensatz Theorem go through except that we must always make an exception with the ideal $(X_1, \ldots, X_n)$. In particular, there is one-to-one correspondence between **projective hypersurfaces** $V = V(F)$ and the forms F that define V, provided F has no multiple factors. A **hyperplane** is a hypersurface defined by a form of degree one. The hyperplanes $V(X_i)$, $i = 1, \ldots, n+1$, are called **hyperplanes at infinity** with respect to U_i.

Let V be a nonempty projective variety in $\mathbb{P}^n$. Then $\Gamma_h(V) = k[X_1, \ldots, X_{n+1}]/I(V)$ is called **homogeneous coordinate ring** of V. Let I be any homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$ and $\Gamma = k[X_1, \ldots, X_{n+1}]/I$. An element $f \in \Gamma$ is called a **form** of degree d if there is a form F of degree d in $k[X_1, \ldots, X_{n+1}]$ whose residue is f.

Let $V_P \subset \mathbb{P}^n$ be an irreducible algebraic subset. An element $F \subset k[X_1, \ldots, X_{n+1}]$ gives a function on $C(V)$, but this will be a function on V_P only if F is homogeneous of degree 0 (the equivalence condition will create problem). However, if f, g are both forms in $\Gamma_h(V)$ of the same degree, then f/g does define a function, when g is not zero (as then $f(\lambda x)/g(\lambda x) = \lambda^d f(x)/\lambda^d g(x) = f(x)/g(x)$, so the value of f/g is independent of the choice of homogeneous coordinates). The **function field** of V, written $k(V)$, is defined as

$$k(V) = \{z \in k_h(V) |\ for\ some\ forms\ f, g\ of\ the\ same\ degree,\ z = f/g\}$$

Elements of $k(V)$ are called **rational function** on V. Let $P \in V$, $z \in k(V)$. We say z is defined at P if z can be written as $z = f/g$, f,g forms of same degree, $g(P) \neq 0$.

We define

$$\mathscr{O}_P(V) = \{z \in k(V) | z \text{ is defined at } P\}$$

$\mathscr{O}_P(V)$ is a local ring (called Local ring of V at P) with maximal ideal

$$\mathfrak{m}_P(V) = \{z | z = f/g,\ g(P) \neq 0, f(P) = 0\}$$

If $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ is a linear change of coordinates, then T takes lines through the origin into lines through the origin. So, T determines a map from $\mathbb{P}^n \to \mathbb{P}^n$, called as **projective change of coordinates**. V is a variety if and only if $T^{-1}(V)$ (denoted by V^T) is a algebraic set in $\mathbb{P}^n$. If $V = V(F_1, \dots, F_r)$ and $T = (T_1, \dots, T_{n+1})$, T_i forms of degree 1, then $V^T = V(F_1^T, \dots, F_r^T)$, where $F_i^T = F_i(T_1, \dots, T_{n+1})$. If V is a variety, T induces an isomorphism from $\Gamma_h(V)$ to $\Gamma_h(V^T)$, $k(V)$ to $k(V^T)$ and $\mathscr{O}_P(V)$ to $\mathscr{O}_Q(V^T)$, where $T(P) = Q$.

5.2 Properties of Projective Varieties

If $F \in k[X_1, \dots, X_{n+1}]$ is a form, we define $F_* \in k[X_1, \dots, X_n]$ be setting $F_* = F(X_1, \dots, X_n, 1)$. Conversely, for any polynomial $f \in k[X_1, \dots, X_n]$ of degree d, write $f = f_0 + f_1 + \cdots + f_d$, where f_i is a form of degree i, and define $f^* \in k[X_1, \dots, X_{n+1}]$ by

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + f_d = X_{n+1}^d f(X_1/X_{n+1}, \dots, X_n/X_{n+1})$$

Let V be an algebraic set in $\mathbb{A}^n$, $I = I(V)$. Let I^* be the ideal in $k[X_1, \dots, X_{n+1}]$ generated by $\{F_* \mid F \in I\}$. $V(I^*) \subset \mathbb{P}^n$. I^* is a homogeneous ideal. Conversely, let V be an algebraic set in $\mathbb{P}^n$, $I = I(V)$. let I_* be the ideal in $k[X_1, \dots, X_n]$ generated by $\{F_* \mid F \in I\}$. $V_* = V(I_*)$.

We consider $\mathbb{A}^n$ as a subset of $\mathbb{P}^n$ by means of the map $\phi_{n+1} : \mathbb{A}^n \to U_{n+1} \subset \mathbb{P}^n$.

Proposition 5.2.1. 1. *If $V \subset \mathbb{A}^n$, then $\phi_{n+1}(V) = V^* \cap U_{n+1}$, and $(V^*)_* = V$.*

2. *If $V \subset W \subset \mathbb{A}^n$, then $V^* \subset W^* \subset \mathbb{P}^n$. If $V \subset W \subset \mathbb{P}^n$, then $V_* \subset W_* \subset \mathbb{A}^n$*

3. *If V is irreducible in $\mathbb{A}^n$, then V^* is irreducible in $\mathbb{P}^n$.*

4. *If $V = \cup_i V_i$ is the irreducible decomposition of V in $\mathbb{A}^n$, then $V^* = \cup_i V_i^*$ is the irreducible decomposition of V^* in $\mathbb{P}^n$.*

5. *If $V \subset \mathbb{A}^n$, then V^* is the smallest algebraic set in $\mathbb{P}^n$ that contains $\phi_{n+1}(V)$.*

6. *If $V \subset \mathbb{A}^n$ (proper and nonempty), and no component of V^* lies in or contain H_∞, then $V_* \subset \mathbb{A}^n$ (proper) and $(V_*)^* = V$.*

7. *If $V \subset \mathbb{P}^n$, and no component of V lies in or contain H_∞, then $V_* \subsetneq \mathbb{A}^n$ and $(V_*)^* = V$.*

Proof. Let $I(V) = V$. Since $(f^*)_* = f$, $(I^*)_* = I$. $(V^*)_* = V$ can be easily checked. Let P be the image of $(a_1, \ldots, a_n) \in V$. To show that $P \in V^*$, i.e. $f^*(P) = 0$ for every $f^* \in I^*$. We have $f^* = X_{n+1}^d f(X_1/X_{n+1}, \ldots, X_n/X_{n+1})$. $f^*(P) = 1^d f(a_1, \ldots, a_n) = 0$. Thus, $f^*(P) = 0$. Conversely, if $[a_1 : \ldots : a_{n+1}] \in V^*$, then $(a_1, \ldots, a_n) \in (V^*)_* = V$. Thus, (1) follows. (2) can be easily checked. Let $I = I(V)$ is prime. Let $FG \in I^*$. Then it can be easily checked that $(FG)_* = F_*G_* \in I \Rightarrow F_* \in I$ or $G_* \in I$. Thus, $(F_*)^* = F \in I^*$ or $(G_*)^* = G \in I^*$.Thus, follows (3). Suppose W is an algebraic set in $\mathbb{P}^n$ that contains $\phi_{n+1}(V)$. So, $W \subset V^* \Rightarrow I(V^*) \subset I(W)$. If $F \in I(W)$, then $F_* \in I(V)$, so $F = X_{n+1}^r (F_*)^* \in I(V)^*$. Therefore, $I(W) \subset I(V)^*$, so $W \supset V^*$. Thus follows (5). (4) follows from (2),(3) and (5).
To prove (6), we can assume that V is irreducible. If $V^* \subset H_\infty = \mathbb{P}^n - U_{n+1}$, then by (1), $\phi_{n+1}(V)$ is empty, which is a contradiction. So, $V^* \not\subseteq H_\infty$. If $V^* \supset H_\infty$, then $I(V)^* \subset I(V^*) \subset I(V^*) \subset I(H_\infty) = (X_{n+1})$. But, if $F \in I(V)$ $(F \neq 0)$, then $F^* \notin (X_{n+1})$ and $F^* \in I(V)^*$. So, $V^* \not\supseteq H_\infty$ proving (6).
To prove (7), we assume $V \subset \mathbb{P}^n$ is irreducible. Since, $\phi_{n+1}(V_*) \subset V$, it suffices to show that $V \subset (V_*)^*$, i.e. $I(V_*)^* \subset I(V)$. Let $F \in I(V_*)$, then $F^N \in I(V)_*$ for some N (Hilbert's Nullstellensatz Theorem), so $X_{n+1}^t (F^N)^* \in I(V)$ for some t. But $I(V)$ is prime, and $X_{n+1} \notin I(V)$ since $V \not\subseteq I(V)$, $F^* \in I(V)$, thus proving (7). $\square$

If V is an algebraic set in $\mathbb{A}^n$, $V^* \subset \mathbb{P}^n$ is called the **projective closure** of V.

Chapter 6

Bezout's Theorem for Projective Plane Curves

A projective plane curve is a hypersurface in $\mathbb{P}^2$. In fact, a projective plane curve is an equivalence class where any two non-constant forms $F, G \in k[X, Y, Z]$ are equivalent if there is a non-zero $\lambda \in k$ such that $G = \lambda F$. Notations and conventions are as described for affine curves in section 4.

Lemma 6.0.2. *Show that for any finite set of points $\{P_1, \ldots, P_n\}$ in $\mathbb{P}^2$, there is a line not passing through any of them.*

Proof. Since, $\mathbb{P}^2$ can be identified with points of $\mathbb{A}^2$ ($\{(a, b, 1) \mid (a, b) \in \mathbb{A}^2\}$) and points of infinity ($\{(a, b, 0) \mid (a, b) \in \mathbb{P}^1\}$). Let $\{P_1, \ldots, P_r\}$ be points of the type $(a_i, b_i, 1)$ and $\{P_{r+1}, \ldots, P_n\}$ be points of the type $(c_i, d_i, 0)$. We assume $L : \alpha X + \beta Y + \gamma Z = 0$ be a line such that it does not pass through P_i's for all $1 \leq i \leq n$. There exists a point $P = (a, b, 0) \in \mathbb{P}^2$ such that $P \in L$ and $P \neq P_j$ for all $(r + 1) \leq j \leq n$ (such a point is possible, because there are infinite points of the form $(a, b, 0)$ in $\mathbb{P}^2$). So $\alpha a + \beta b = 0$ and $(a, b) \neq (c_i, d_i)$ for all $(r + 1) \leq i \leq n$. So, P_i does not lie on L for all $(r + 1) \leq i \leq n$. Also, $\alpha = \lambda b$ and $\beta = -\lambda a$ for some $\lambda \neq 0$. If $P_i \in L$ for some $i \in \{1, \ldots, r\}$, we have $\lambda b a_i - \lambda a b_i + \gamma = 0$. Taking $\gamma \neq -\lambda b a_i + \lambda a b_i \in k$ for all $1 \leq i \leq r$ (such a λ exists because k is infinite). Thus, $P_i \notin L$ for all i. $\square$

