A THEOREM OF COWSIK AND NORI

By

D. SURYA RAMANA

A Thesis Submitted to the

FACULTY OF SCIENCE AND HUMANITIES

in partial fulfilment of the requirements
for the award of the degree of

MASTER OF SCIENCE
(by research)
in
MATHEMATICS

ANNA UNIVERSITY
MADRAS - 600 025

APRIL 1996

BONAFIDE CERTIFICATE

Certified that this thesis titled A Theorem of Cowsik and Nori is the bonafide work of Mr. D.Surya Ramana who carried out the research work under my supervision.Certified further that, to the best of my knowledge, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

15/4/96

Head of the Department,	Prof. Sathya Mandal,
Department of Mathematics,	Institute of Mathematical Sciences,
Anna University,	Madras - 600 113.
Madras - 600 025.	

ABSTRACT

This thesis provides an expository account of a proof of the theorem of R.C.Cowsik and M.V.Nori which asserts that curves in affine spaces over fields of positive characteristic are set theoretic complete intersections.

சுருக்கம்

மிகைச் சிறப்பெண் களங்களின் மீதான நேர்வெளியின் வளை கோடுகள், கண இயல் முழுமை லைட்டுக்களாம் என்பது இரா.ச.கௌசிக்கும் மா.வி.நோரியும் நிருபித்த தோற்றத்தின் முடிவு.

இவ்வாய்வுக் கட்டுரை மேற்கூறிய நிருபணத்தை விளக்குகிறது.

ACKNOWLEDGEMENT

I would like to thank Prof.Satya Mandal from whose guidance, suggestions and notes I learnt the proof of the Cowsik-Nori theorem.Without his help I would have found it impossible to complete this thesis.

I wish to thank Prof. R.Balasubramanian, Dr.D.S.Nagraj and Dr. Vijay Kodiyalam for their kindness and encouragement.

I am indebted to my friends at Matscience particularly Ravindra and Swarup Mohalik for helping me in the production of this thesis.

D. Surya Ramana

15 April 1996

TABLE OF CONTENTS

Abstract iii

Chapter 1 Preliminaries 1

1.1 Introduction 1

1.2 Affine algebraic curves 2

1.3 Set-theoretic Complete Intersections 4

Chapter 2 Basic Theorems 7

2.1 Introduction 7

2.2 The Ferrand-Szpiro theorem 9

2.3 A Theorem of Suslin 15

2.4 A Theorem of Mandal 16

2.5 Proof of The Main Theorem 22

Chapter 3 The Cowsik–Nori Theorem 23

3.1 Introduction 23

3.2 A Change of Variables Theorem 23

3.3 The Cowsik-Nori theorem 26

3.4 Some concluding remarks 28

References 30

Chapter 1
PRELIMINARIES

1.1 Introduction

This thesis is an expository account of a proof of the theorem of R.C.Cowsik and M.V.Nori (1978), which asserts that every algebraic curve in an affine space over a field of positive characteristic is a set theoretic complete intersection.

The plan of this thesis is as follows. In the remaining sections of this chapter, we develop some background material which we hope will put this theorem in context.We end this chapter with a precise statement of the Cowsik-Nori theorem.

The proof of this theorem that this thesis presents depends crucially on a theorem of Ferrand- Szpiro and Mohan Kumar. We present a proof of this theorem in Chapter 2.

In chapter 3, which is the final chapter of this thesis, we present a proof of the Cowsik-Nori theorem.This chapter ends with some concluding remarks relating to the main theme of this thesis.

1.2 Affine algebraic curves

In this section we will review the notion of an affine algebraic curve and some other related concepts.

Let k denote an arbitrary field. The set of n tuples $(a_1, a_2, \dots, a_n)$ where each a_i is in $k, 1 \leq i \leq n$, is called the *affine n dimensional space* over k. This set is denoted by $\mathbb{A}_k^n$ or by $\mathbb{A}^n$ when the field k under consideration is obvious from the context.

We wish to give $\mathbb{A}^n$ a topology called the *Zariski topology.* This topology will be prescribed by specifying the collection of its closed sets. This is done as follows.

Let $k[x_1, x_2, \dots, x_n]$ denote the polynomial ring over k in n variables. We will interpret the elements of $k[x_1, x_2, \dots, x_n]$ as functions from $\mathbb{A}^n$ into k by writing $f(P) = f(a_1, a_2, \dots, a_n)$ for any f in $k[x_1, x_2, \dots, x_n]$ and any $P = (a_1, a_2, \dots, a_n)$ in $\mathbb{A}^n$.

Let T be any subset of $k[x_1, x_2, \dots, x_n]$, then we define $Z(T)$, the *zero set* of T in $\mathbb{A}^n$, to be the set of all P in $\mathbb{A}^n$ such that $f(P) = 0$ for all f in T. That is , $Z(T)$ is the set of "common zeros" of the elements of T.

We will define a subset of $\mathbb{A}^n$ to be closed in the Zariski topology on $\mathbb{A}^n$ if and only if it is the zero set of some subset T of $k[x_1, x_2, \dots, x_n]$. Prop. 1.1 in Hartshorne (1977) shows that the Zariski topology is indeed a topology on $\mathbb{A}^n$.

We will define a nonempty subset Y of $\mathbb{A}^n$ to be *irreducible* if Y cannot be written as the union of two proper closed subsets of $\mathbb{A}^n$.

Definition 1.1 An *affine algebraic variety* is an irreducible closed set of $\mathbb{A}^n$ in the Zariski topology.

In order to define an affine algebraic curve, which is a special type of affine algebraic variety, we need to introduce the notion of the dimension of affine algebraic varieties.

Given an affine variety Y in $\mathbb{A}^n$ we may consider the set of all polynomials in n variables over k whose zero set in $\mathbb{A}^n$ is precisely Y. This set of polynomials is easily seen to be a prime ideal in $k[x_1, x_2, \ldots, x_n]$. We denote this ideal by $I(Y)$. Further, we define $\mathbb{A}^n(Y) = k[x_1, x_2, \ldots, x_n]/I(Y)$ to be the affine coordinate ring of the variety Y.

The dimension of the variety Y is defined to be the Krull dimension of its affine coordinate ring $A(Y)$.We will also use the following relation between the height of $I(Y)$ and the dimension of Y.

$$height(I(Y)) + dim(Y) = n \tag{1.1}$$

We refer to Matsumura (1989), page 30 for a definition of dimension and height in this context.

Definition 1.2 An *affine algebraic curve* in $\mathbb{A}^n$ is a one dimensional affine algebraic variety in $\mathbb{A}^n$.

Example 1.1: An affine line is perhaps the simplest example of an affine algebraic curve.

Let $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_n)$ be two fixed points in $\mathbb{A}^n$. The affine line joining A and B is defined as the set of all points

$(x_1, x_2, \ldots, x_n)$ in $\mathbb{A}^n$ which satisfy $x_i = \lambda a_i + (1-\lambda)b_i$ for all $1 \leq i \leq n$ and some $\lambda \in k$.

