On Forster's Conjecture and Related Results

Rabeya Basu & Raja Sridharan
Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai - 400005

Introduction

The aim of this expository paper is to give a self contained account which is accessible to students of some of the work done by Indian mathematicians in the field of projective modules. This is one of the topics in which algebraists at the Tata Institute (T.I.F.R) have worked on a lot. Our aim is not to give a historical account of their contributions but to focus on the proof of some of the results which were proved following the proof of the "Quillen - Suslin" theorem. We have chosen to focus on results whose proofs can be easily understood by students. In order to keep the presentation totally elementary we do not even introduce the notion of a projective module. We use only results about projective modules given by "unimodular rows". We believe that a student who has read this paper will be able to understand and appreciate the many other contributions that mathematicians have made to the subject and read the recent work done in this area. We would like to emphasise that the self contained presentation we have made here has been possible because the subject matter evolved with time thanks to the efforts of many mathematicians some of whose work is not mentioned in this paper. We hope that the reader of this paper will delve into the many things we left out by looking at the references and MathSciNet for example. We now give a brief account of the contents of this paper.

Let $A = k[X_1, \ldots, X_n]$ be the polynomial ring in n variables over a field k and $\mathfrak{p} \subset A$ be a prime ideal. Then $\mathfrak{p}$ is finitely generated as A is Noetherian. We define $\mu(\mathfrak{p})$ to be the minimum number of elements needed to generate $\mathfrak{p}$. By Krull's dimension theorem $\mu(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{p})$. One can ask if $\mu(\mathfrak{p})$ is bounded. This is however false. There are classical examples of height 2 prime ideals $\mathfrak{p}$ in $\mathbb{C}[X_1, X_2, X_3]$ constructed by Macaulay (*cf.* [2]) which require an arbitrary large number of generators. In Macaulay's examples, the ring $\mathbb{C}[X_1, X_2, X_3]/\mathfrak{p}$ has a singularity at the origin.

However, if $A = k[X_1, \ldots, X_n]$ and $\mathfrak{p} \subset A$ is a prime ideal such that $A/\mathfrak{p}$ is regular, then Forster (*cf.* [9]) proved that $\mathfrak{p}$ is generated by $n+1$ elements. He conjectured that $\mathfrak{p}$ is generated by n elements. The conjecture of Forster was settled by Sathaye (*cf.* [34]) in the case where k is infinite and shortly afterwards by Mohan Kumar (*cf.* [23]) in general. One of the aims of this paper is to give a proof of their theorem namely;

Theorem 1. Let $A = k[X_1, \ldots, X_n]$ be the polynomial ring in n variables over a field k and $\mathfrak{p} \subset A$ be a prime ideal such that $A/\mathfrak{p}$ is regular. Then $\mathfrak{p}$ is generated by n elements.

We shall begin by considering some special cases of this theorem.

1. $A = k[X]$ is a PID and there is nothing to prove.

2. $A = k[X_1, \ldots, X_n]$. If $\mathfrak{m} \subset A$ is a maximal ideal, then $\mathfrak{m}$ is generated by n elements, *cf.* 3.4.1.

3. $A = k[X_1, X_2]$. If $\mathfrak{p} \subset A$ is a prime ideal, then $\mathrm{ht}(\mathfrak{p}) = 1$ or $\mathrm{ht}(\mathfrak{p}) = 2$. If $\mathrm{ht}(\mathfrak{p}) = 1$, $\mathfrak{p}$ is principal (*cf.* 1.10.5). If $\mathrm{ht}(\mathfrak{p}) = 2$, $\mathfrak{p}$ is maximal and hence is generated by 2 elements.

4. Let $A = k[X_1, X_2, X_3]$. To prove Forster's conjecture it is enough to prove that if $\mathfrak{p} \subset A$ is a prime ideal of height 2 such that $A/\mathfrak{p}$ is regular, then $\mathfrak{p}$ is generated by 3 elements. This was proved independently by Abhyankar and Murthy in [1] and [24], thus, settling the first non trivial case of Forster's conjecture.