By projective change of coordinates, we can take L to line of infinity Z.
Let F be a curve of degree d, let $F_* = \frac{F}{L^d} \in k(\mathbb{P}^2)$. This F_* depends on L. Suppose we have another line L' not passing through any of the points above, then $\frac{F}{(L')^d} = (\frac{L}{L'})^d F_*$

and $\frac{L}{L'}$ is a unit in each of $\mathscr{O}_{P_i}(\mathbb{P}^2)$. We will use notation F_* for suitable L. If L is the line at infinity, then $F_* = \frac{F}{Z^d} = F(\frac{X}{Z}, \frac{Y}{Z}, 1)$. Thus, under the natural identification of $k(\mathbb{A}^2)$ with $k(\mathbb{P}^2)$, F_* is same as we defined in previous section.
Let $P = (a, b, 1)$ be a point on a curve F. Now,

$$\mathscr{O}_P(F) = \left\{ \frac{H}{G} : G, H \in \Gamma_h(F),\ G, H \ homogeneous\ of\ same\ degree,\ G(P) \neq 0 \right\}$$

$$\mathscr{O}_{(a,b)}(F_*) = \big\{ \frac{H}{G} :\ G, H \in \Gamma(V(F_*)),\ G(P) \neq 0 \big\}$$

Let $\phi : \mathscr{O}_P(F) \to \mathscr{O}_{(a,b)}(F_*)$, $\phi(\frac{H}{G}) = \frac{H_*}{G_*}$. This is an isomorphism. Thus, $\mathscr{O}_P(F)$ is isomorphic to $\mathscr{O}_{(a,b)}(F_*)$.
By Theorem 4.0.16, multiplicity of a curve $m_P(F)$ depends only on the local ring of the curve at that point. So, if F is a projective plane curve, $P \in U_i$ $(i = 1, 2, 3)$, we can dehomogenize F with respect to X_i and define the **multiplicity** of F at P, $m_P(F) = m_p(F_*)$. The multiplicity is independent of the choice of U_i, and is invariant under projective change of coordinates.
Let F, G be projective plane curves, $P \in \mathbb{P}^2$. We define the intersection number as

$$I(P, F \cap G) = \dim_k(\mathscr{O}_P(\mathbb{P}^2)/(F_*, G_*))$$

This satisfies all the properties of intersection multiplicity defined in section 4 (T should be projective change of coordinates and A should be a form with $\deg(A) = \deg(G) - \deg(\mathrm{F})$). As defined in the affine case, in projective case also, a line L is tangent to F at P if and only if $I(P, F \cap L) > m_P(F)$ and a point P is an ordinary multiple point of F if and only if F has $m_P(F)$ distinct tangents at P.

Theorem 6.0.3. ***Bezout's Theorem:*** *Let F and G be projective plane curves of degree m and n respectively. We assume that F and G have no common component. Then*

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = mn$$

Proof. We have already shown that $F \cap G$ is finite if F and G having no common component. Also, we can assume that none of the points in $F \cap G$ lie on the line $Z = 0$ at infinity (by Lemma 6.0.2).

By Corollary 4.0.20, we have

$$\sum_P I(P, F \cap G) = \sum_P (I, F_* \cap G_*) = \dim_k(k[X,Y]/(F_*, G_*))$$

Let $\Gamma_* = k[X,Y]/(F_*, G_*)$, $\Gamma = k[X,Y,Z]/(F,G)$ and $R = k[X,Y,Z]$. Let Γ_d and R_d be the vector space of forms of degree d in Γ and R respectively. The Theorem will be proved if we show that $\dim \Gamma_* = \dim \Gamma_d = mn$ for some $d \gg 0$.
Let $\pi : R \to \Gamma$ be the natural map $H \mapsto H + (F,G)$. Let $\pi : R \times R \to R$ be defined by $\phi(A,B) = AF + BG$, and $\psi : R \to R \times R$ be defined by $\psi(C) = (GC, -FC)$. We consider the sequence:

$$0 \to R \xrightarrow{\psi} R \times R \xrightarrow{\phi} R \xrightarrow{\pi} \Gamma \to 0$$

Claim: This sequence is exact. Let $C \in R$. $\psi(C) = (GC, -FC) = (0,0)$. Since, any one of the two curve is non zero, $C = 0$. Hence, ψ is one-one. Let $(A,B) \in image(\psi)$, i.e. there exists $C \in R$ such that $(A,B) = (GC, -FC)$. Hence, $\psi(A,B) = \phi(GC, -FC) = 0$. Thus, $image(\psi) \subset ker(\phi)$. Conversely, let $(A,B) \in ker(\phi)$, i.e. $\phi(A,B) = AF + BG = 0 \Rightarrow AF = -BG$. Since F and G have no common component, F divides B and G divides A. Suppose $B = FC_1$ and $A = GC_2$. Thus, $GC_2F = -FC_1G \Rightarrow C_1 = -C_2$. Taking $C = C_2$, $\psi(C) = (A,B)$. Thus, $image(\psi) = ker(\phi)$. Also, π, as defined, is a onto map. Thus, the sequence is exact. If we restrict these maps to the forms of various degrees, we get the following exact sequences:

$$0 \to R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\phi} R_d \xrightarrow{\pi} \Gamma_d \to 0$$

as $\dim R_d = \frac{(d+1)(d+2)}{2}$ (as set of all monomials of degree d in R form a basis for R_d). Hence,

$$\dim(\Gamma_d) = \dim(R_d) - \dim(R_{d-m} \times R_{d-n}) + \dim(R_{d-m-n}) = mn$$

Thus, for all $d \geq m+n$, $\dim(\Gamma_d) = mn$.
We consider the map $\alpha : \Gamma \to \Gamma$ defined by $\alpha(\overline{H}) = \overline{ZH}$ (where bar denotes residue modulo (F,G)).
Claim: α is one-one. Let $\alpha(\overline{H}) = \overline{0}$, i.e. there exist $A, B \in R$ such that $ZH = AF + BG$. For $J \in R$, denote $J(X,Y,0) = J_0$. Thus, $ZH = AF + BG \Rightarrow A_0F_0 = -B_0G_0$.

Since, F and G have no common zeroes, F_0 and G_0 are relatively prime forms in $k[X,Y]$. So, $B_0 = F_0C$ and $A_0 = -G_0C$ for some $C \in k[X,Y]$. Let $A_1 = A + CG$ and $B_1 = B - CF$. Since $(A_1)_0 = (B_1)_0 = 0$, we have $A_1 = ZA'$ and $B_1 = ZB'$ for some A', B'. Thus,

$$ZH = AF + BG = (A_1 - CG)F + (B_1 + CF)G = A_1F + B_1G = ZA'F + ZB'G$$

Therefore, $H = A'F + B'G \Rightarrow \overline{H} = \overline{0}$. Hence, α is one-one.
We can restrict the map α from $\Gamma_d \to \Gamma_{d+1}$. This restricted map α_d (say) is an isomorphism if $d \geq m+n$ (Since, one-one linear map of vector spaces of same dimension is a vector space). Choose $A_1, \ldots, A_{mn} \in R_d$ whose residues in Γ_d form a basis for Γ_d. Let $A_{i*} = A_i(X,Y,1) \in k[X,Y]$, and let a_i be the residue of A_{i*} in Γ_*. Since, α_d is an isomorphism, the residues $Z^rA_1, \ldots, Z^rA_{mn}$ form a basis for Γ_{d+r} for all $r \geq 0$.
Claim: $a_1, \ldots, a_{mn}$ generate Γ_*. If $h = \overline{H} \in \Gamma_*$, $H \in k[X,Y]$, there exists some N such that Z^NH^* is a form of degree $d+r$. So, $Z^NH^* = \sum_{i=1}^{mn} \lambda_i Z^rA_i + BF + CG$ for some $\lambda_i \in k$, $B, C \in k[X,Y,Z]$. Then $H = (Z^NH*)_* = \sum_{i=1}^{mn} \lambda_i A_{i*} + B_*F_* + C_*G_*$ and hence $h = \sum_{i=1}^{mn} \lambda_i a_i$. Thus, $a_1, \ldots, a_{mn}$ generate Γ_*.
Claim: a_i's are linearly independent. Suppose $\lambda_i, \ldots, \lambda_{mn} \in k$ such that $\sum_{i=1}^{mn} \lambda_i A_{i*} = BF_* + CG_*$. Thus, there exist r, s, t such that $Z^r \sum_{i=1}^{mn} \lambda_i \overline{Z^rA_i} = Z^sB^*F + Z^tC^*G \Rightarrow \sum_{i=1}^{mn} \lambda_i \overline{Z^rA_i} = 0$ in Γ_{d+r}. But as we have proved earlier, $\overline{Z^rA_i}$ forms a basis for Γ_{d+r}. Thus, $\lambda_i = 0$ for all $i = 1, \ldots, mn$. Therefore, $a_1, \ldots, a_{mn}$ forms a basis for Γ_*; whence, $\dim_k \Gamma_* = mn$. This proves

$$\sum_P I(P, F \cap G) = \dim_k(k[X,Y]/(F_*, G_*)) = \dim(\Gamma_*) = mn$$

□

The following Corollary follows from property (5) of intersection multiplicity and Bezout's Theorem.

Corollary 6.0.4. *If F and G have no common component, then*

$$\sum_P m_P(F)m_P(G) \leq \deg(F) \cdot \deg(G)$$

Corollary 6.0.5. *If F and G meet in mn distinct points, $m = \deg(F)$, $n = \deg(G)$, then these points are all simple points on F and on G.*

Proof. Let $F \cap G = \{P_1, \ldots, P_{mn}\}$. By previous Corollary

$$mn = \deg(F) \cdot \deg(G) \geq \sum_{i=1}^{mn} m_{P_i}(F) m_{P_i}(G)$$

Last inequality is due to the fact that F and G meet at mn distinct points. Hence, $m_{P_i}(F) = 1$ and $m_{P_i}(G) = 1$ for all $i = 1, \ldots, mn$. □

The following Corollary directly follows from Bezout's Theorem.

Corollary 6.0.6. *If two curves of degrees m and n have more than mn points in common, then they have a common component.*

Chapter 7

Appendix

7.1 Affine Algebraic Sets

Problem 7.1.1. *Let R be a domain. (a) If F, G are forms of degree r, s respectively in $R[X_1, \ldots, X_n]$, show that FG is a form of degree $r+s$. (b) Show that any factor of a form in $R[X_1, \ldots, X_n]$ is a form.*

Solution. (a) F has all coefficients $a_{(i)} = 0$ except those having degree r. So F is of the form

$$F = \sum_{i_1+i_2+\ldots+i_n=r} a_{i_1 i_2 \ldots i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$$

where each i_k is a nonnegative integer. Similarly for G

$$F = \sum_{j_1+j_2+\ldots+j_n=s} a_{j_1 j_2 \ldots j_n} X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n}$$

In FG each term will be $a_{i_1 i_2 \ldots i_n} b_{j_1 j_2 \ldots j_n} X_1^{i_1+j_1} X_2^{i_2+j_2} \ldots X_n^{i_n+j_n}$. So, the degree of each term will be

$$(i_1+j_1)+(i_2+j_2)+\ldots+(i_n+j_n) = (i_1+i_2+\ldots+i_n)+(j_1+j_2+\ldots+j_n) = r+s$$

So, each term of FG has degree $r+s$. FG is a form of degree $r+s$.