By eliminating the variable λ from the equations defining the affine line one may see that an affine line is the zero set of $n-1$ linearly independent linear polynomials (with constant terms). Consequently, one may show that the dimension of the affine line is 1, making it an affine algebraic curve.

Note that as a variety the dimension of $\mathbb{A}^n$ is n. Hence,in analogy with the notion of a hyperplane in linear algebra we define

Definition 1.3 A *hypersurface* in $\mathbb{A}^n$ is an affine variety of dimension $n-1$.

Just as a hyperplane in linear algebra is determined as the zero set of a single nonconstant linear polynomial we have

Proposition 1.1 An affine algebraic variety in $\mathbb{A}^n$ is a hypersurface if and only if it is the zero set of a single nonconstant irreducible polynomial in $k[x_1, x_2, \ldots, x_n]$.

Proof: See Hartshorne (1977), page 7.

1.3 Set-theoretic complete intersections

In this section we will define the basic question that is considered in this thesis.

$(x_1, x_2, \ldots, x_n)$ in $\mathbb{A}^n$ which satisfy $x_i = \lambda a_i + (1-\lambda)b_i$ for all $1 \leq i \leq n$ and some $\lambda \in k$.

By eliminating the variable λ from the equations defining the affine line one may see that an affine line is the zero set of $n-1$ linearly independent linear polynomials (with constant terms). Consequently, one may show that the dimension of the affine line is 1, making it an affine algebraic curve.

Note that as a variety the dimension of $\mathbb{A}^n$ is n. Hence,in analogy with the notion of a hyperplane in linear algebra we define

Definition 1.3 A *hypersurface* in $\mathbb{A}^n$ is an affine variety of dimension $n-1$.

Just as a hyperplane in linear algebra is determined as the zero set of a single nonconstant linear polynomial we have

Proposition 1.1 An affine algebraic variety in $\mathbb{A}^n$ is a hypersurface if and only if it is the zero set of a single nonconstant irreducible polynomial in $k[x_1, x_2, \ldots, x_n]$.

Proof: See Hartshorne (1977), page 7.

1.3 Set-theoretic complete intersections

In this section we will define the basic question that is considered in this thesis.

To get to it we will let ourselves be lead by the analogy with linear varieties that we have pursued so far. In example 1.1 it has been remarked that every affine line is the intersection of $n-1$ hyperplanes. Here, by intersection we mean the intersection of the hyperplanes viewing them as subsets of $\mathbb{A}^n$. Emphasizing this we may say that an affine line is the *set-theoretic complete intersection* of $n-1$ hyperplanes. Motivated by this observation we ask

Question 1.1 *Is every affine algebraic curve in the affine space $\mathbb{A}^n$ over a field k the set-theoretic complete intersection of $n-1$ hypersurfaces in $\mathbb{A}^n$?*

This question is the basic theme of this thesis. We will prefer to restate this question in a more algebraic language, as follows.We will need the following definition.

Definition 1.4 An ideal I of height m is said to be of *pure height m* if the radicals of all the ideals that appear in the primary decomposition of I are of height m.

We refer to Matsumura (1989) for a definition of primary decomposition.

Let Y be an affine curve. Since $I(Y)$ is a prime ideal ,we know from equation 1.1, $I(Y)$ is of pure height $n-1$. Further, we will introduce the following terminology.

Definition 1.5 An ideal I in $k[x_1, x_2, \ldots, x_n]$ is said to be set-theoretically generated by $n-1$ elements if there exist irreducible polynomials $f_1, \ldots, f_{n-1}$ in $k[x_1, x_2, \ldots, x_n]$ such that $\sqrt{I} = \sqrt{f_1 \ldots, f_{n-1}}$.

It follows from the Nullstellensatz and Proposition 1.1 that Y is a set theoretic intersection of $n-1$ hypersurfaces if and only if $I(Y)$ is set theoretically generated by $n-1$ elements. See Hartshorne (1977) prop. 1.2.d for a proof.

In the light of these observations we may rewrite question 1.1 as follows.

Question 1.2 *Let k be an arbitrary field and I be an ideal of pure height $n-1$ in $k[x_1, x_2, \ldots, x_n]$. Is I set theoretically generated by $n-1$ elements ?*

The theorem of Cowsik and Nori answers this question in the affirmative for fields of positive characteristic.

Theorem 1.1 (Cowsik-Nori) Let k be a field of positive characteristic and let I be an ideal of pure height $n-1$ in $k[x_1, x_2, \ldots, x_n]$. Then I is set-theoretically generated by $n-1$ elements.

At this point the reader is perhaps curious to know what happens over characteristic zero fields. For this and related remarks we direct the reader's attention to the section titled some concluding remarks in Chapter 3.

Chapter 2
BASIC THEOREMS

2.1 Introduction

The proof of the Cowsik-Nori theorem presented in this thesis proceeds by showing that an ideal I of pure height $n-1$ in $k[x_1, x_2, \ldots, x_n]$ is a *locally complete intersection ideal* and then appealing to a theorem of Ferrand-Szpiro and Mohan Kumar which asserts that if I is a locally complete intersection ideal of height $n-1$ in $k[x_1, x_2, \ldots, x_n]$, then I is set theoretically generated by $n-1$ elements.

In this chapter we give a proof of the theorem of Ferrand-Szpiro and Mohan Kumar that is used in this context. In order to state this theorem we will need some definitions.

Definition 2.1 Let A be a commutative ring and I and J be two ideals in A. Then I and J are said to be *equal upto radicals* if $\sqrt{I} = \sqrt{J}$.

Definition 2.2 Let A be a noetherian commutative ring. An ideal I is called a *complete intersection ideal* of height r if I is generated by a regular sequence $a_1, \ldots, a_r$ of length r.

We refer to page 123 of Matsumura (1989) for a definition of a regular sequence.

Definition 2.3 An ideal I of a noetherian commutative ring A is said to be a *locally complete intersection ideal* of height r if $I_\wp$ is complete intersection ideal of height r for all $\wp$ in $V(I) = \{\wp \text{ in } SpecA : I \subseteq \wp\}$.

Theorem 2.1 (Ferrand-Szpiro, Mohan Kumar) Let I be a locally complete intersection ideal in $k[x_1, x_2, \ldots, x_n]$ of height $n-1$.Then I is set theoretically generated by $n-1$ elements in $k[x_1, x_2, \ldots, x_n]$.

The proof of this theorem proceeds as follows. Given a locally complete intersection ideal I in $k[x_1, x_2, \ldots, x_n]$ of height $n-1$ we will produce an ideal J which is set theoretically generated by $n-1$ elements and which is equal to the ideal I upto radicals. It then follows that the ideal I is also set theoretically generated by $n-1$ elements.

The proof of the Ferrand-Szpiro, Mohan Kumar theorem is accordingly broken up into two parts .

The first part is a theorem of Ferrand-Szpiro which suggests a candidate for the ideal J, given the ideal I. This theorem is proved in sec. 2.2.

The second part is a theorem of Mohan Kumar which proves that the ideal J suggested by the first part actually satisfies the requirements. The aim of sections 2.3 to 2.5 is to give a proof of this theorem.