Now, suppose $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ is such that $A/\mathfrak{p}$ is regular. Then it follows from a theorem of Forster-Swan (*cf.* [9], [41]) that $\mathfrak{p}/\mathfrak{p}^2$ is generated by n elements. Thus, Forster's conjecture will be true if the following question has an affirmative answer.

Question 1 : Suppose $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ is a prime ideal such that $\mathfrak{p}/\mathfrak{p}^2$ is generated by n elements. Is $\mathfrak{p}$ generated by n elements ?

Sathaye and Mohan Kumar settled Forster's conjecture by giving an affirmative answer to Question 1.

More generally Mohan Kumar proved the following :

Theorem 2. Let $A = k[X_1, \ldots, X_n]$ and $I \subset A$ be an ideal such that I/I^2 is generated by r elements, where $r \geq \dim(A/I) + 2$. Then I is generated by r elements.

Using Theorem 2, one can settle Question 1, and hence Forster's conjecture as follows.

If $\mathrm{ht}(\mathfrak{p}) = 1$, then $\mathfrak{p}$ is principal and there is nothing to prove. Assume $\mathrm{ht}(\mathfrak{p}) \geq 2$. Then $\dim(A/\mathfrak{p}) \leq n - 2$. Therefore, $n \geq \dim(A/\mathfrak{p}) + 2$. Now, since $\mathfrak{p}/\mathfrak{p}^2$ is generated by n elements, by Theorem 2, $\mathfrak{p}$ is generated by n elements.

The following theorem of Mandal (*cf.* [19]) is a generalisation of Theorem 2.

Theorem 3. Let A be a Noetherian domain, I an ideal of $A[X]$ containing a monic polynomial. Suppose that I/I^2 is generated by n elements, where $n \geq \dim(A[X]/I) + 2$. Then I is generated by n elements.

In this paper we give a proof of Theorem 3 (*cf.* 3.3.2) which easily implies Forster's conjecture (*cf.* 3.3.3).

We also apply Theorem 3, to prove the following addition principle (*cf.* 3.4.7).

Theorem 4. Let A be a Noetherian domain with $\dim(A) = d$. Let $n \geq \frac{d+3}{2}$. Let J_1 and J_2 be two ideals of A of height n such that $J_1 + J_2 = A$. Assume that J_1 and J_2 are both generated by n elements. Then $J_1 \cap J_2$ is generated by n elements.

The layout of this paper is as follows. In the first section we prove some basic results in commutative algebra. These results can be found in [21] and are included only to make the paper self contained and accesible to students. In Section 2, we prove variants of theorems of Quillen and Suslin which are used in the proof of Theorem 3. In Section 3, we prove Theorem 3 of S. Mandal (*cf.* 3.3.2) and use it to deduce Theorem 1 (Forster's Conjecture). In Section 4, we give another proof of Theorem 1. We end the section with a variant (due to Mandal) of Theorem 3.

1 Basic Commutative Algebra

In this section we review certain basic concepts which we need later. We give three methods of building new rings from old ones.

Throughout this paper by a ring we mean a commutative ring with an identity element.

1.1 The construction of new Rings from old ones

Polynomial Rings: Let A be a ring. The ring $A[X_1, \ldots, X_n]$ denotes the polynomial

ring in n variables $X_1, X_2, \ldots, X_n$ over A and consists of elements of the form,

$$f = \sum_{i=1}^{n} \lambda_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}, \;\; \lambda_{i_1 \ldots i_n} \in A, \;\; (i_1, \ldots, i_n) \in \mathbb{Z}_+^n.$$

An expression $X_1^{i_1} \ldots X_n^{i_n}$ is called a **monomial** and $i_1 + \cdots + i_n$ is called its **degree**. A typical element of this ring, called a **polynomial**, is a finite A-linear combination of monomials. A polynomial which is a finite A-linear combination of monomials each of degree d is called a **homogeneous polynomial of degree** d. Clearly, any polynomial is a finite sum of homogeneous polynomials. The **degree of a polynomial** is defined to be the maximum of the degrees of its homogeneous components.