(b) Let F be a form of degree d and $F = GH$. If G is not a form, it has monomial of degree r_1 and r_2 ($r_1 \neq r_2$). If H is a form of degree s, then F has monomials of degree r_1+s and r_2+s which are equal as F is a form $\Rightarrow r_1 = r_2$. If H is not a form, say, it has monomials of degree s_1 and s_2 ($s_1 \neq s_2$). So, F has monomials of degree $r_1 + s_1$, $r_1 + s_2$, $r_2 + s_1$ and $r_2 + s_2$. Since, F is a form

$$r_1 + s_1 = r_1 + s_2 = r_2 + s_1 = r_2 + s_2 = d \Rightarrow s_1 = s_2 \textit{ and } r_1 = r_2 \Rightarrow\Leftarrow$$

Thus both F and G are forms.

Problem 7.1.2. *Let R be a UFD, K the quotient field of R. Show that every element z of K may be written $z = a/b$, where $a, b \in R$ have no common factors; this representative is unique up to units in R.*

Solution. Every element z of K is of the form a/b, $a, b \in R$. Since, R is a UFD, $a = \alpha p_1^{r_1} \dots p_n^{r_n}$ and $b = \beta q_1^{s_1} \dots q_n^{s_m}$ (p_i's, q_i's are irreducible elements and α, β units). We can cancel out the common primes and get $z = a'/b'$, where a' and b' have no common factors.
(*Uniqueness*:) Let $z = a/b = c/d$, where a, b have no common factors and c, d have no common factors. Let $a = \alpha p_1 \dots p_n$, $b = \beta q_1 \dots q_m$, $c = \gamma p'_1 \dots p'_{n_1}$, $d = \delta q'_1 \dots q'_{m_1}$, where $\alpha, \beta, \gamma, \delta$ are units and p_i, q_i, p'_i, q'_i's are irreducible elements (may not be distinct).

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc$$
$$\Rightarrow \alpha\delta p_1 \dots p_n q'_1 \dots q'_{m_1} = \gamma\beta q_1 \dots q_m p'_1 \dots p'_{n_1}$$

In UFD, prime factorization is unique up to units. Thus, p_1 equals some q_i or p'_j. But, a and b have no common factors $\Rightarrow p_1 = p'_i$ for some i up to units. Thus, for every j, there exists i such that $p_j = p'_i$ up to units. Conversely, for every prime p'_i, there exists p_j such that $p'_i = p_j$ up to units. So, $a = c$ and $d = b$ up to units $\Rightarrow a/b$ is unique up to some units in R.

Problem 7.1.3. *Let R be a PID, Let P be a nonzero, proper, prime ideal in R. (a) Show that P is generated by an irreducible element. (b) Show that P is maximal.*

Solution. (a) Let $P = (a)$ for some $0 \neq a \in R$ (a non-unit). If a is reducible element, say, $a = bc$ (b and c both non-units) $\Rightarrow b \in P$ or $c \in P \Rightarrow b = ar$ or $c = as$ $r, s \in R$. Say $b \in P$, i.e. $b = ar = bcr \Rightarrow cr = 1$. Thus, c is a unit $\Rightarrow\Leftarrow$. So, P is generated by irreducible element.

(b) Let M is an ideal containing P

$$M = (m) \supset (a) = P \Rightarrow a = rm \ (r \in R)$$

But a is irreducible $\Rightarrow r$ or m is a unit $\Rightarrow M = P$ or $M = R \Rightarrow P$ is maximal ideal.

Problem 7.1.4. *Let k be an infinite field, $F \in k[X_1, \dots, X_n]$. Suppose $F(a_1, \dots, a_n) = 0$ for all $a_1 \dots, a_n \in k$. Show that $F = 0$.*

Solution. Let $n = 1$. $F \in k[X_1]$. let $F(a_1) = 0$ for all $a_1 \in k$. Since, F has infinite number of roots (k is infinite) $\Rightarrow F = 0$.
We assume induction hypothesis,

$$F(a_1, \dots, a_{n-1}) = 0 \ (\forall a_1, \dots, a_{n-1} \in k) \Rightarrow F = 0$$

$F(a_1, \dots, a_n) = 0$ for all $a_1, \dots, a_n \in k$ (given). F can be written as a polynomial in X_n over $k[X_1, \dots, X_{n-1}]$, i.e. $F = \sum_i F_i X_n^i$. So,

$$\sum_i F_i X_n^i = 0 \quad \forall a_n \in k \text{ and } F_i(a_1, \dots, a_{n-1}) = 0 \quad \forall a_1, \dots, a_{n-1} \in k$$

By induction hypothesis, $F_i = 0 \ (\forall i) \Rightarrow F = 0$.

Problem 7.1.5. *Let k be any field. Show that there are infinite number of irreducible monic polynomials in $k[X]$*

Solution. Let $F_1, \dots, F_n$ are all irreducible monic polynomials in $k[X]$. We consider the polynomial $F = (F_1 \dots F_{n+1}) + 1$. F is not irreducible (as $F \neq F_i \ \forall i$). So, there exists F_i such that $F_1 \mid F$. Also, $F_1 \mid F_1 \dots F_n$. $F_1 \mid 1 \Rightarrow\Leftarrow$. There are infinite number of irreducible monic polynomials in $k[X]$.

Problem 7.1.6. *Show that any algebraically closed field is infinite*

Solution. Let algebraically closed field k is finite. $a_1 \dots a_n \in k$ are all elements of k. We consider the irreducible monic polynomials $(X - a_i)$ $(\forall i)$. By previous problem, $F = (X - a_1)(X - a_2) \dots (X - a_n) + 1$ is irreducible. As k is algebraically closed, every polynomial with coefficients in k has a root in k. F has a root in k. But $a_1, a_2, \dots, a_n$ are not roots of F. $\Rightarrow\Leftarrow$ k is infinite.

Problem 7.1.7. *We will use induction hypothesis. Let k be a field. $F \in k[X_1 \dots, X_n]$, $a_1, \dots, a_n \in k$. (a) Show that*

$$F = \sum \lambda_{(i)}(X_1 - a_1)^{i1} \dots (X_n - a_n)^{i_n},\ \lambda_{(i)} \in k$$

(b) If $F(a_1, \dots, a_n) = 0$, Show that $F = \sum_{i=1}^{n} (X_i - a_i)G_i$ for some (not unique) G_i in $k[X_1 \dots X_n]$.

Solution. (a) We consider for $n = 1$. k is a field $\Rightarrow k[X]$ is a Euclidean domain. Considering $F = \sum_{i=0}^{d} b_i X^i \in k[X]$, $\deg(F) = d$.
By Euclidean domain property, $F = (X - a)q(X) + \lambda_0$ (where $a \in k$ and $\lambda_0 \in k$) Since, F has degree d, $q(X)$ has degree $< d$ say $(d - 1)$. Applying Euclidean domain property on $q(X)$ and continuing, we get

$$F = \lambda_d(X - a)^d + \lambda_{d-1}(X - a)^{d-1} + \dots + \lambda_1(X - a) + \lambda_0\ (\forall \lambda_i \in k)$$

We assume the statement to be true for $n - 1$ by induction hypothesis. Now, let $F \in k[X_1, \dots, X_n]$ and $a_1, \dots, a_n \in k$. F can be considered a polynomial in $k[X_1, \dots, X_{n-1}][X_n]$, i.e. $F = \sum F_i X_n^i$, where $F_i \in k[X_1, \dots, X_{n-1}]$. Using Euclidean property for $k[X_1, \dots, X_{n-1}][X_n]$ and for $n = 1$ case, we have

$$F = f_d(X_n - a_n)^d + f_{d-1}(X_n - a_n)^{d-1} + \dots + f_1(X_n - a_n) + f_0\ (f_i \in k[X_1, \dots, X_{n-1}])$$

Using induction hypothesis,

$$f_j = \sum \lambda_{(i)}(X_1 - a_1)^{i_1} \dots (X_{n-1} - a_{n-1})^{i_{n-1}}\ (\lambda_(i) \in k)$$

$$F = \sum_{l=1}^{d} \left[\sum \lambda_i (X_1 - a_1)^{i_1} \dots (X_{n-1} - a_{n-1})^{i_{n-1}} \right] (X_n - a_n)^l$$
$$F = \sum \lambda_{(i)}(X_1 - a_1)^{i_1} \dots (X_n - a_n)^{i_n},\ \lambda_{(i)} \in k$$

(b) $F(a_1, \dots, a_n) = 0 \Rightarrow \lambda_i = 0$ when $i_1 = \dots = i_n = 0$. For a nontrivial term $F_{(i)} = \lambda_{(i)}(X_1 - a_1)^{i_1} \dots (X_n - a_n)^{i_n}$, some $i_k \neq 0$. So,

$$F_{(i)} = (X_k - a_k)[\lambda_{(i)}(X_1 - a_1)^{i_1} \dots (X_k - a_k)^{i_k - 1} \dots (X_n - a_n)^{i_n}]$$

Thus, $F = \sum_{i=1}^{k} (X_i - a_i)G_i$, $(G_i = k[X_1, \dots, X_n])$.

Problem 7.1.8. *Show that the algebraic subsets of $\mathbb{A}^1(k)$ are just the finite subsets, together with $\mathbb{A}^1(k)$ itself.*

Solution. We consider $X \subset \mathbb{A}^1(k)$. If X is algebraic $\Rightarrow$ there exists a set of polynomials $S \in k[X]$ such that $X = V(S)$, i.e. $F(X) = 0$ $\forall x \in X$ and $F \in S$. Since, F has finite number of roots (if $F \neq 0$) $\Rightarrow$ X is a finite set (as $X = \cap_{F \in S} V(F)$). If $F = 0$, we have $V(F) = \mathbb{A}^1(k)$.

Problem 7.1.9. *If k is a finite field, show that every subset of $\mathbb{A}^n(k)$ is algebraic*

Solution. Since k is a finite field say $|k| = l$, then $|\mathbb{A}^n(k)| = l^n$ and every subset X of $\mathbb{A}^n(k)$ is finite. Thus, by above Problem 7.1.8, X is algebraic.

Problem 7.1.10. *Give an example of countable collection of algebraic sets whose union is not algebraic.*

Solution. We consider $\mathbb{A}^1(\mathbb{R})$ and algebraic sets $X_i = \{i\} = V(X - i)$ $(i \in \mathbb{Z})$. Each X_i is finite $\Rightarrow$ X_i is algebraic set. We consider $X = \cup_{i \in \mathbb{Z}} X_i = \mathbb{Z}$. X is not finite $\Rightarrow$ X is not algebraic (Problem 7.1.8).