2.2 The Ferrand-Szpiro theorem

Before stating the Ferrand-Szpiro theorem we state a number of preliminary results that will be used in the proof of the Ferrand-Szpiro theorem.

The first theorem is the theorem of the basic element of Eisenbud and Evans. We state for the convenience of the reader a few notations and definitions.

Let A be a noetherian commutative ring and let M be a finitely generated A-module.

$\mu(M)$ will denote the minimal number of generators of M. For a prime ideal $\wp$, $\mu(M_\wp)$ will denote the minimal number of generators of $M_\wp$ as an $A_\wp$-module.

Definition 2.4 An element m of M is said to be a *basic element* of M *at a prime ideal* $\wp$ if m is not in $\wp M_\wp$.An element m of M is said to be a *basic element* of M if m is basic in M at all the prime ideals $\wp$ of A. We also say that m is *basic in M on a subset X of Spec A* if m is basic in$M$ at all prime ideals in X.

Definition 2.5 A submodule M' of M is said to be $w-fold\ basic$ in M, for a non negative integer w, at a prime ideal $\wp$, if $\mu((M/M')_\wp) \leq \mu(M_\wp) - w$.We say that a set of elements $\{m_1, \ldots, m_t\}$ of M is $w-fold\ basic$ in M at $\wp$ if $M' = \sum_{i=1}^{t} Am_i$ is w-fold basic in M at $\wp$.

Let X be a subset of Spec A and let $\mathcal{N} = \{0, 1, 2, \ldots\}$ be the set of natural numbers. Let $d : X \to \mathcal{N}$ be a function.We define a partial ordering on X by defining $\wp_1 \ll \wp_2$ if $\wp_1 \subseteq \wp_2$ and $d(\wp_1) > d(\wp_2)$ for $\wp_1, \wp_2$ in X. Then we have

Definition 2.6 A function $d : X \to \mathcal{N}$ is said to be a *generalized dimension function* if for any ideal I of A, $V(I) \cap X$ has only finite number of minimal elements with respect to the partial ordering $\ll$ defined above.

Theorem 2.2 (Eisenbud-Evans) Let A be a noetherian commutative ring and let $d : X \to \mathcal{N}$ be a generalized dimension function on a subset X of spec A. Let M be a finitely generated A-module. Then

(i) If $\mu(M_\wp) > d(\wp)$ for all $\wp$ in X, then M has a basic element on X.

(iia) Let M' be a submodule of M, such that M' is $(d(\wp)+1)$-fold basic in M for all $\wp$ in X. Then M' contains an element that is basic in M on X.

(iib) Let $m_1, m_2, \ldots, m_r$ be elements in M that is $(d(\wp)+1)$-fold basic in M for all $\wp$ in X. If (a, m_1) is basic in $A \oplus M$ on X, then there is $m' = a_2m_2 + a_3m_3 + \ldots + a_rm_r$ for $a_2, \ldots, a_r$ in A such that $m_1 + am'$ is basic in M on X.

Proof: See Evans and Griffiths (1985), chapter 2. This reference gives the proof for a specific dimension function. However, modifying the proof for the generalised dimension function is straightforward.

We shall presently state two fundamental theorems about projective modules which may be proved as corollaries to the Eisenbud-Evans theorem given above.

Theorem 2.3 (Serre) Let A be a noetherian commutative ring of dimension d and let P be a finitely generated projective A-module such then rank $(P_{\wp}) > d$ for all $\wp$ in Spec A. Then P is the direct sum of a free module and a projective module of rank 1.

Proof: See Evans and Griffiths (1985), chapter 2.

Theorem 2.4 (Bass) Let P be a finitely generated projective module over a noetherian commutative ring A, with rank $(P_{\wp}) > \dim A$, for all $\wp$ in Spec A. Then $P \oplus Q \approx P' \oplus Q$ for finitely generated projective A-modules P' and Q implies that $P \approx P'$.

Proof: See Bass (1960).

The following consequence of the Eisenbud-Evans theorem is also used in the proof of the Ferrand-Szpiro theorem.

Lemma 2.1 Let A be a noetherian commutative ring of dimension ≤ 1. Let L_1 and L_2 be two rank one projective A-modules.Then $L_1 \oplus L_2 \approx A \oplus L_1 L_2$.

Proof: Without loss of generality, we can assume that A is reduced. Let S be the set of all nonzero divisors of A. Since $S^{-1}L_1 \approx S^{-1}A$, we can assume that $L_1 = I_1$ is an ideal of A. By Theorem 2.2, there is an f in $Hom(L_2, A)$ that is basic on $V(I_1)$ and also at all the minimal primes of A. Let $f(L_2) = I_2$,then $L_2 \approx I_2$ and $I_1 + I_2 = A$. Hence we have an exact sequence

$$0 \longrightarrow I_1 \bigcap I_2 \longrightarrow I_1 \oplus I_2 \longrightarrow A \longrightarrow 0\,.$$

Since $I_1 \bigcap I_2 = I_1 I_2 \approx L_1 L_2$, the proof of is complete.

We end this list of preliminary theorems by stating and proving

Theorem 2.5 Let A be a noetherian commutative ring and let L be a projective A-module of constant rank one. Then L has *cancellative property*, i.e. $L \oplus Q \approx L' \oplus Q$ for finitely generated projective A-modules L' and Q implies that $L \approx L'$.

Proof: Let $L \oplus Q \approx L' \oplus Q$. By tensoring with $L'^{-1} = \mathrm{Hom}(L', A)$, we get $LL'^{-1} \oplus Q' \approx A \oplus Q'$ where $Q' = Q \otimes L'^{-1}$. Since it is enough to prove $LL'^{-1} \approx A$, we can assume that $L' = A$.

So, we have $L \oplus Q \approx A \oplus Q$. Since $Q \oplus Q_1 \approx A^n$ is free for some Q_1, we have $L \oplus A^n \approx A^{n+1}$ for some integer $n \geq 0$.

Let $f : L \oplus A^n \longrightarrow A^{n+1}$ be an isomorphism. Let $e_2 = (0, 1, \ldots, 0)$, $e_3 = (0, 0, 1, 0, \ldots, 0), \ldots, e_{n+1} = (0, 0, \ldots, 1)$ be the standard basis of A^n in $L \oplus A^n$ and let $e'_1, e'_2, \ldots, e'_{n+1}$ be the standard basis of A^{n+1}. For x in L, let

$$\begin{pmatrix} f(x) \\ f(e_2) \\ f(e_3) \\ \vdots \\ f(e_{n+1}) \end{pmatrix} = u(x) \begin{pmatrix} e'_1 \\ e'_2 \\ \vdots \\ e'_{n+1} \end{pmatrix}$$

where $u(x)$ is an $(n+1) \times (n+1)$- matrix in $\mathcal{M}_{n+1}(A)$. Define a map $F : L \longrightarrow A$ as $F(x) = \det u(x)$. Since $L_\wp \approx A_\wp$ for all $\wp$ in Spec A, and $f_\wp : A_\wp^{n+1} \longrightarrow A_\wp^{n+1}$ is an isomorphism, $F_\wp(e)$ an unit in $A_\wp$ if e is a generator of $L_\wp$. Hence $F_\wp$ is isomorphism for all $\wp$ in Spec A. So, $F : L \longrightarrow A$ is an isomorphism.