Factor Rings: (**residue class rings**) If I is an ideal in a ring A, then the collection of cosets $\{x + I \,|\, x \in A\}$ form a ring under the induced operation from A. This ring is called the **factor ring** or the **residue class ring** of A modulo I and is denoted by A/I. The natural homomorphism $\phi : A \to A/I$, given by $x \mapsto x + I$, shows that there is a one-to-one correspondence between ideals of A/I and the ideals of A which contain I, given by $K \to \phi(K)$ and $J \to \phi^{-1}(J)$.

Definition 1.1.1 A proper ideal $\mathfrak{p}$ of a ring A is said to be a **prime** ideal if $ab \in \mathfrak{p}$ implies that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Definition 1.1.2 An ideal $\mathfrak{m}$ of A is said to be **maximal** if $\mathfrak{m}$ is not properly contained in any other ideal of A.

Remark 1.1.3 An ideal $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain. An ideal $\mathfrak{m}$ of A maximal if and only if $A/\mathfrak{m}$ is a field. In particular maximal ideals are prime. If $\mathfrak{p}$ is a prime ideal of a ring A and $I, J \subset A$ are ideals such that $IJ \subset \mathfrak{p}$, then either $I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$. For, if $I \nsubseteq \mathfrak{p}$ and $J \nsubseteq \mathfrak{p}$, then there exists $a \in I$, $a \notin \mathfrak{p}$ and $b \in J$, $b \notin \mathfrak{p}$, but $ab \in \mathfrak{p}$. This is a contradiction.

Definition 1.1.4 Let $\mathfrak{p}$ be a prime ideal of a ring A which contains an ideal I. Then $\mathfrak{p}$ is said to be **minimal over** I if $I \subset \mathfrak{p}' \subseteq \mathfrak{p}$ for any prime ideal $\mathfrak{p}'$ of A implies that $\mathfrak{p} = \mathfrak{p}'$. We call a prime ideal $\mathfrak{p}$ of A **minimal** if $\mathfrak{p}$ is minimal over the zero ideal.

Definition 1.1.5 The set of all prime ideals of a ring A is called the **Spectrum** of A and is denoted by $\mathrm{Spec}(A)$. Let I be an ideal of A and $V(I) = \{\mathfrak{p} \in \mathrm{Spec}(A) \,|\, I \subset \mathfrak{p}\}$. It can be shown that the collection $\{V(I) \,|\, I \subset A\}$ are closed subsets of $\mathrm{Spec}(A)$ with respect to a certain topology on $\mathrm{Spec}(A)$ called the **Zariski Topology**.

Notation. 1.1.6 The set of all maximal ideals of a ring A is a subset of $\mathrm{Spec}(A)$. It is denoted by $\mathrm{Max}(A)$.

Definition 1.1.7 A ring A is said to be a **local ring** if A has a unique maximal ideal. A ring A is said to be **semilocal** if A has only finitely many maximal ideals.

Definition 1.1.8 Let A be a ring. By a chain of prime ideals of A we mean a finite strictly increasing sequence of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of A. The integer n is called the length of the chain. The **Krull dimension** of A is the supremum of the lengths of chains of prime ideals of A. It is denoted by $\dim(A)$.

In this paper, by $\dim(A)$ we mean the Krull dimension of A.

Definition 1.1.9 Let A be a ring. If $\mathfrak{p} \in \mathrm{Spec}(A)$, then the **height** of $\mathfrak{p}$, denoted by $\mathrm{ht}(\mathfrak{p})$, is defined to be the supremum of the lengths of chains of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}$ which end at $\mathfrak{p}$. For any ideal $I \subseteq A$, we define $\mathrm{ht}(I) = \mathrm{Inf}\ \mathrm{ht}(\mathfrak{p})$, where infimum is taken over all prime ideals of A which are minimal over I. Note that $\mathrm{ht}(\mathfrak{p})$ could be infinite.

Definition 1.1.10 Let A be a ring. A a subset S of A is said to be **multiplicative closed** if $1 \in S$, $0 \notin S$ and $a, b \in S$ implies that $ab \in S$.