Problem 7.1.11. *Show that the following are algebraic sets:*

1. $\{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$
2. $\{(cos(t), sin(t)) \in \mathbb{A}^2(\mathbb{R}) \mid t \in \mathbb{R}\}$
3. *The set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r, θ) satisfy the equation $r = sin(\theta)$*

Solution. Let $V = \{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$.
Claim: $V = V(F) \cap V(G)$, where $F = X^2 - Y$ and $G = X^3 - Z$. $P \in V$ satisfies F and G. So, $V \subset V(F) \cap V(G)$. Now, let $P = (x, y, z) \in V(F) \cap V(G) \Rightarrow x^2 - y = 0$ and $x^3 - z = 0 \Rightarrow P = (x, x^2, x^3)$ for $x \in k \Rightarrow P \in V \Rightarrow V(F) \cap V(G) \subset V$, i.e. $V(F) \cap V(G) = V$.

Let $V = \{(cos(t), sin(t)) \in \mathbb{A}^2(\mathbb{R}) \mid t \in \mathbb{R}\}$. Claim $V = V(F)$, where $F = X^2+Y^2-1$. $P \in V$ satisfies F. So, $V \subset V(F)$. Let $P = (x, y) \in V(F) \Rightarrow x^2 + y^2 - 1 = 0 \Rightarrow x = \pm\sqrt{(1 - y^2)}$. Take $t = \sin^{-1} x = cos^{-1} y$, we have $P \in V$. So, $V(F) \subset V$, i.e. $V(F) = V$.
Similarly, for (3), we have $V = V(F)$, where $F = X^2 + Y^2 - X$.

Problem 7.1.12. *Suppose C is an affine plane curve, and L is a line in $\mathbb{A}^2(k)$, $L \not\subseteq C$. Suppose $C = V(F)$, $F \in k[X,Y]$ a polynomial of degree n. Show that $L \cap C$ is a finite set of no more than n points.*

Solution. Let $L = V(Y - (aX + b))$ (L can be V(X-a), and proof will be similar) in $\mathbb{A}^2(k)$. $L \cap C = V(F \cup \{Y - aX + b\})$. F is a polynomial of degree n. If $P = (x, y) \in \mathbb{A}^2(k)$ satisfies F and $Y - a(aX + b)$, then $F(x, ax + b) = 0$. If there exists x s.t. $F(x, ax + b) = 0 \Rightarrow F(x, y) = 0$, where $y = ax + b \Rightarrow (x, y) \in L$. Therefore,

$$L \cap C = \{(x, ax + b) \in \mathbb{A}^2 \mid F(x, ax + b) = 0\}$$

F is of degree $n \Rightarrow F(x, ax+b)$ is of degree atmost $n \Rightarrow$ Has atmost n roots $\Rightarrow L \cap C$ is a finite set of no more than n points.

Problem 7.1.13. *Show that each of the following is not algebraic:*

1. $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin x\}$
2. $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\}$
3. $\{(\cos(t), \sin(t), t) \in \mathbb{A}^3(\mathbb{R}) \mid t \in \mathbb{R}\}$

Solution. Let $V = \{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin x\}$ be algebraic set, i.e. $X = \cap_{F \in S} V(F)$ for some subset S of polynomials in $\mathbb{R}[X, Y]$. Let $L = \{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = 0\}$ a line. L is not contained in X. Take one polynomial $F \in S$. $V(F)$ is contains X, and L is not contained in $V(F)$. So, $L \cap V(F) \subset L \cap X$. Also, by Problem 7.1.12, $L \cap X = \{(m\pi, 0) \mid m \in \mathbb{Z}\}$ is a finite set $\Rightarrow\Leftarrow$. So, V is not algebraic.
Similarly, for (2), we can take $L = \{z = 0\}$ line in $\mathbb{A}^2(\mathbb{C})$ and applying Problem 7.1.12, we get $L \cap X = \{(0, w) \mid |w|^2 = 1\}$ is a finite set which is again a contradiction.
For (3), take $L = \{(1, 0, t) \in \mathbb{A}^3(\mathbb{R}) \mid t \in \mathbb{R}\}$ and apply Problem 7.1.12

Problem 7.1.14. *Let F be a non constant polynomial in $k[X_1, \ldots, X_n]$, k algebraically closed. Show that $\mathbb{A}^n(k)/V(F)$ is infinite if $n \geq 1$, and $V(F)$ is infinite if $n \geq 2$. Conclude that the complement of any proper algebraic set is infinite.*

Solution. Let $\mathbb{A}^n(k)/V(F) = \{P_1, \ldots, P_m\}$ be finite, where $P_i = (a_{i1}, \ldots, a_{in})$ for all $1 \leq i \leq m$. Consider the polynomial

$$G = F(X_1 - a_{11})(X_1 \ldots a_{21}) \ldots (X_1 \ldots a_{m1})$$

Take $P \in \mathbb{A}^n(k)$. If $P \in V(F)$, then $F(P) = 0 \Rightarrow G(P) = 0$. If $P \in V(F)$ i.e. $F(P) \neq 0$, then $P \in \mathbb{A}^n(k)/V(F) \Rightarrow P = P_i$ for some $i \Rightarrow (X_1 - a_{i1}) = 0 \Rightarrow G(P) = 0$. Thus, $P \in \mathbb{A}^(k)$. By, Problem 1.4, $G = 0$. A contradiction. Thus, $\mathbb{A}^n(k)/V(F)$ is infinite if $n \geq 1$.
Write $F = \sum F_i X_n^i$, where $F_i \in k[X_1, \ldots, X_{n-1}]$. If all F_i is constant, $F \in k[X_n]$. Since, k is algebraically closed, there exist $a \in k$ such that $F(a) = 0$ in $k[X_n]$. Taking the elements of the set $B = \{(a_1, \ldots, a_{n-1}, a) \mid a_i \in k\}$. Then, $B \subset V(F)$. Since, B is infinite set, as k is algebraically closed, we have $V(F)$ as infinite set.
Suppose F_i is not constant for all i. Hence, by part (a), $\mathbb{A}^{n-1}(k)/V(F_i)$ is infinite (where F_i is non-constant polynomial), i.e. there exist infinite points $(a_1, \ldots, a_{n-1})$ such that $F_i(a_1, \ldots, a_{n-1}) \neq 0$. Thus, we can choose $a_n \in k$ s.t. $F(a_1, \ldots, a_{n-1}, a_n)$ $= 0$ (as k is algebraically closed, such a_n exists). Thus, $V(F)$ is infinite set.
If $V = V(S)$ is a proper algebraic set of $\mathbb{A}^n(k)$. Take $F \in S$. Now, $V \subset V(F)$ $\Rightarrow \mathbb{A}^n(k)/V(F) \subset \mathbb{A}^n(k)/V$. By part (b), $\mathbb{A}^n(k)/V(F)$ is infinite, thus $\mathbb{A}^n(k)/V$ is infinite.

Problem 7.1.15. *Let $V \subset \mathbb{A}^n(k)$ be algebraic sets. Show that:*

$$V \times W = \{(a_1, \ldots, a_n, b_1, \ldots, b_m) \mid (a_1, \ldots, a_n) \in V, (b_1, \ldots, b_m) \in W\}$$

is an algebraic set in $\mathbb{A}^{n+m}(k)$. It is called the product of V and W.

Solution. Let $V = V(S_1)$ and $W = V(S_2)$, where S_1 and S_2 are subsets of polynomials in $k[X_1, \ldots X_n]$ and $k[X_1, \ldots, X_m]$ respectively. Let $S = \{F(X_1, \ldots, X_n) \mid F \in S_1\} \cup \{G(X_{n+1}, \ldots, X_{n+m}) \mid G \in S_2\} \subset k[X_1, \ldots, X_{n+m}]$. Since,

$$V \times W = \{(a_1, \ldots, a_n, b_1, \ldots, b_m) \mid (a_1, \ldots, a_n) \in V, (b_1, \ldots, b_m) \in W\}$$

we have, $V \times W = V(S)$.

Problem 7.1.16. *Let V, W be algebraic sets in $\mathbb{A}^n(k)$. Show that $V = W$ if and only if $I(V) = I(W)$.*

Solution. Claim: For any two algebraic sets V and W, $V \subset W$ if and only if $I(V) \supset I(W)$. ($\Rightarrow$) is true by property 6. ($\Leftarrow$) We assume $I(W) \subset I(V)$. Let $(a_1, \ldots, a_n) \in V$. Then, $\forall F \in I(V), F(a_1, \ldots, a_n) = 0 \Rightarrow \forall F \in I(W), F(a_1, \ldots a_n) = 0 \Rightarrow (a_1, \ldots, a_n) \in V(I(V)) \Rightarrow (a_1, \ldots, a_n) \in V$ as for algebraic sets $V(I(V)) = V$. So, $W \subset V$.

Problem 7.1.17. *1. Let V be an algebraic set in $\mathbb{A}^n(k)$, $P \in \mathbb{A}^n(k)$ a point not in V. Show that there is a polynomial $F \in k[X_1, \ldots, X_n]$ such that $F(Q) = 0$ for all $Q \in V$ but $F(P) = 1$.*

2. *Let $P_1, \ldots, P_r$ be distinct points in $\mathbb{A}^n(k)$, not in an algebraic set V. Show that there are polynomials $F_1, \ldots, F_r \in I(V)$ such that $F_i(P_j) = 0$ for $i \neq j$ and $F_i(P_i) = 1$.*

3. *With $P_1, \ldots, P_r$ and V as above and $a_{ij} \in k$ for $1 \leq i, j \leq r$, show that there are $G_i \in I(V)$ with $G_i(P_j) = a_{ij}$ for all i and j.*

Solution. (1) Let $I(V) = I(V \cup \{P\}) \Rightarrow P \in V(I(V)) \Rightarrow P \in V$ (as V is algebraic) $\Rightarrow\Leftarrow$ as P does not belong to $V \Rightarrow I(V) \neq I(V \cup \{P\})$.
So, there exits $F \in I(V)$ s.t. $F(P) \neq 0$. Let $F(P) = a \neq 0$. We consider $G = \frac{f}{a}$ (k is a field). $G(Q) = 0\ \forall Q \in V$ and $g(P) = 1$
(2) Let $W = V \cup \{P_1, \ldots, P_i, \ldots, P_r\}/\{P_i\}$. Using (1), there exists a function $F_i \in I(W)$ s.t. $F_i(Q) = 0$ for all $Q \in W$ and $F_i(P_i) = 1$. Repeating this, we get $F_1, \ldots, F_r \in I(V)$ s.t. $F_i(P_j) = 0$ if $i \neq j$ and $F_i(P_i) = 0$.
(3) Let $G_i = \sum_j a_{ij} F_j$. Then $G_i(P_k) = \sum_j a_{ij} F_j(P_k) = a_{ik}\ \forall i, k$.