We are now in a position to state and prove the Ferrand-Szpiro theorem.

Theorem 2.6 (Ferrand-Szpiro) Let A be a noetherian commutative ring and let I be a locally complete intersection ideal of height $r \geq 2$ and $\dim R/I \leq 1$. Then there is a locally complete intersection ideal J of height r such that

(i) $\sqrt{I} = \sqrt{J}$

(ii) J/J^2 is free A/J-module of rank r.

Proof: Since rank $I/I^2 = r > \dim(A/I)$, by (2.3), $I/I^2 = F \oplus L$ where L is a projective A/I-module of rank oneand F is a free A/I-module of rank $r-1$. Since $I/I^2 \otimes L$ has a free direct summand (2.3), there is a surjective map $\phi : I/I^2 \longrightarrow L^{-1}$, where $L^{-1} = Hom(L, A/I)$. Let $J/I^2 =$ kernel (ϕ).

Since $I^2 \subseteq J \subseteq I$ we have $\sqrt{I} = \sqrt{J}$. To see that J is a locally complete intersection ideal of height r, let $\wp$ be a prime ideal in $V(I) = V(J)$.

Let f_r be an element in $I_\wp$ be such that image of f_r in $L_\wp^{-1}$, via ϕ, generates $L_\wp^{-1}$ and let $f_1, \ldots, f_{r-1}$ be in $J_\wp$ be such that their images generate $(J/I^2)_\wp$. So, $I_\wp = (f_1, f_2, \ldots, f_{n-1}, f_r) + I_\wp^2$ and hence $I_\wp = (f_1, f_2, \ldots, f_{r-1}, f_r)$. By induction, we shall prove that for $1 \leq i \leq r$ there are $g_1, \ldots, g_i$ in $I_\wp$ such that (1) $I_\wp = (g_1, \ldots, g_i, f_{i+1}, \ldots, f_r)$, (2) $g_1, \ldots, g_i$ is a regular sequence and (3) $g_i - f_i$ is in $J_\wp^2$. To do this we assume that the assertions holds for $i < r$ and prove the assertions for $i+1$. We write $A' = A_\wp, I' = I_\wp, J' = J_\wp$. Let $\wp_1, \ldots, \wp_k$, be the associated primes of $A'/(g_1, \ldots, g_i)A'$ and let $P_1, \ldots, P_t$ be maximal elements in the set $\{\wp_1 \ldots, \wp_k\}$. For $\ell = 1$ to t, since depth $A'_{P_k} = i < r$ and since I' is generated by a regular sequence of length r, it follows that I' is not contained in P_ℓ. Hence J' is not contained in P_ℓ. Letf_{i+1} be in $P_1, \ldots, P_{t_0}$ and not in $P_{t_0+1}, \ldots, P_t$ and let λ be in $J'^2 \bigcap P_{t_0+1} \bigcap \ldots \bigcap P_t \backslash P_1 \bigcup \ldots \bigcup P_{t_0}$ and let $g_{i+1} = f_{i+1} + \lambda$. So, $J' = (g_1, \ldots, g_i, g_{i+1}, f_{i+2}, \ldots, f_r) + I'^2$ and hence

$I' = (g_1, \ldots, g_{i+1}, f_{i+2}, \ldots, f_r)$. This establishes the assertion.

Hence there are $g_1, \ldots, g_r$ such that (1) $I' = (g_1, \ldots, g_r)$, (2) $g_1, \ldots, g_r$ is a regular sequence, (3) the images of$g_1, \ldots, g_{r-1}$ generate J'/I'^2 and the image of g_r generate $L_{\wp}^{-1}$. Note that g_r^2 is in J'. Now if g is in J' then $g - (\lambda_1 g_1 + \ldots + \lambda_{r-1} g_{r-1})$ is in $I'^2 = (g_1, \ldots, g_r)^2$. Hence g is in $(g_1, \ldots, g_{r-1}, g_r^2)$. So, $J' = (g_1, \ldots, g_{r-1}, g_r^2)$ is generated by a regular sequence of length r. Therefore J is a locally complete intersection ideal of height r.

To prove that J/J^2 is free A/J-module of rank r, note that I/J is nilpotent in A/J and hence it is enough to prove that $J/J^2 \otimes A/I \approx J/IJ$ is free A/I-module.

We have two exact sequences

$$0 \longrightarrow J/I^2 \longrightarrow I/I^2 \longrightarrow L^{-1} \longrightarrow 0$$

and

$$0 \longrightarrow I^2/IJ \longrightarrow J/IJ \longrightarrow J/I^2 \longrightarrow 0$$

of projective A/I-modules. Also note that $L^{-1} \approx I/J$ and $L^{-2} \approx I/J \otimes I/J \approx I^2/IJ$. Again by (2.3) $J/IJ \approx F \oplus L_0$ for some projective A/I-module L_0 of rank one. It is enough to prove that $L_0 \approx A/I$. We have $J/I^2 \oplus L^{-1} \approx I/I^2 \approx F \oplus L_0$ and $L^{-2} \oplus J/I^2 \approx J/IJ \approx F \oplus L_0$. So, $L^{-2} \oplus (F \oplus L) \approx L^{-2} \oplus (J/I^2 \oplus L^{-1}) \approx F \oplus L_0 \oplus L^{-1}$. By the Theorem 2.4, $L^{-2} \oplus L \approx L_0 \oplus L^{-1}$. Now the theorem follows from Theorem 2.5 and Lemma 2.1.

2.3 A theorem of Suslin

In this section we present an important theorem of Suslin which guarantees that under a change of variables any ideal with a suitably large height in a polynomial ring has a monic polynomial. We begin with the following lemma.

Lemma 2.2 Let $R = A[X]$ be a polynomial ring over a noetherian commutative ring A and I be an ideal in R. Let $\ell(I) = \{a \in A :$ there is an f in R such that $f = aX^n + a_1X^{n-1} + \ldots + a_n\}$. Then the $\ell(I)$ is an ideal in A and height $(\ell(I)) \geq$ height I.

Proof: It is obvious that $\ell(I)$ is an ideal. Further, since $\ell(\sqrt{I}) \subseteq \sqrt{\ell(I)}$, we can assume that I is a reduced ideal. Let $I = \wp_1 \bigcap \ldots \bigcap \wp_k$ where $\wp_1, \ldots, \wp_k$ are minimal primes over I. As $\ell(\wp_1)\ell(\wp_2)\ldots\ell(\wp_k) \subseteq \ell(I)$, it is enough to prove the lemma for prime ideals I. If I is an extended prime ideal then $I = \ell(I)R$ and hence height (I) = height $(\ell(I))$. If I is not extended then let $\wp = I \bigcap A$. Then $\wp R \neq I$ and height $\wp$ = height $(I) - 1$. Note that $\wp \subseteq \ell(I)$. Let $\wp'$ be a minimal prime over $\ell(I)$. As height $(\wp)'$ = height $(\wp)$ would imply that $\ell(I) = \wp$ and $I = \wp R$ is extended, we have height $\wp' >$ height $\wp$ = height$(I) - 1$. This completes the proof.