Example 1.1.11 Let A be a ring and $a \in A$ be such that $a^n \neq 0$ for every natural number n. Then $S = \{1, a, a^2, \dots\}$ is a multiplicative closed set.

Now we give a third method of constructing new rings from old ones *viz.*

Localization: This is a construction analogous to the construction of the field of rationals $\mathbb{Q}$ from the ring of integers $\mathbb{Z}$. For any ring A and a multiplicative closed subset S of A we define the **ring of fractions** $S^{-1}A$, consisting of elements of the form $\frac{a}{s}$, where $a \in A$ and $s \in S$, with addition and multiplication defined as follows:

$$(a/s) + (b/t) = (at + bs)/st; \quad (a/s)(b/t) = ab/st.$$

The notion of equality in $S^{-1}A$ is understood in the following way: $\frac{a}{s} = \frac{b}{t} \Leftrightarrow r(at - bs) = 0$ for some $r \in S$.

Some facts on localisation:

1. There is a ring homomorphism $f : A \to S^{-1}A$ defined by $f(x) = x/1$. In general f is not injective. Clearly, f is injective $\Leftrightarrow S$ does not contain any zero divisors.

2. Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is unit in B for all $s \in S$. Then there exists a ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$, where h is defined as, $h(a/s) = g(a)g(s)^{-1}$ and f is as in (1).

3. If $I \subset A$ is an ideal, then $S^{-1}I = \{\frac{i}{s} | i \in I, s \in S\}$ is an ideal of $S^{-1}A$. Any ideal of $S^{-1}A$ is of the form $S^{-1}I$, where $I \subset A$ is an ideal.

4. The prime ideals of $S^{-1}A$ are in bijective correspondence with the prime ideals of A which does not meet S. This correspondence is given by sending $\mathfrak{p} \in \mathrm{Spec}(A)$, which satisfies the property that $\mathfrak{p} \cap S = \Phi$, to $S^{-1}\mathfrak{p}$ and sending an ideal $\mathfrak{q} \in \mathrm{Spec}(S^{-1}A)$ to the prime ideal $f^{-1}(\mathfrak{q})$ of A (where f is as in (1)).

The surjectivity of this correspondence is easy to prove. We prove the injectivity by contradiction. Let $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Spec}(A)$ be such that $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $\mathfrak{p}_1 \cap S = \mathfrak{p}_2 \cap S = \Phi$. We show that $S^{-1}\mathfrak{p}_1 \neq S^{-1}\mathfrak{p}_2$. Without loss of generality we may assume that $\mathfrak{p}_1 \nsubseteq \mathfrak{p}_2$. Then we show that if $a \in \mathfrak{p}_1 - \mathfrak{p}_2$, $a/s \notin S^{-1}\mathfrak{p}_2$. Assume to the contrary let $\frac{a}{s} = \frac{b}{t}$ for some $b \in \mathfrak{p}_2$ and $t \in S$. This means there exists $r \in S$ such that $r(at - bs) = 0$. This implies $rat \in \mathfrak{p}_2$. Since $rt \notin \mathfrak{p}_2$, $a \in \mathfrak{p}_2$, a contradiction. Conversely, if $S^{-1}\mathfrak{p}_1 \neq S^{-1}\mathfrak{p}_2$, then obviously $\mathfrak{p}_1 \neq \mathfrak{p}_2$. In particular, if $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ and $\mathfrak{p}_1 \cap S \subset \mathfrak{p}_2 \cap S = \Phi$, then $S^{-1}\mathfrak{p}_1 \subsetneq S^{-1}\mathfrak{p}_2$. Thus, the above correspondence is inclusion preserving.

Let $A = \mathbb{Z}$, $S = \{1, 3, 3^2, \dots\}$, $I_1 = 2\mathbb{Z}$, $I_2 = 6\mathbb{Z}$ $I_3 = 18\mathbb{Z}$. Then $S^{-1}I_1 = S^{-1}I_2 = S^{-1}I_3$ even though $I_1 \cap S = I_2 \cap S = I_3 \cap S = \Phi$. Note however that I_2 and I_3 are not prime ideals.