Problem 7.1.18. *Let I be an ideal in a ring R. IF $a^n \in I$, $b^m \in I$, show that $(a+b)^{n+m} \in I$. Show that* Rad(I) *is an ideal, infact a radical ideal. Show that any prime ideal is radical.*

Solution. $(a+b)^{n+m} = \sum_{i=0}^{n+m} \begin{pmatrix} m \\ i \end{pmatrix} a^i b^{m+n-i}$. If $i \leq n$, then $m + n - i \geq m \Rightarrow m^{m+n-i} \in I$ (as $b^m \in I$). If $i \geq n$ then $a^i \in I \Rightarrow a^i b^{m_n - i} \in I\ \forall i \in \{0, \ldots, n+m\} \Rightarrow (a+b)^{n+m} \in I$.
Thus, Rad(I) is closed under addition. If $a \in \text{Rad}(I) \Rightarrow a^n \in I \Rightarrow (-a)^n \in I \Rightarrow -a \in \text{Rad}(I)$. $0 \in \text{Rad}(I)$ as $0^n \in I \Rightarrow \text{Rad}(I)$ is a group. If $a, b \in \text{Rad}(I) \Rightarrow a^n \in I$ and $b^m \in I$ for some n and $m \Rightarrow (ab)^{m+n} \in I \Rightarrow \text{Rad}(I)$ is a subring. Now, if $a \in \text{Rad}(I) \Rightarrow a^n \in I$ for some n. If $r \in R$, $r^n a^n \in I \Rightarrow (ra)^n \in I \Rightarrow ra \in \text{Rad}(I) \Rightarrow$ Rad(I) is an ideal.
If $a \in \text{Rad}(I) \Rightarrow a^n \in \text{Rad}(I)$ for some $n \Rightarrow a^{nm} \in I$ for some m and $n \Rightarrow a \in \text{Rad}(I)$ $\Rightarrow \text{Rad}(\text{Rad}(I)) \subset \text{Rad}(I) \Rightarrow \text{Rad}(\text{Rad}(I)) = \text{Rad}(I)$.
Let P be a prime ideal. $a \in \text{Rad}(P) \Rightarrow a^n \in P$ for some n. Since, P is prime $\Rightarrow$ either $a \in P$ or $a^{n-1} \in P$. If $a \in P \Rightarrow \text{Rad}(P) = P$. If $a^{n-1} \in P$, repeat the process to get $a \in P \Rightarrow \text{Rad}(P) = P$.

Problem 7.1.19. *Show that $I = (X^2 + 1) \subset \mathbb{R}[X]$ is a radical (even a prime) ideal, but I is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$.*

*Solution***.** Since, $(X^2 + 1) \in \mathbb{R}[X]$ is irreducible over $\mathbb{R} \Rightarrow (X^2 + 1)$ is a prime ideal $\Rightarrow (X^2 + 1)$ is a radical ideal (by previous problem). Also, for any $x \in \mathbb{A}^1(\mathbb{R})$, $(X^2 + 1) \neq 0 \Rightarrow \nexists$ set $X \subset \mathbb{A}^1(\mathbb{R})$ s.t. $x^2 + 1 = 0\ \forall x \in X$.

Problem 7.1.20. *Show that for any ideal I in $k[X_1, \ldots, X_n]$, $V(I) = V(\text{Rad}(I))$ and* $\text{Rad}(I) \subset I(V(I))$

*Solution***.** Let $P = (a_1, \ldots, a_n) \in V(I) \Rightarrow f(a_1, \ldots, a_n) = 0\ \forall f \in I$. Let $g \in \text{Rad}(I) \Rightarrow$ there exists m s.t $g^m \in I \Rightarrow g^m(P) = 0 \Rightarrow g(P) = 0 \Rightarrow P \in \text{Rad}(I) \Rightarrow V(I) \subset V(\text{Rad}(I))$. Since, $I \subset \text{Rad}(I) \Rightarrow V(\text{Rad}(I)) \subset V(I)$. So, $V(\text{Rad}(I)) = V(I)$. Let $F \in \text{Rad}(I) \Rightarrow \exists\ n$ s.t. $F^n \in I$. Let $P \in V(\text{Rad}(I)) \Rightarrow F(P) = 0\ \forall F \in \text{Rad}(I) \Rightarrow$ For any $P \in V(I)$, $F(P) = 0\ \forall F \in \text{Rad}(I) \Rightarrow \text{Rad}(I) \subset I(V(I))$.

Problem 7.1.21. *Show that $I = (X_1 - a_1, \ldots, X_n - a_n) \subset k[X_1, \ldots, X_n]$ is a maximal ideal, and that the natural homomorphism from k top $k[X_1, \ldots, X_n]/I$ is an isomorphism.*

*Solution***.** We consider the homomorphism

$$\phi : k[X_1, \ldots, X_n] \to k$$

$$f(X_1, \ldots, X_n) \to f \bmod (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) = f \bmod I$$

Map is onto.

$$Ker(\phi) = \{f \in k[X_1, \ldots, X_n] \mid f \bmod (X_1 - a_1, \ldots, X_n - a_n) = 0\}$$

So, $(X_1 - a_1, \ldots, X_n - a_n) \mid f \Rightarrow f \in (X_1 - a_1, \ldots, X_n - a_n)$. Thus, $ker(\phi) = I \Rightarrow k[X_1, \ldots, X_n]/I \cong k(field) \Rightarrow I$ is maximal ideal.

Problem 7.1.22. *Let I be an ideal in a ring R, $\pi : R \to R/I$ the natural homomorphism.*

1. *Show that for every ideal J' of R/I, $\pi^{-1}(J') = J$ is ideal of R containing I, and for every ideal J of R containing I, $\pi(J) = J'$ is an ideal of R/I. This sets up a natural one-to-one correspondence between $\{$ideals of $R/I\}$ and $\{$ideals of R that contain $I\}$.*

2. *Show that J' is a radical ideal if and only if J is radical. Similarly for prime and maximal ideals.*

3. *Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian. Any ring of the form $k[X_1, \ldots, X_n]/I$ is Noetherian.*

Solution. (1) If $a, b \in J$, $a+I, b+I \in J'$ s.t. $\pi^{-1}(a+I) = a$ and $\pi^{-1}(b+I) = b$. Since, J' is an ideal $\Rightarrow a+b+I \in J'$ and $ab+I \in J' \Rightarrow (a+b) \in \pi^{-1}(J')$ and $ab \in \pi^{-1}(J')$ $\Rightarrow (a+b), ab \in J \Rightarrow J$ is an ideal of R. $\because 0 \in J' \Rightarrow \pi^{-1}(0) \in J \Rightarrow I \subset J$.
Now, J is an ideal containing I, $\pi(I) = 0 \Rightarrow 0 \in J'$. Let $a, b \in J \Rightarrow ab \in J$ and $a+b \in J \Rightarrow ab \bmod I \in J'$ and $a+b \bmod I \in J' \Rightarrow J'$ is an ideal. Thus, there exists a natural one-one correspondence between ideals of R/I and ideals of R containing I.
(2) If $\mathrm{Rad}(J') = J'$, then $a \bmod I \in \mathrm{Rad}(J') \Rightarrow \exists\, m$ s.t. $a^m \bmod I \in J'$. Let $a \in \mathrm{Rad}(J) \Rightarrow \exists\, n$ s.t. $a^n \in J \Rightarrow a^n \bmod I \in J'$ (as $\pi(J) = J'$) $\Rightarrow a \bmod I \in \mathrm{Rad}(J')$ $\Rightarrow a \bmod I \in J'$ (as $\mathrm{Rad}(J') = J'$) $\Rightarrow a \in J \Rightarrow \mathrm{Rad}(J) \subset J \Rightarrow \mathrm{Rad}(J) = J$. Reversing the argument, we get if J is radical ideal, then J' is radical ideal.
If J' is maximal ideal $\Rightarrow$ there exists any ideal J'' between J' and R/I. $\because$ There is one-to-one correspondence between ideals of R/I and ideals of R containing I, $\nexists$ any ideal J_1 between J and $R \Rightarrow J$ is maximal ideal. Since, the correspondence is $1-1$, we can prove the other way round.
If J' is prime ideal, i.e. $ab \bmod I \in J' \Rightarrow a \bmod I \in J'$ or $b \bmod I \in J'$. If $ab \in J \Rightarrow ab \bmod I \in J' \Rightarrow a \bmod I \in J'$ or $b \bmod I \in J' \Rightarrow a \in J$ or $b \in J \Rightarrow J$ is prime ideal. Similarly, other way round.
(3) Let $J = (a_1, \ldots, a_n)$ a_i's $\in R$. $J' = \pi(J) \Rightarrow J'$ contains $a_1 \bmod I, \ldots, a_n \bmod I$. Let $\exists\, a \bmod I \in J'$ s.t. $a \bmod I$ is not generated by $a_1 \bmod I, \ldots, a_n \bmod I$. $\because$ $a \bmod I \in J' \in a \in J \Rightarrow a = \sum_{i=1}^{n} r_i a_i$ $(r_i \in R) \Rightarrow a \bmod I = \sum_{i=1}^{n} a_i a_i \bmod R \Rightarrow a$ is generated by $a_1 \bmod I, a_2 \bmod I, \ldots, a_n \bmod I \Rightarrow\Leftarrow$. $\Rightarrow J'$ is finitely generated.
So, If R is Noetherian $\Rightarrow R/I$ is Noetherian. Hence, $k[X_1, \ldots, X_n]$ is Noetherian (by Hilbert Basis Theorem) $\Rightarrow k[X_1, \ldots, X_n]/I$ is Noetherian.

Problem 7.1.23. *Give an example of collection τ of ideals in Noetherian ring such that no maximal member of τ is a maximal ideal.*

Solution. In $\mathbb{Z}$, we consider the collection $\tau = \{(4), (8), (16), \ldots\}$. (4) is the maximal member of τ but not a maximal ideal.

Problem 7.1.24. *Show that every proper ideal I in Noetherian ring is contained in a maximal ideal.*

Solution. We consider the collection $\tau = \{\text{proper ideals that contain } I\}$. It has a maximal member say M. If M is a maximal ideal, then we are done. If there exists a proper ideal M' containing M, $I \subset M \subset M' \Rightarrow M' \in \tau$. Thus, M is not maximal member of $\tau \Rightarrow\Leftarrow$. So, no such M' exists and M is maximal ideal.

Problem 7.1.25. 1. *Show that $V(Y - X^2) = \mathbb{A}^2(\mathbb{C})$ is irreducible and $I(V(Y - X^2)) = (Y - X^2)$*

2. *Decompose $V(Y - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subset \mathbb{A}^3(\mathbb{C})$ into irreducible components.*

Solution. (1) If is sufficient to show that $I = I(V(Y - X^2))$ is prime ideal. As $I(V(I)) = I$ if I is an ideal of algebraic set. So, $I = (Y - X^2)$. Since, $(Y - X^2)$ is irreducible in $\mathbb{C}[X, Y]$, $(Y - X^2)$ is prime in $\mathbb{C}[X, Y]$. (2) $F = Y^4 - X^2 = (Y^2 + X)(Y^2 - X)$ and $G = Y^4 - X^2Y^2 + XY^2 - X^3 = (Y^2 + X)(Y^2 - X^2)$.

$$\begin{aligned}
V(F, G) &= V((Y^2 - X)(Y^2 + X)) \bigcap V((Y^2 + X), Y^2 - X^2) \\
&= \left[V(Y^2 + X) \cup V(Y^2 - X)\right] \bigcap \left[V(Y^2 + X) \cup V(Y^2 - X^2)\right] \\
&= V(Y^2 + X) \cup V(Y^2 + X, Y^2 - X^2) \cup V(Y^2 - X, Y^2 - X^2)
\end{aligned}$$

$V(Y^2 - X, Y^2 - X^2) = \{(0, 0), (1, \pm 1)\} = V(X, Y) \cup V(X - 1, Y + 1) \cup V(X - 1, Y + 1)$

$V(Y^2 + X, Y^2 - X^2) = \{(0, 0), (-1, \pm 1)\} = V(X, Y) \cup V(X + 1, Y + 1) \cup V(X + 1, Y + 1)$

$V(Y^2 - X, Y^2 + X) = \{(0, 0)\} = V(X, Y)$ and by (1), $V(Y^2 + X)$ is irreducible. Hence, the irreducible components are $V(Y^2 + X)$, $V(X, Y)$, $V(X + 1, Y + 1)$, $V(X + 1, Y - 1)$, $V(X - 1, Y + 1)$ and $V(X - 1, Y - 1)$.