Now we state the theorem of Suslin.

Theorem 2.7 (Suslin) Let $R = A[X_1, \ldots, X_n]$ be a polynomial ring over a noetherian commutative ring A and let I be an ideal in R such that height $(I) > \dim A$. Let $\phi : R \longrightarrow R$ be the A-algebra automorphism such that $\phi(X_i) = X_i + X_n^{r_i}$ for $i = 1, \ldots, n-1$ and $\phi(X_n) = X_n$, where $r_1, \ldots, r_n$ are nonnegative integers. If $r_1, \ldots, r_n$ are large enough then $\phi(I)$ contains a monic polynomial in X_n with coefficients in $A[X_1, \ldots, X_{n-1}]$. In particular, if A is a field then for any nonzero polynomial f in R, $\phi(f)$ is monic in X_n with coefficients in $A[X_1, \ldots, X_{n-1}]$.

Proof: The theorem is established by a straightforward induction argument on the number of variables n , using the above lemma at each step.

2.4 A theorem of Mandal

Our proof of the Ferrand-Szpiro, Mohan Kumar theorem proceeds via the theorem of Mandal on efficient generation of ideals in polynomial rings.This theorem gives a sufficient condition for an ideal I in a polynomial ring to be generated by $\mu(I/I^2)$ elements.The importance of this result stems from the fact that one can prove that it requires at least $\mu(I/I^2)$ elements to generate I.

In this section we give a proof of this theorem. As usual we begin with some definitions and preliminary theorems.

Definition 2.7 Let $R = A[X, X^{-1}]$ be a Laurent polynomial ring over a commutative ring A. A Laurent polynomial f is called a *doubly monic polynomial* if the both the coefficients of the highest and lowest degree terms of f are units in A.

The first theorem that we state is the Quillen-Suslin theorem on the freeness of projective modules over polynomial rings.

Theorem 2.8 (Quillen-Suslin) Let $R = A[X_1, \ldots, X_n]$ be a polynomial ring over a principal ideal domain A. Then any finitely generated projective R-module is free.

Proof: See Lam (1978)

The next theorem we need is Plumstead's theorem on patching.

Theorem 2.9 (Plumstead) Let A be a commutative noetherian ring and let $R = A[X]$ be the polynomial ring. Let s_1, s_2 be in A such that $As_1 + As_2 = A$. For two R-modules M and M', let $f_1 : M_{s_1} \longrightarrow M'_{s_1}$ and $f_2 : M_{s_2} \longrightarrow M'_{s_2}$ be two isomorphisms such that $(f_1)_{s_2} \equiv (f_2)_{s_1}$ (module X). Also assume that $M_{s_1 s_2}$ is extended from $A_{s_1 s_2}$. Then there is an isomorphism $f : M \longrightarrow M'$such that $(f)_{s_i} \equiv f_i$ modulo X.

Proof: See Plumstead (1979)

Finally, we need the following lemma on *prime avoidance*.

Lemma 2.3 Let A be a commutative noetherian ring and let I, J be two ideals of A so that $J \subseteq I$. Let $n = \mu(I/I^2)$ and let $f_1, f_2, \ldots, f_r$ be elements of I with $r < n$. Assume that

(1) $(f_1, f_2, \ldots, f_r, g_{r+1}, \ldots g_n) + I^2 = I$ for some $g_{r+1}, \ldots, g_n$ in I,

(2) whenever a prime ideal $\wp$ contains $(f_1, \ldots, f_r) + J$ and does not contain I, the image of $\wp$ in $A/(f_1, J)$ has height at least d, for some fixed integer d.

Then one can find an element f_{r+1} in I such that

(1) $(f_1, \ldots, f_r, f_{r+1}, g_{r+2}, \ldots, g_n) + I^2 = I$

(2) whenever a prime ideal $\wp$ contains $(f_1, \ldots, f_r, f_{r+1}) + J$ and I is not contained in $\wp$, then the image of $\wp$ in $A/(f_1, J)$ has height at least $d + 1$.

Proof: Let $\wp_1, \ldots, \wp_k$ be minimal primes over $(f_1, \ldots, f_r) + J$ that does not contain I. Note that images of $\wp_i$ in $A/(f_1, J)$ has height at least d. Assume that g_{r+1} is in $\wp_1 \ldots, \wp_t$ and not in $\wp_{t+1}, \ldots, \wp_k$. Let λ be in $I^2 \bigcap \wp_{t+1} \bigcap \cdots \bigcap \wp_k \backslash \wp_1 \bigcup \cdots \bigcup \wp_t$. The assertion follows with $f_{r+1} = g_{r+1} + \lambda$.

Now we shall state and prove the main theorem of this section.

Theorem 2.10 (Mandal) Let $R = A[X]$ be a polynomial ring over a noetherian commutative ring A and let I be an ideal of R that contains a monic polynomial. If $\mu(I/I^2) \geq \dim(R/I) + 2$, then $\mu(I) = \mu(I/I^2)$.

Proof: Let $J = A \bigcap I$. Let $n = \mu(I/I^2)$ and $I = (g_1, \ldots, g_n) + I^2$ for some $g_1, \ldots, g_n$ in I. Since I contains a monic polynomial, for large enough integer $p, f_1 = g_1 + f^p$ is monic and $I = (f_1, g_2, \ldots, g_n) + I^2$. Since $A/J \longrightarrow R/I$ and $A/J \longrightarrow R/(J, f_1)$ are integral extensions, $\dim(R/I) = \dim(A/J) = \dim(R/(J, f_1))$. By repeated application of Lemma 2.3, we can find $f_2, \ldots, f_n$ such that $I = (f_1, \ldots, f_n) + I^2$ and for any prime ideal $\wp$ in Spec R, if $(f_1, \ldots, f_n) + JR$ is contained in $\wp$ and I is not contained in $\wp$ then image of $\wp$ in $R/(J, f_1)$ has height at least $n - 1$, which is impossible because $n - 1 > \dim R/(J, f_1)$. Hence for any prime $\wp$ in Spec R, if $(J, f_1, f_2, \ldots, f_n)$ is contained in $\wp$ then I is also contained in $\wp$.

Now let $R_1 = R[T, T^{-1}] = A[X, T, T^{-1}]$ be the Laurent polynomial ring in variable T over R.

Let $\psi : R_1 \longrightarrow R_1$ be the A-automorphism such that $\psi(X) = X + T + T^{-1}$ and $\psi(T) = T$.