5. If I, J are ideals of A, then $S^{-1}(I + J) = S^{-1}I + S^{-1}J$, $S^{-1}(IJ) = S^{-1}I.S^{-1}J$, $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$, and $S^{-1}I = S^{-1}A$ if and only if $I \cap S \neq \Phi$.

6. If A is a domain and $S = A - \{0\}$, then $S^{-1}A$ is the **quotient field** of A. For any prime ideal $\mathfrak{p}$ of A and $S = A - \mathfrak{p}$, $S^{-1}A$ is denoted by $A_{\mathfrak{p}}$ and is called the **localization of A at the prime ideal** $\mathfrak{p}$. The ring $A_{\mathfrak{p}}$ is a local ring with maximal ideal $S^{-1}\mathfrak{p}$.

Remark 1.1.12 From the above discussion it is clear that for a prime ideal $\mathfrak{p}$ of a ring A, $\mathrm{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$.

Definition 1.1.13 An element a of a ring A is said to be nilpotent if $a^n = 0$ for some $n > 0$.

Notation. 1.1.14 We write A_a for $S^{-1}A$, and I_a for $S^{-1}I$, where $S = \{a^n | n \geq 0\}$, where a is not nilpotent.

Localization of Modules: Let A be a ring, M an A-module and $S \subset A$ a multiplicative closed subset. Then we can define an $S^{-1}A$-module denoted by $S^{-1}M$. First, we define a relation $\equiv$ on $M \times S$ as follows:

$$(m, s) \equiv (m', s') \Leftrightarrow t(sm' - s'm) = 0 \text{ for some } t \in S.$$

It can easily be shown that $\equiv$ is an equivalence relation. The equivalence class of (m, s) is denoted by m/s and the set of equivalence classes is denoted by $S^{-1}M$. Now we define addition of two elements $m/s, m'/s' \in S^{-1}M$ by $m/s + m'/s' = (s'm + sm')/ss'$ and multiplication of a scalar $a/s \in S^{-1}A$ and $m'/s' \in S^{-1}M$ by $(a/s)(m'/s') = (am')/(ss')$. It is easy to check that under these operations $S^{-1}M$ is an $S^{-1}A$-module. Now if $\mathfrak{p}$ is a prime ideal and $S = A - \mathfrak{p}$, then the $A_{\mathfrak{p}}$-module $S^{-1}M$ is denoted by $M_{\mathfrak{p}}$ and it is called the localization of M at $\mathfrak{p}$.

Let M, N be two A-modules and $f \in \mathrm{Hom}_A(M, N)$. Define $S^{-1}f : S^{-1}M \to S^{-1}N$ by $(S^{-1}f)(m/s) = f(m)/s$. It can be easily seen that $S^{-1}f$ is well-defined and that it belongs to $\mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$.

Definition 1.1.15 Let A be a ring. A sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is of A-modules is said to be **exact** if $\mathrm{Ker}(g) = \mathrm{Im}(f)$, f is injective and g is surjective.

Proposition 1.1.16 *Let A be a ring and*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

an exact sequence of A-modules. Then

$$0 \longrightarrow S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'' \longrightarrow 0$$

is an exact sequence of $S^{-1}A$-modules.

Proposition 1.1.17 *Let A be a ring and M, N be two A-modules. Then*

$$S^{-1}(M \oplus N) \cong S^{-1}M \oplus S^{-1}N.$$

In particular, if $M = A^n = A \oplus A \oplus \cdots \oplus A$ (n times), then $S^{-1}M \cong (S^{-1}A)^n$.