Problem 7.1.26. *Show that $F = Y^2 + X^2(X - 1)^2 \in \mathbb{R}[X, Y]$ is an irreducible polynomial but that $V(F)$ is reducible.*

Solution. $V(F) = \{(0, 0), (1, 0)\} = V(X, Y) \cup V(X - 1, Y)$. So, $V(F)$ is reducible. Suppose F is reducible, then $F = (Y + F_1)(Y + F_2)$ for some $F_1, F_2 \in \mathbb{R}[X, Y]$. Equating terms of Y, we get $F_2 = -F_1$ and $F_1^2 = -X^2(X - 1)^2$. No such F_1 exists in $\mathbb{R}[X, Y]$. Thus, F is irreducible.

Problem 7.1.27. *Let V, W be algebraic sets in $\mathbb{A}^n(k)$ with $V \subset W$. Show that each irreducible component of V is contained in some irreducible component of W.*

Solution. Let $V_1, \ldots, V_m$ and $W_1, \ldots, W_r$ are irreducible algebraic sets of V and W respectively such that $V = V_1 \cup \ldots \cup V_m$ ($V_i \not\subseteq V_j$ for all $i \neq j$) and $W = W_1 \cup \ldots \cup W_r$ ($W_i \not\subseteq V_j$ for all $i \neq j$). $\because V \subset W \Rightarrow V_1 \cup \ldots \cup V_m \subset W_1 \cup \ldots \sup W_r \Rightarrow V_i = \cup_j (W_j \cap V_i) \Rightarrow V_i \subset W_{j(i)}$ $\forall i$ (as V_i's and W_j's are irreducible). So, each irreducible component of V is contained in some irreducible component of W.

Problem 7.1.28. *If $V = V_1 \cup \ldots V_r$ is the decomposition of an algebraic set into irreducible components. Show that $V_i \not\subseteq \cup_{j \neq i} V_j$.*

Solution. Let $V_i \subset \cup_{j \neq i} V_j$ (i fixed) $\Rightarrow V_i = \bigcup_{j \neq i} (V_i \cap V_j)$. But V_i is irreducible $\Rightarrow \exists\ j(i)$ ($\neq i$) s.t. $V_i \subset V_{j(i)} \Rightarrow\Leftarrow$ (as $V_i \not\subseteq V_j$ $\forall i \neq j$). Thus, $V_i \not\subseteq \cup_{j \neq i} V_j$.

Problem 7.1.29. *Show that $\mathbb{A}^n(k)$ is irreducible if k is infinite.*

Solution. $\because k$ is infinite $\Rightarrow I(\mathbb{A}^n(k)) =$ zero polynomial (by Problem 7.1.14) which is prime $\Rightarrow \mathbb{A}^n(k)$ is irreducible.

Problem 7.1.30. *Let $k = \mathbb{R}$.*

1. *Show that $I(V(X^2 + Y^2 - 1)) = (1)$.*

2. *Show that every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to $V(F)$ for some $F \in \mathbb{R}[X, Y]$.*

Solution. (a) $X^2 + Y^2 + 1 = 0$ has no solutions in $\mathbb{A}^2(\mathbb{R}) \Rightarrow V(X^2 + Y^2 + 1) = \Phi$. So, $I(V(X^2 + Y^2 + 1)) = I(\Phi) = (1)$.
(b) Let V be an algebraic subset of $\mathbb{A}^2(\mathbb{R})$, then by Theorem 3.1.5, there are unique irreducible algebraic sets $V_1, \ldots, V_m$ such that $V = V_1 \cup \ldots V_m$ and $V_i \subset V_j$ for all $i \neq j$.
Claim: Every irreducible algebraic subsets V_i of $\mathbb{A}^2(\mathbb{R})$ are : $\mathbb{A}^2(\mathbb{R})$, Φ, points, and irreducible plane curves $V(F)$. If V_i is finite or $I(V_i) = 0$, then the claim. If $I(V_i)$ contains a non constant polynomial F. We can consider F to be irreducible as $I(V_i)$ is prime. Now, if $G \in I(V_i)$ and $G \notin (F)$, we have $V_i \subset V(F, G)$ which is finite (by Theorem 4.0.12). Thus, $I(V_i) = (F)$ which is irreducible plane curves.
So, If V_i's are $\mathbb{A}^2(\mathbb{R})$ or Φ, there is nothing to prove. If V_i is point (a_1, b_i), we have

$V_i = V((X-a_i)^2+(Y-b_i)^2)$, or V_i is irreducible plane curve given by $V(F_i)$ for some irreducible polynomial in $F_i \in \mathbb{R}[X,Y]$. We consider

$$F = ((X-a_1)^2+(Y-b_1)^2)\dots((X-a_r)^2+(Y-b_r)^2)F_{r+1}\dots F_m$$

$V = V_1 \cap \dots \cap V_m = V(F)$. Thus, $V = V(F)$ for some $F \in \mathbb{R}[X,Y]$.

Problem 7.1.31. *1. Find the irreducible components of $V(Y^2-XY-X^2Y+X^3)$ in $\mathbb{A}^2(\mathbb{R})$, and also in $\mathbb{A}^2(\mathbb{C})$.*

2. Do the same for $V(Y^2-X(X^2-1))$ and for $V(X^3+X-X^2-Y)$.

Solution. (*a*) $Y^2-XY-X^2Y+X^3 = (Y-X)(Y-X^2)$. $(Y-X)$ is of degree 1, so is irreducible and $(Y-X^2)$ is irreducible both in $\mathbb{A}^2(\mathbb{R})$ and $\mathbb{A}^2(\mathbb{C})$(by Problem 7.1.25). Thus, irreducible components are $V(Y-X)$ and $V(Y-X^2)$.
(*b*) $V(Y^2-X(X^2-1))$ is irreducible in $\mathbb{C}[X,Y]$ (can be checked by assuming that it is reducible and thus will have the form $(Y+f(X))(Y+g(X))$ and getting a contradiction that $X(X^2-1)$ is square of some polynomial). Thus, $V(Y^2-X(X^2-1))$ is itself irreducible component in $\mathbb{A}^2(\mathbb{R})$ and $\mathbb{A}^2(\mathbb{C})$.
$V(X^3+X-X^2-Y) = V(X^2+1)\cup V(X-Y)$ in $\mathbb{A}^2(\mathbb{R})$ as irreducible components and $V(X^3+X-X^2-Y) = V(X+i)\cup V(X-i)\cup V(X-Y)$ in $\mathbb{A}^2(\mathbb{C})$ as irreducible components.

Problem 7.1.32. *Show that Weak Hilbert's Nullstellensatz Theorem (Theorem 3.4.5), Nullstellensatz Theorem (Theorem 3.4.7) and all of its corollaries (Corollaries 3.4.8, 3.4.9 and 3.4.10) are false if k is not algebraically closed.*

Solution. For weak Nullstellensatz Theorem: Let $I = (X^2+Y^2+1=0)$ be a proper ideal in $\mathbb{R}[X,Y]$. $V(X^2+Y^2+1) = \Phi$ as for no real values $x^2+y^2+1=0$. $V(I) = \Phi$. For Nullstellensatz Theorem: For the same ideal above, I is irreducible in $\mathbb{R}[X,Y] \Rightarrow$ I is prime ideal $\Rightarrow \sqrt{I} = I$. Also (by Problem 7.1.30) $I(V(I)) = (1) \neq \sqrt{I}(=I)$.

Problem 7.1.33. *1. Decompose $V(X^2+Y^2-1, X^2-Z^2-1) \subset \mathbb{A}^3(\mathbb{C})$ into irreducible components.*

2. Let $V = \{(t,t^2,t^3) \in \mathbb{A}^3(\mathbb{C}) \mid t \in \mathbb{C}\}$. Find $I(V)$, and show that V is irreducible.

Solution. $V(X^2+Y^2-1, X^2-Z^2-1) = V(X^2+Y^2-1, Y^2+Z^2)$. In $\mathbb{C}$, X^2+Y^2-1 is irreducible (can be checked by taking $X^2+Y^2-1 = (aX+bY+c)(dX+eY+f)$, where $a, b, \ldots, f \in \mathbb{C}$ and getting a contradiction). $Y^2 + Z^2 = (Z + Y\iota)(Z - Y\iota)$, where $\iota = \sqrt{1}$. So,

$$V(X^2+Y^2-1, X^2-Z^2-1) = V(X^2+Y^2-1, Z+\iota Y) \cup V(X^2+Y^2-1, Z-\iota Y) = V_1 \cup V_2$$

where $V_1 = V(X^2 + Y^2 - 1, Z + \iota Y)$ and $V_2 = V(X^2 + Y^2 - 1, Z - \iota Y)$. Also, $k[X, Y, Z]/I(V_1) = k[X, Y]/(X^2 + Y^2 - 1)$, which is a domain (as $X^2 + Y^2 - 1$ is irreducible). Thus, $I(V_1)$ is prime and V_1 is irreducible Similarly for V_2. Thus V_1 and V_2 are irreducible components of V.
By Problem 7.1.11, $V = V(X^2 - Y, X^3 - Z)$. Also, $(X^2 - Y, X^3 - Z)$ is radical ideal. Thus, by Hilbert's Nullstellensatz Theorem, $I(V) = V$. So,

$$k[X, Y, Z]/I(V) = k[X, Y, Z]/V = k[X]$$

which is a domain. Thus, $I(V)$ is prime and V is irreducible.

Problem 7.1.34. *Let R be a UFD.*

1. *Show that a monic polynomial of degree two or three in $R[X]$ is irreducible if and only if it has no roots in R.*

2. *The polynomial $X^2 - a \in R[X]$is irreducible if and only if a is not a square in R*

Solution. If $f(x)$ is irreducible if and only if it doesn't have any factor of degree 1 $\Leftrightarrow$ has no roots in R. R is UFD is needed as in UFD sum of degree of each factor polynomial of $f(X)$ is equal to the degree of $f(X)$. Thus for $n = 2$, (1,1) is the only possibility and for $n = 3$, $(1, 1, 1)$ or $(1, 2)$ are the only possibility for the degree of the factors. In each case there is a factor polynomial of degree 1. This factor of degree 1 can be made monic as $f(X)$ is monic.
Using above part, $X^2 - a$ is irreducible if and only if it has no roots in R if and only if it doesn't have a factor of degree 1 if and only if a is not a square in R (as $(X^2 - a) = (X - \sqrt{a})(X + \sqrt{a})$).