We shall write $I_1 = \psi(IR_1), I' = I_1 \bigcap R[T]$ and $J' = I' \bigcap R = I_1 \bigcap R$. Since $\psi(J) = J$ is contained in J', it follows that

(i) $(\psi(f_1), \ldots, \psi(f_n)) + I_1^2 = I_1$,

(ii) if $(\psi(f_1, \ldots, \psi(f_n)R_1 + J'R_1$ is contained in a prime ideal $\wp$ in Spec R_1, then I_1 is also contained in $\wp$.

Since f_1 is monic in $X, \psi(f_1)$ is doubly monic in T over R. Hence there is an integer $r_1 \geq 0$ such that $a_1 = T^{r_1}\psi(f_1)$ is a monic polynomial in $R[T]$ with $a_1(0) = 1$. We can pick integers $r_2, \ldots, r_n$ such that $a_i = T^{r_i}\psi(f_i)$ isin $TR[T]$.

Since $TR[T] + a_1R[T] = R[T]$, it follows from (i) and (ii) that (iii) $I' = (a_1, \ldots, a_n)R[T] + I'^2$,

(iv) if $(a_1, \ldots, a_n)R[T] + J'R[T]$ is contained in a prime ideal $\wp$ in Spec $R[T]$, then I' is also contained in $\wp$.

We shall prove that I' is generated n elements.

First claim that $I'_{1+J'} = (a_1, \ldots, a_n)R_{1+J'}[T]$.

To see this let m be a maximal ideal in Spec $(R_{1+J'}[T])$ that contains $(a_1, \ldots, a_n)$. Since $R_{1+J'} \longrightarrow R_{1+J'}[T]/(a_1)$ is an integral extension, J' is in the radical of $R_{1+J'}/(a_1)$ and hence by (iv) it follows that $I'_{1+J'}$ is contained in m. So, by (iii) it follows that $(I'_{1+J'})_m = (a_1, \ldots, a_n)R_{1+J'}[T]_m$. Therefore $I'_{1+J'} = (a_1, a_2, \ldots a_n)R_{1+J'}[T]$.

So there is an s in J' such that $I'_{1+s} = (a_1, \ldots, a_n)R_{1+s}[T]$. Let $\phi_1 : R_{1+s}[T]^n \longrightarrow I'_{1+s}$ be the surjective map defined by $\phi_1(e_i) = a_i$, where $e_1, \ldots, e_n$ is the standard basis of $R^n_{1+s}[T]$. Also let $\phi_2 : R_s[T]^n \longrightarrow I'_s = R_s[T]$ be the surjective map defined by $\phi_2(e_1) = 1$ and $\phi_i(e_i) = 0$ for $i = 2$ to n.

Now let K = kernel ϕ_1 and $K' = kernel(\phi_2)$. Note that $K'$is free. Further, since K_s is projective and $(K_s)_{a_1}$ is free, by the theorem of Quillen and Suslin (Theorem 2.8), K_s is free.

Now let "bar" denote "modulo T". Since $\bar{a}_1 = 1$ and $\bar{a}_i = 0$ for $i = 2, \ldots, n$ it follows that $\overline{(\phi_1)}_s = (\overline{\phi_2})_{1+s}$. So, we have an isomorphism $\beta_0 : K_s \longrightarrow K'_{1+s}$ such that the following diagram of exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \bar{K}_s & \longrightarrow & R^n_{s(1+s)} & \longrightarrow & \bar{I}'_{s(1+s)} & \longrightarrow & 0 \\
 & & \downarrow \beta_0 & & \| & & \| & & \\
0 & \longrightarrow & K'_{1+s} & \longrightarrow & R_{s(1+s)} & \longrightarrow & \bar{I}^1_{s(1+s)} & \longrightarrow & 0
\end{array}$$

commutes.

Since K_s and K'_{1+s} are extended modules, there is an isomorphism $\beta : K_s \longrightarrow K'_{1+s}$ such that $\bar{\beta} = \beta_0$. Using splittings of $(\phi_1)_s$ and $(\phi_2)_{1+s}$ which are equal "modulo T", there is an isomorphism $\theta : R_{s(1+s)}[T]^n \longrightarrow R_{s(1+s)}[T]^n$

such that $\bar{\theta} = Id$ and the following diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & K_s \arrow[r] \arrow[d, "\beta"] & R_{s(1+s}[T]^n \arrow[r, "\phi_1"] \arrow[d, "\theta"] & I_{s(1+s)} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & K'_{1+s} \arrow[r] & R_{s(1+s}[T]^n \arrow[r, "\phi_2"] & \bar{I}_{s(1+s)} \arrow[r] & 0
\end{tikzcd}$$

commutes.

Since $sR + (1+s)R = R$, we have the following fibre product diagram :

$$\begin{tikzcd}
Q \arrow[rr] \arrow[dr, "\phi"] \arrow[dd] & & R_s[T]^n \arrow[dr, "\phi_2"] \arrow[dd] & \\
& I' \arrow[rr] \arrow[dd] & & I'_s \arrow[dd] \\
R_{1+s}[T]^n \arrow[rr, "F"] \arrow[dr, "\phi_1"] & & R_{s(1+s)}[T]^n \arrow[dr] & \\
& I'_{1+s} \arrow[rr] & & I'_{s(1+s)}
\end{tikzcd}$$

Here $F : R_{1+s}[T]^n \longrightarrow R_{s(1+s)}[T]^n$ is the composition map $R_{1+s}[T]^n \to R_{s(1+s)}[T]^n \xrightarrow{\theta} R_{s(1+s)}[T]^n$. In this diagram Q is the fibre product of $R_s[T]^n$ and $R_{1+s}[T]^n$ via θ. The map $\phi : Q \longrightarrow I'$ is got by properties of fibre product. ϕ is surjective because ϕ_1 and ϕ_2 are surjective.

If $\theta_1 : Q_s \longrightarrow R_s[T]^n$ and $\theta_2 : Q_{1+s} \longrightarrow R_{1+s}[T]^n$ are the natural isomorphisms, then $(\theta_1)_{1+s} o (\theta_2^{-1})_s = \theta \equiv Id$ modulo T. By (2.9), it follows that $Q \approx R[T]^n$ is free. Hence I' is generated by n elements.

Therefore, $\psi(IR[T, T^{-1}]) = I_1 = I'_T$ is also generated by n elements and hence so is $IR[T, T^{-1}]$. Now by substituting $T = 1$, it follows that I is generated by n elements. The proof is is complete.

2.5 Proof of the main theorem

In this section we will show how the theorem of Ferrand-Szpiro and Mohan Kumar is a consequence of the theorem of Mandal proved in the previous section.

Theorem 2.11 ***(Mohan Kumar)*** *Suppose $R = k[X_1, \ldots, X_n]$ is a polynomial ring over a field k and I is an ideal of R. If $\mu(I/I^2) \geq dim(R/I) + 2$ then $\mu(I) = \mu(I/I^2)$.*

Proof: *This theorem is an immediate consequence of Theorem 2.1 and the change of variable theorem ,Theorem 2.7.*

Theorem 2.1 (Ferrand-Szpiro, Mohan Kumar) Let I be a locally complete intersection ideal in $k[x_1, x_2, \ldots, x_n]$ of height $n-1$.Then I is set theoretically generated by $n-1$ elements in $k[x_1, x_2, \ldots, x_n]$.

Proof: We can assume $n \geq 3$. By Theorem 2.6 there is a locally complete intersection ideal J such that

(1) $\sqrt{J} = \sqrt{I}$

(2) J/J^2 is free A/J-module of rank $n-1$.

Hence by theorem (2.11) $\mu(J) = \mu(J/J^2) = n-1$. This completes the proof of Theorem 2.1.

Chapter 3

THE COWSIK-NORI THEOREM

3.1 Introduction

In this chapter we give a proof of the Cowsik-Nori theorem based on Luybeznik's survey paper, Luybeznik (1987).

We begin with a change of variables lemma whose proof was kindly supplied by Prof. M.Balwant Singh.

3.2 A change of variables theorem

We begin with the following lemmas.

Lemma 3.1 Let $k[X, Y]$ be a polynomial ring in two variables over a perfect field k with *characteristic* $k = p$ and f be an irreducible polynomial. Then either $\partial f/\partial X \neq 0$ or $\partial f/\partial Y \neq 0$.

Proof: Assume $p \geq 1$. In case $\partial f/\partial X = \partial f/\partial Y = 0$ then $f = g^p$ for some g in $k[X, Y]$. But since f is irreducible the proof is complete.

Lemma 3.2 Let $k[X,Y]$ and f be as in lemma Then for large enough m, if p does not divide m, we have $f(X+Y^m,Y)$ is monic in Y and $\partial f(X+Y^m,Y)/\partial Y \neq 0$.

Proof: Let $F = F_m = f(X+Y^m,Y)$. By Theorem 2.7, F is monic in Y. We also have $\frac{\partial F}{\partial Y} = mY^{m-1}\frac{\partial f}{\partial X}(X+Y^m,Y) + \frac{\partial f}{\partial Y}(X+Y^m,Y)$. Now if $\frac{\partial f}{\partial Y} \neq 0$ then there is an integer m_0 such that $\partial f/\partial Y$ is not in (Y^{m_0}) . Hence for any nonnegative integer m, $\frac{\partial f}{\partial Y}(X+Y^m,Y)$ is not in (Y^{m_0}). It follows in this case that for $m \geq m_0+1$, $\partial F/\partial Y \neq 0$.In case $\partial f/\partial Y = 0$ then by (3.1) $\partial f/\partial X \neq 0$ and hence $\partial F/\partial Y = mY^{m-1}\frac{\partial f}{\partial X}(X+Y^m,Y) \neq 0$ if p does not divide m.

We need the following standard fact.

Lemma 3.3 Let $k \to K$ be a finite field extension and $K = k(y,z)$ where y is separable over k. Then $L = k(ay+z)$ for all but finitely many a in k.

Proof: See Marcus (1977), p. 259 for a proof over the field of rationals.The general proof follows in an identical manner.

Finally we state

Lemma 3.4 Let $A = k[Y,Z]$ be a polynomial ring over a field k and $\wp_1, \wp_2$ be two distinct maximal ideals in A. Then $\wp_1 \cap k[aY+Z] \neq \wp_2 \cap k[aY+Z]$ for all but finitely many a in k.

Proof: Let L be the algebraic closure of k and for $i = 1,2$ let L_i be the fraction field of $A/\wp_i$. Since k L_i is finite we can fix two k-embeddings $L_i \to L$. For $i = 1,2$ let y_i, z_i denote the images of Y, Z, respectively, in L_i.

Let E be the set of all k-embeddings $\sigma : L_1 \to L$. Then E is finite. Write $S = \{a \text{ in } k : \textit{ for some } \sigma \text{ in } E\ a(\sigma(y_1) - y_2) = z_2 - \sigma(z_1)\}$. Clearly, S is finite.

Suppose a is in k that is not in S. We will see that $\wp_1 \cap k[aY+Z] \neq \wp_2 \cap k[aY+Z]$. For $i = 1,2$ since $\wp_i$ is the kernel of the map $k[Y,Z] \to L_i$, note that for σ in E, $(\sigma(y_1), \sigma(z_1)) \neq (y_2, z_2)$. Hence it follows that $\sigma(ay_1 + z_1) \neq ay_2 + z_2$ for all σ in E. So, $ay_1 + z_1$ and $ay_2 + z_2$ are not conjugates and therefore they have distinct minimal monic polynomials over k. For $i = 1,2$ let $f_i(T)$ be the minimal monic polynomial of $ay_i + z_i$.It is easy to see that $f_i(aY + Z)$ are distinct irreducible elements in $k[aY + Z]$ and are in $\wp_i \cap k[aY + Z]$. Hence $\wp_1 \cap k[aY + Z] = \wp_2 \cap k[aY + Z]$.

The following is the theorem to which all the lemmas of this section were heading.

Theorem 3.1 Let $A = k[X_1, \ldots, X_n]$ be a polynomial ring over a perfect field k and I be a reduced ideal of pure height $n-1$. Then, after a change of variables $\phi : A \to A$, $k[X_1, X_2]/I \cap k[X_1, X_2] \to A/I$ is integral and birational.

Proof: By Theorem 2.7, after a change of variables, $k \to k[X_1] \to \ldots \to k[X_1, \ldots, X_n]/I_n$ are all integral, $I_r = I \cap k[X_1, \ldots, X_r]$. Assume for the moment that $k[X_1, X_2]/I_2 \to k[X_1, X_2, X_3]/I_3$ is integral and birational. Hence $k[X_1, X_2, X_4, \ldots, X_n]/J \to k[X_1, \ldots, X_n]$ is integral and birational, where $J = I \cap k[X_1, X_2, X_4, \ldots, X_n]$. Hence, by induction, again after a change of variables $k[X_1, X_2]/I \cap k[X_1, X_2] \to k[X_1, \ldots, X_n]/I$ is integral and birational. So, it is enough to prove the theorem for $n = 3$.

We write $X_1 = X, X_2 = Y, X_3 = Z$.Also write $I = \wp_1, \ldots, \wp_r$,where $\wp_i$ are in $\mathrm{Spec}(k[X, Y, Z])$. Again by Suslin's theorem, we assume that $k[X, Y]/I \cap k[X, Y] \to k[X, Y, Z]/I$ is integral. We have $\wp_i \cap k[X, Y] = f_i k[X, Y]$ for some irreducible f_i in $k[X, Y]$. By Lemma 3.2, for large enough m that is not divisible by p, $g_i = f_i(X + Y^m, Y)$ is monic and $\partial g_i/\partial Y \neq 0$ for $i = 1, \ldots, r$. Hence after the change of variables $X \to X + Y^m$, $Y \to Y$ we assume that $\partial f_i/\partial Y \neq 0$.