Problem 7.1.35. *Show that $V(Y^2 - X(X - 1)(X - \lambda)) \subset \mathbb{A}^2(k)$ is an irreducible curve for any algebraically closed field k, and any $\lambda \in k$*

Solution. If $f(X) = Y^2 - X(X - 1)(X - \lambda)$ is reducible in $k[X, Y]$, using Gauss's Lemma, $Y^2 - X(X - 1)(X - \lambda)$ is reducible in $k(X)[Y]$. By previous problem,

$X(X-1)(X-\lambda)$ must be a square in $k(X)$ which is not possible as $X(X-1)(X-\lambda)$ has degree odd. Thus $f(X)$ is irreducible.

Problem 7.1.36. *Let* $I = (Y^2 - X^2, Y^2 + X^2) \subset \mathbb{C}[X,Y]$. *Find* $\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/I)$ *and* $V(I)$.

Solution. $V(I) = \{(0,0)\}$. X^2 and Y^2 are both zero in $\mathbb{C}[X,Y]$. Thus, $\mathbb{C}[X,Y]/I$ is the residue of an element $a + bX + cY + dXY$ for some $a,b,c,d \in \mathbb{C}$. Hence, $\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/I) = 4$

Problem 7.1.37. *Let* K *be any field.* $F \in K[X]$ *a polynomial of degree* $n > 0$. *Show that the residues* $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ *form a basis of* $K[X]/(F)$ *over* K.

Solution. Since, $K[X]$ is a UFD, Any polynomial $g(X) \in K[X]$ can be written as

$$g(X) = p(X)F(X) + r(X)$$

where $r(X)$ has degree less than n. Taking modulo $F(X)$, we have $\overline{g(X)} = \overline{r(X)}$, where $\overline{r(X)}$ has degree less than n. Thus, $\overline{r(X)}$ can be written as linear combination of $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1} \Rightarrow \{\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}\}$ ia spanning set of $K[X]/(F)$. If $\sum \lambda_i \overline{X}^i = \overline{0}$ $(\lambda_i \in K) \Rightarrow \sum_{\lambda_i X^i} \in (F)$. But F has degree at least n or 0. Thus, $\lambda_i = 0\ \forall i \Rightarrow$ $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ form a basis of $K[X]/(F)$ over K.

Problem 7.1.38. *Let* $R = k[X_1, \ldots, X_n]$, k *algebraically closed.* $V = V(I)$. *Show that there is a natural one-to-one correspondence between algebraic subsets of* V *and radical ideals in* $k[X_1, \ldots, X_n]/I$ *and that irreducible algebraic set (resp. points) correspond to prime ideals (resp. maximal ideals).*

Solution. By Problem 7.1.22, there exists $1-1$ correspondence between radical ideals of R/I and radical ideals of R containing I. By Corollary 3.4.8(1), there exists 1-1 correspondence between algebraic sets of $\mathbb{A}^n(k)$ and radical ideals of $k[X_1, \ldots, X_n]$. Let V' be an algebraic subset of V, i.e. there exists ideal $I' \subset k^n$ such that $V' = V(I') \subset V = V(I) \Rightarrow I(V(I')) \supset I(V(I)) \Rightarrow \sqrt{I'} \supset \sqrt{I} = J$ (say). $\sqrt{I'}$ is a radical ideal in $k[X_1, \ldots, X_n]$. Corresponding to $\sqrt{I'}$, there exists a radical ideal J'' in $k[X_1, \ldots, X_n]/I$ such that $\pi(J'') = J'$ (where $\pi : R \to R/I$ is projection map).Thus, there exists $1-1$ correspondence between algebraic set of I and radical ideals of $k[X_1, \ldots, X_n]/I$. Similarly using Corollary 3.4.8(2) (resp. 3.4.9(3)), we can show $1-1$ correspondence between irreducible algebraic sets (resp. points) and prime ideals (resp. maximal ideals).

Problem 7.1.39. *1. Let R be a UFD and let $P = (t)$ be principal, proper prime ideal. Show that there is no prime ideal Q such that $0 \subset Q \subset P$ ($Q \neq 0$, $Q \neq P$).*

2. Let $V = V(F)$ be an irreducible hypersurface in $\mathbb{A}^n$. Show that there is no irreducible algebraic set W such that $V \subset W \subset \mathbb{A}^n$, $W \neq V$, $W \neq \mathbb{A}^n$.

Solution. (1) Let $\exists$ Q s.t. $Q \subset P$ and Q prime ($Q \neq 0$, $Q \neq P$). Then $\exists$ $q \in Q$ s.t. $q = ta$ for some $a \in R$. Since R is a UFD, $q = t^\alpha b$, where $t \nmid b$. Q is prime $\Rightarrow t^\alpha \in Q$ or $b \in Q \Rightarrow t \in Q$ or $b \in Q$. $t \in Q \Rightarrow Q = P \Rightarrow\Leftarrow$. If $b \in Q \Rightarrow b = tc$ for some $c \in R$ but $t \nmid b$. Thus, contradiction. So, no such prime ideal Q exists.
(2) $V = V(F)$ is irreducible algebraic subset in $\mathbb{A}^n$. By Hilbert's Nullstellensatz Theorem, (F) is prime ideal in $k[X_1, \ldots, X_n] \Rightarrow \nexists$ Q prime s.t. $Q \subseteq (F)$ $(Q \neq 0) \Rightarrow$ $\nexists$ any prime ideal Q s.t. $V = V(F) \subseteq V(Q) = W \Rightarrow \nexists$ any algebraic subset W s.t. $V \subset W$ $(V \neq W)$ (by Hilbert's Nullstellensatz Theorem).

Problem 7.1.40. *Let $I = (X^2 - Y^3, Y^2 - Z^3) \subset k[X, Y, Z]$. Define $\alpha : k[X, Y, Z] \to k[T]$ by $\alpha(X) = T^9$, $\alpha(Y) = T^6$, $\alpha(Z) = T^4$.*

1. *Show that every element of $k[X, Y, Z]/I$ is the residue of an element $A + XB + YC + XYD$, for some $A, B, C, D \in k[Z]$.*

2. *If $F = A + XB + YC + XYD$, $A, B, C, D \in k[Z]$, and $\alpha(F) = 0$, compare like powers of T to conclude that $F = 0$*

3. *Show that $Ker(\alpha) = I$, so I is prime, $V(I)$ is irreducible, and $I(V(I)) = I$.*

Solution. We consider any term $X^i Y^j Z^k$ in an element of $k[X, Y, Z]$, where $i, j \geq 2$. If $i \neq 2$ then taking out the factor of $X^2 - Y^2$ will leave power of X as 1. If $j \geq 3$ then taking out factor $Y^2 - Z^3$ will leave power of Y as 1. Thus, $k[X, Y, Z]/I$ has element of the form $A + XB + YC + XYD$ for some $A, B, C, D \in k[Z]$.

$$\alpha(F) = 0 \Rightarrow \alpha(F) = A' + B'T^9 + C'T^6 + D'T^{15} = 0$$

$\deg(A') = \deg(B'T^9 + C'T^6 + D'T^{15})$. If any of B, C, D is non zero, B', C', D' have power as multiple of $4 \Rightarrow \deg(B'T^9 + C'T^6 + D'T^{15})$ is not multiple of $4 \Rightarrow \deg(A')$ is not multiple of 4. Contradiction. So, $A = 0$. Also, $\deg(C'T^6)$ is even and $\deg(B'T^9)$ and $\deg(D'T^{15})$ are odd $\Rightarrow C = 0$. So, $\alpha(F) = B'T^9 + D'T^{15} = 0 \Rightarrow \deg(B'T^9) =$

$\deg(D'T^{15})$ which is not possible for any natural number. Thus $F = 0$.
$\alpha(I) = 0 = Ker(\alpha)$ by previous part. Thus, $k[X,Y,Z]/Ker(\alpha) = k[T]$, which is integral domain. Thus, $ker(\alpha) = I$ is prime $\Rightarrow V(I)$ is irreducible $\Rightarrow I(V(I)) = I$.

7.2 Affine Varieties

Problem 7.2.1. *Let $\phi : V \to W$ be a polynomial map of affine varieties, $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$ the induced map on coordinate rings. Suppose $P \in V, \phi(P) = Q$. Show that $\tilde{\phi}$ extends to a ring homomorphism (also written $\tilde{\phi}$) from $\mathscr{O}_Q(W)$ to $\mathscr{O}_P(V)$. Show that $\tilde{\phi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$.*

Solution. See Lemma 4.0.11

Problem 7.2.2. *Let $T : \mathbb{A}^n \to \mathbb{A}^n$ be an affine change of coordinates, $T(P) = Q$. Then $\tilde{T} : \mathscr{O}_Q(\mathbb{A}^n) \to \mathscr{O}_P(\mathbb{A}^n)$ is an isomorphism. Also, $\tilde{T}$ induces an isomorphism from $\mathscr{O}_Q(V)$ to $\mathscr{O}_P(V^T)$ if $P \in V^T$, for V a subvariety of $\mathbb{A}^n$.*

Solution. By previous problem $\tilde{T}$ is a ring homomorphism. Since, T is affine change of coordinates, (T_i are polynomials of degree 1), T is invertible. Thus, T^{-1} is also affine change of coordinates. By previous problem, $\widetilde{T^{-1}} : \mathscr{O}_P(\mathbb{A}^n) \to \mathscr{O}_Q(\mathbb{A}^n)$ is well defined. Also, by composition of polynomial maps, we have

$$\widetilde{T^{-1}} \circ \widetilde{T} = \widetilde{T \circ T^{-1}} = \tilde{1} = Id_{\mathscr{O}_Q(\mathbb{A}^n)}$$

Similarly, $\widetilde{T} \circ \widetilde{T^{-1}}$ is identity. Thus $\tilde{T}$ induces an isomorphism from $\mathscr{O}_Q(\mathbb{A}^n)$ to $\mathscr{O}_P(\mathbb{A}^n)$. Restricting $\tilde{T}$ to $\mathscr{O}_Q(V)$ we get an isomorphism from $\mathscr{O}_Q(V)$ to $(O)_P(V^T)$.

Problem 7.2.3. *Let V be a variety in $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \dots, X_n]$, $P \in V$, and let J be an ideal of $k[X_1, \dots, X_n]$ that contains I. Let J' be the image of J in $\Gamma(V)$. Then there is a natural isomorphism φ from $\mathscr{O}_P(\mathbb{A}^n)/J\mathscr{O}_P(\mathbb{A}^n)$ to $\mathscr{O}_P(V)/I\mathscr{O}_P(V)$. In particular, $\mathscr{O}_P(\mathbb{A}^n)/I\mathscr{O}_P(\mathbb{A}^n)$ is isomorphic to $\mathscr{O}_P(V)$.*

Solution. See Lemma 4.0.15

Problem 7.2.4. *Let V be a non empty variety. Show that the map that associates to each $F \in k[X_1, \dots, X_n]$ a polynomial function in $F \in k[X_1, \dots, X_n]$ a polynomial function in $\mathscr{F}(V, k)$ (the set of all function from V to k) is a ring homomorphism whose kernel is I(V).*

Solution.

$$\phi : k[X_1, \ldots, X_n] \to (V, k)$$

$$F \to f$$

where $f : V \to k$, $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$ (the restriction map). The set of all polynomial function forms a ring homomorphism, thus ϕ is a ring homomorphism. If $F \in ker(\phi) \Leftrightarrow F(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V \Leftrightarrow F \in I(V)$.

Problem 7.2.5. *Let $V \subset \mathbb{A}^n$ be a variety. A subvariety of V is a variety $W \subset \mathbb{A}^n$ that is contained in V. Shoe that there is a natural one-to-one correspondence between algebraic subsets (resp. subvarieties, resp. points) of V and radical ideals (resp. prime ideals, resp. maximal ideals) of $\Gamma(V)$.*

Solution. $\Gamma(V) = k[X_1, \ldots, X_n]/I(V)$. The statement follows from Problem 7.1.38.

Problem 7.2.6. *Let $V \subset \mathbb{A}^n$ be a nonempty variety. Show that the following are equivalent:* (1) *V is a point,* (2) *$\Gamma(V) = k$,* (3) $\dim_k \Gamma(V) < \infty$.

Solution. (1) $\Rightarrow$ (2): By Corollary 3.4.8, $I(V) = (X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal. Thus, $\Gamma(V) = k[X_1, \ldots, X_n]/I(V) = k$. (2) $\Rightarrow$ (3): $\dim_k \Gamma(V) = \dim_k k = 1$. (3) $\Rightarrow$ (1): By Corollary 3.4.9, number of points in $V(I(V))$ is atmost 1. Thus, V is a point (as V is nonempty).

Problem 7.2.7. *Let F be an irreducible polynomial in $k[X, Y]$, and suppose F i monic in Y: $F = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$, with $n > 0$. Let $V = V(F) \subset \mathbb{A}^2$. Show that the natural homomorphism from $k[X]$ to $\Gamma(V) = k[X, Y]/(F)$ is one-to-one, so that $k[X]$ may be regarded as a subring of $\Gamma(V)$.*

Solution. ϕ: $k[X] \mapsto k[X, Y]/(F)$, taking $g \to g$ mod (F). If $g_1, g_2 \in k[X]$ $(g_1 \neq g_2)$ such that g_1 mod $(F) = g_2$ mod $(F) \Rightarrow (g_1 - g_2) \in (F) \Rightarrow F \mid (g_1 - g_2)$. But F is a function of X and Y ($\deg(Y) > 0$) and $(g_1 - g_2)$ is function of X. Thus, $F \nmid (g_1 - g_2)$. So, ϕ is one-one. $k[X]$ can be considered a subring of $\Gamma(V)$.

Problem 7.2.8. *Let $\phi : V \to W$ is a polynomial map, and X is an algebraic subset of W, Show that $\phi^{-1}(X)$ is an algebraic subset of V. If $\phi^{-1}(X)$ is irreducible, and X is contained in the image of ϕ, Show that X is irreducible.*

Solution. $X = V(F_1, \ldots, F_r)$, where $S = \{F_1, \ldots, F_r\} \in k[X_1, \ldots, X_n]$. $\phi^{-1}(X)$ $= \phi^{-1}(V(F_1, \ldots, F_r)) = V(F_1 \circ \phi, \ldots, F_r \circ \phi)$. Since, ϕ is onto, $\phi^{-1}(X) \subset V$. Hence,

$\phi^{-1}(X)$ is irreducible.
Let $X = X_1 \cup X_2$, then $\phi^{-1}(X) = \phi^{-1}(X_1) \cup \phi^{-1}(X_2)$. But, both are algebraic, by part (a). Thus, $\phi^{-1}(X) = \phi^{-1}(X_1)$ or $\phi^{-1}(X) = \phi^{-1}(X_2)$. Since, X is contained in image of ϕ, we have $X = X_1$ or $X = X_2$. Thus, X is irreducible.

Problem 7.2.9. (a) *Show that* $X = \{(t, t^2, t^3) \in \mathbb{A}^(k) \mid t \in k\}$ *is affine variety.* (b) *Show that* $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y) \subset \mathbb{A}^3(\mathbb{C})$ *is a variety.*

Solution. X is algebraic set (By Problem 1.11(a)). Let $\phi : \mathbb{C} \to \mathbb{C}^3$ mapping $t \mapsto (t, t^2, t^3)$. Taking $T_1 = X$, $T_2 = X^2$ and $T_3 = X^3$, ϕ is a polynomial map. X is algebraic subset of W. $\phi^{-1}(X) = \mathbb{C}$ is irreducible and X is contained in image of ϕ $\Rightarrow$ X is irreducible (by above problem). Thus, X is affine variety.
Note that $Y^3 - X^4 = -Y(XZ - Y^2) + X(YZ - X^3)$, $Z^3 - X^5 = Z(Z^2 - X^2Y) + X^2(YZ - X^3)$ and $Z^40Y^5 = Z^2(Z^2 - X^2Y) + (XYZ + Y^3)(ZX - Y^2)$. Consider the polynomial map $\phi : \mathbb{C} \to \mathbb{C}^3$ taking $t \mapsto (t^3, t^4, t^5)$. By above problem, it only remains to show that V is contained in image of ϕ. Consider $(x, y, z) \in V$ not all $x, y, z = 0$. Since, $\mathbb{C}$ is algebraically closed, there exists $t \in \mathbb{C}$ such that $x = t^3$. Then $y^3 = t^{12}$ and $z^3 = t^{15}$. So $y = t^4\omega^i$ and $z = t^5\omega^j$ where ω is primitive third root of unity (with $i, j = 0, 1, 2$). By the relation $YZ = X^3$, $t^9\omega^{i+j} = t^9$ or $\omega^j = \omega^{-i}$. Hence, $(x, y, z) = (t^3, t^4\omega^i, t^5\omega^j) = (s^3, s^4, s^5) \in V$ where $s = t\omega^i$.

7.3 Multiple Points and Tangent Lines

Problem 7.3.1. *Prove that in the curves* $C = X^2 - Y^3$, $D = Y^2 - X^3 - X^2$, $E = (X^2 + Y62)^2 + 3X^2Y - Y^3$ *and* $F = (X^2 + Y^2)^3 - 4X^2Y^2$, $P = (0, 0)$ *is the only multiple point on the curve.*

Solution. $\frac{\partial C}{\partial X} = -3X^2$ and $\frac{\partial C}{\partial Y} = 2Y$. By letting $\frac{\partial C}{\partial X} = \frac{\partial C}{\partial Y} = 0$, we get $(X, Y) = (0, 0) \in C$. Thus, C is the only multiple point on C. Similarly for all other curves.

Problem 7.3.2. *If a curve* F *of degree* n *has a point* P *of multiplicity* n*, show that* F *consists of* n *lines through* P *(not necessarily distinct).*

Solution. $F = F_m + F_{m+1} + \cdots + F_n$ where F_i's are forms. $m_P(F) = n$. Let P be $(0, 0)$. Since P is of multiplicity n, $m = n$. Therefore, F is a form in $k[X, Y]$ of degree n. So, we can write $F = \prod L_i^{r_i}$, where L_i are distinct lines passing through P (not distinct).

If $P = (a, b) \neq (0, 0)$ then by using translation $F^T = F(X + a, X + b)$, degree of F^T remains same as degree of F and we can get the result.

Problem 7.3.3. *Let P be double point on curve F. Show that P is a node if and only if $F_{XY}(P)^2 \neq F_{XX}(P)F_{YY}(P)$.*

Solution. Note: An ordinary double point is called node i.e. F has only 2 distinct simple tangents at P (simple tangent L_i means $r_i = 1$). A double point on curve F has $m_P(F) = 2$.
Let $P = (0, 0)$. Let P is ordinary double point on F i.e. $F_m L_1 L_2$.

$$F_m = L_1 L_2 = (\alpha_1 X + \beta_1 Y)(\alpha_2 X + \beta_2 Y)$$

where $\frac{\alpha_1}{\beta_1} \neq \frac{\alpha_2}{\beta_2}$ (as L_1 L_2 are distinct lines). $F = F_m +$ (higher degree terms). Then, $(F_{XX}(P)) = 2\alpha_1\alpha_2$, $(F_{YY}(P)) = 2\beta_1\beta_2$ and $(F_{XY}(P))^2 = (\alpha_1\beta_2 + \beta_1\alpha_2)^2 \neq \alpha_1\alpha_2\beta_1\beta_2$ (as $\frac{\alpha_1}{\beta_1} \neq \frac{\alpha_2}{\beta_2}$).
If P is not a node i.e. $F_m = (\alpha_1 X + \beta_1 Y)^2$, then $F_{XX}(P) = 2\alpha_1^2$, $F_{YY}(P) = 2\beta_1^2$ and $(F_{XY}(P))^2 = (2\alpha_1\beta_1)^2 = F_{XX}(P)F_{YY}(P)$. Using translation, we can prove the statement for any general point $P = (a, b)$.

Problem 7.3.4. (char$(k) = 0$). *Show that $m_P(F)$ is the smallest degree m such that for some $i + j = m$, $\frac{\partial^m F}{\partial X^i \partial Y^j}(P) \neq 0$. Find an explicit description for the leading form for F at P in terms of the derivatives.*

Solution. Consider $P = (0, 0)$. Leading form for F at P in terms of these derivatives is

$$F_m = \sum_{i+j=m} \frac{\partial^n F}{\partial X^i \partial y^j} \cdot \frac{X^i Y^j}{i!j!}$$

$m_P(F)$ is leading form for F at P i.e. F_m. Now if $F = F_m + F_{m+1} + \cdots + F_n$, then differentiating w.r.t. X reduces power of X by 1 and differentiating w.r.t. Y reduces power of Y by 1. $F_m = \prod L_1^{r_i}$. Differentiating F_m, m times w.r.t. X, gives coefficient of X^m in F_m and differentiating F_m, i times w.r.t. X and j times w.r.t. Y, gives coefficient of $X^i Y^j$ in F_m. Since, $F_m \neq 0 \Rightarrow$ there exists i, j $(i + j = m)$ such that $X^i Y^j$ has coefficient non zero. Since, $F_{m'} = 0$ for all $m' < m \Rightarrow X^i Y^j$ $(i + j < m)$ has coefficient zero. So, $\frac{\partial^m F}{\partial X^i \partial Y^j}(P) \neq 0$ for some $i + j = m$.

Bibliography

[1] Algebraic Curves by W. Fulton.

[2] Commutative Algebra by N. S. Gopalakrishnan

[3] Abstract Algebra by Dummit and Foote

[4] Conics and Cubics by R. Bix

[5] On a certain Lemma en-route to the proofs of the Nullstellensatz Theorem, Quillin Suslin Theorem and Forster's Conjecture by R. Sridharan (The Mathematics Student, Special Centenary Volume (2007), 237-240)