For $i = 1, \ldots, r$, let K_i be the fraction field of $k[X, Y, Z]/\wp_i$ and x_i, y_i, z_i be the images of X, Y, Z in K_i. It follows that $k(X) \to K_i$ is integral and y_i is separable over $k(X)$. Since $k(X)$ is infinite, by lemmas (3.3) and (3.4) there is an a in $k(X)$ such that $K_i = k(X)(ay_i + z)$ for all $i = 1, \ldots, r$ and $k(X)[Y, Z] \cap wp_i$ are distinct. Hence it follows that for $k(X)[Y, Z]/I$ is generated by $aY + Z$ over $k(X)$. Write $a = c/d$ with c, d in $k[X]$ and $\lambda c + \beta d = 1$. Then $k(X)[Y, Z]/I$ is generated by $cY + dZ$ over $k(X)$.

Now $\alpha = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & d \\ 0 & \lambda & \beta \end{pmatrix}$ is invertible. After the change of variables X, Y, Z to $\alpha(X, Y, Z)^t$, we have that $k(X)[Y, Z]/I$ is generated by Y over $k(X)$. Hence $k[X, Y]/I \cap k[X, Y] \to k[X, Y, Z]/I$ is birational.

3.3 The Cowsik-Nori theorem

Theorem 3.2 **(Cowsik-Nori)** Let k be a field of positive characteristic p. Suppose I is an ideal of pure height $n-1$ in $R = k[X_1, X_2, \ldots, X_n]$. Then I is set theoretically generated by $n-1$ elements.

Proof: Let $K = k^{1/\infty}$. Let $R' = K[X_1, \ldots, X_n]$ and $I' = IR'$. If I' is set theoretically generated by $f_1, \ldots, f_{n-1}$ then for some large enough N, we have $f_1^{p^N}, \ldots, f_{n-1}^{p^N}$ are in I and generate I set theoretically. So, we can assume that k is perfect. We can also assume that I is a reduced ideal since we are interested in ideals only upto radicals.

By the theorem of the previous section, after a change of variables, we can assume that $k[X_1, X_2]/I \cap k[X_1, X_2] \to R/I$ is integral and birational.

Now write $A_0 = k[X_1, X_2]/I \cap k[X_1, X_2]$ and let us define C as $\{t \ in \ A_0 \ : tA \subseteq A_0\}$. C is called *the conductor* of A_0 into A, where $A = k[X_1, \ldots, X_n]/I$.

We claim that C is a height 1 ideal in A_0.Clearly the height of C in A_0 is atmost 1. Hence we need only to show that the height is non-zero. To do this we show that C contains a non-zero divisor of A_0. Then C cannot be contained in any minimal prime of A_0.

To show that C contains a non-zero divisor we observe that since the extension A_0 to A is integral, finite A is finitely generated as a module over A_0. Moreover, if $t_1, \ldots, t_k$ are a basis over A_0 then since the extension is birational we may assume that the t_i have denominators which are non-zero divisors in A_0. Thus if t denotes the product of these denominators then t is in C and is a non-zero divisor.

Hence the height of C in A_0 is 1.Thus $dim(A_0/C)$ is zero.This implies that $dim(A/C)$ is zero and hence that A/C is Artinian and hence $dim_k A$ is finite.

Let x_i be the image of X_i in A/C and let V_{ir} be the k-linear subspace of A/C generated by $\{x_i^{p^j} : j = r, r+1, \ldots\}$. There is an integer N such that $V_{ir} = V_{iN}$ for $i = 3, \ldots, n$ and $r = N, N+1, \ldots$. As x_i^N is in $V_{i(N+1)}$, there are $\lambda_{i1}, \lambda_{i2}, \ldots, \lambda_{it}$ in k and $c_3, \ldots, c_n$ in $k[X_1, X_2]$ such that

$f_i = X_i^{p^N} + \lambda_{i1} X_i^{p^{N+1}} + \cdots + \lambda_{it} X_i^{p^{N+t}} + c_i$ is in I for $i = 3, \ldots, n$.

For $i = 3, \ldots, n$ write $Y_i = X_i^{p^N}$, $R_0 = k[X_1, X_2, Y_3, \ldots, Y_n], I_0 = I \cap R_0$. Since $\sqrt{I} = \sqrt{I_0 R}$, we shall prove that I_0 is set theoretically generated by $n-1$ elements in R_0.

Since $(\partial f_i / \partial Y_j)_{i,j=3,\ldots n}$ is identity,we have by the only if part of Theorem 2.1 of Hartshorne,(1977) that $R_1 = R_0/(f_3, \ldots, f_n)$ is regular of dimension 2. Hence $I_0/(f_3, \ldots, f_n)$ is a height one ideal in a regular ring and hence is an invertible ideal.But invertible ideals in regular rings are locally principal ideals and since R_1 is of dimension $2, I_0/(f_3, \ldots, f_n)$ is a locally complete intersection ideal in R_1. Hence I_0 is a locally complete intersection ideal of height $n-1$ in R_0. Therefore, by Theorem 2.1, I_0 is set theoretically generated by $n-1$ elements.

3.4 Some concluding remarks

First let us point the following generalzation of the Cowsik-Nori theorem. From the result for affine curves Lyubeznik has shown that

Theorem 3.3 Every algebraic set V in $\mathbb{A}^n$ over k, a field of positive characteristic, consisting of irreducible components of positive dimensions can be defined by $n-1$ equations.

In contrast with this positive result in characteristic p we will point out that it is still unknown if every irreducible curve in affine three dimensional space over the complex numbers is even locally a set theoretic complete intersection. For example, it is unknown if the following curve

$x = t^6 + t^3$, $y = t^8$, $z = t^{10}$ is a set theoretic complete intersection locally at the origin.

In projective space the question seem to be harder. One may ask the following question

Question 3.3 *Can every geometrically connected algebraic subset of positive dimension in a projective n dimensional space over a field k be defined set theoretically by n-1 equations ?*

The answer is unknown even for smooth curves over algebraically closed fields.

For a detailed survey on this topic we refer to Lyubeznik (1989).

REFERENCES

1. Bass H. (1968), Algebraic K-theory, W.A.Benjamin Inc..

2. Cowsik R.C. and Nori M.V. (1978), Affine Curves in characteristic p are set theoretic complete intersections, Inventionae Mathematicae, 45, 111-114.

3. Evans and Griffiths (1985), Syzygies, London Math. Soc. Lecture notes series, Vol 106, Cambridge University, Press.

4. Hartshorne R. (1977), Algebraic Geometry, GTM 52,Springer-Verlag.

5. Kunz E. (1985) , Introduction to Commutative Algebra and Algebraic Geometry, Birkhauser.

6. Lam T.Y. (1978), Serre's conjecture, Lecture notes in Mathematics, 635 , Springer Verlag.

7. Luybeznik G. (1989), A survey of problems and results in the number of defining equations. in Commutative Algebra, eds. Hochster M., Huneke C. and Sally J.D., MSRI Publications.

8. Marcus M. (1977),Number Fields, Springer Verlag.

9. Matsumura H. (1989), Commutative Ring theory, Cambridge studies in Advanced Mathematics.

10. Plumstead A. (1979), The conjectures of Eisenbud and Evans, Ph.D thesis, University of Chicago, Illinois.