1.2 Prime Avoidance Lemma

Lemma 1.2.1 (Prime Avoidance Lemma) *Let A be a ring and $I \subset A$ an ideal. Suppose $I \subset \cup_{i=1}^{n} \mathfrak{p}_i$, where $\mathfrak{p}_i \in \mathrm{Spec}(A)$. Then $I \subset \mathfrak{p}_i$ for some i, $1 \leq i \leq n$.*

Proof. To prove the lemma it suffices to show the following implication:

$$I \not\subseteq \mathfrak{p}_i, \forall i, 1 \leq i \leq n \Rightarrow I \not\subseteq \cup_{i=1}^{n} \mathfrak{p}_i.$$

We shall show this by induction on n. Clearly, this is true for $n = 1$. By induction, for each i, there exists $x_i \in I$ such that $x_i \notin \mathfrak{p}_j$ for $i \neq j$. If $x_i \notin \mathfrak{p}_i$, then we are through. If $x_i \in \mathfrak{p}_i$, then consider the element $y = \sum_{i=1}^{n} x_1 \dots x_{i-1} \hat{x}_i x_{i+1} \dots x_n$. Clearly, $y \notin \mathfrak{p}_i$, $1 \leq i \leq n$ and $y \in I$. This proves the lemma. □

Lemma 1.2.2 *Let A be a ring, $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathrm{Spec}(A)$ and $I = \langle a_1, \dots, a_n \rangle$ be an ideal of A such that $I \not\subseteq \mathfrak{p}_\mathfrak{i}$, $1 \leq i \leq r$. Then there exist $b_2, \dots, b_n \in A$ such that the element*

$$c = a_1 + a_2 b_2 + \cdots + a_n b_n \notin \cup_{i=1}^{r} \mathfrak{p}_\mathfrak{i}.$$

Proof. Without any loss of generality we may assume that $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for $i \neq j$. We prove the lemma by induction on r. Suppose by induction we have chosen $c_2, \dots, c_n \in A$ such that $d_1 = a_1 + c_2 a_2 + \cdots + c_n a_n \notin \cup_{i=1}^{r-1} \mathfrak{p}_i$. If $d_1 \notin \mathfrak{p}_r$, then we are through by taking $b_i = c_i$, $2 \leq i \leq r$. So we assume that $d_1 \in \mathfrak{p}_r$.

If $a_2, \dots, a_n$ all belong to $\mathfrak{p}_r$, then $d_1 - \sum_{i=2}^{n} a_i c_i = a_1 \in \mathfrak{p}_r$. But, this will imply that $I \subset \mathfrak{p}_r$. Thus, at least one of the $a_i \notin \mathfrak{p}_r$, $2 \leq i \leq n$. Without loss of generality we assume that $a_2 \notin \mathfrak{p}_r$. Since $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for $i \neq j$, we can choose $x \in \cap_{i=1}^{r-1} \mathfrak{p}_i$ such that $x \notin \mathfrak{p}_r$. Then $c = d_1 + x a_2 = a_1 + a_2 b_2 + \cdots + a_n b_n \notin \cup_{i=1}^{r} \mathfrak{p}_i$. This proves the lemma. □

1.3 Nakayama Lemma

Definition 1.3.1 The intersection of all the maximal ideals of a ring A is called the **Jacobson radical** of A. We denote it by $\mathrm{Jac}(A)$.

Remark 1.3.2 Let $x \in \mathrm{Jac}(A)$. Then for every $a \in A$, $1 - ax$ is a unit of A.

Lemma 1.3.3 (First version of Nakayama Lemma) *Let A be a ring, M a finitely generated A-module and I be an ideal of A such that $IM = M$. Then there exists an element $a \in I$ such that $(1 - a)M = 0$.*

Proof. Suppose $M \neq 0$ and $m_1, \dots, m_r$ is a generating set of M. Since $IM = M$, $m_i = \sum_{j=1}^{r} \lambda_{ij} m_j$, where $\lambda_{ij} \in I$. This implies that

$$\begin{pmatrix} 1 - \lambda_{11} & -\lambda_{12} & \cdots & -\lambda_{1r} \\ -\lambda_{21} & 1 - \lambda_{22} & \cdots & -\lambda_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ -\lambda_{r1} & -\lambda_{r2} & \cdots & 1 - \lambda_{rr} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ . \\ m_r \end{pmatrix} = 0.$$

Let

$$\alpha = \begin{pmatrix} 1 - \lambda_{11} & -\lambda_{12} & \cdots & -\lambda_{1r} \\ -\lambda_{21} & 1 - \lambda_{22} & \cdots & -\lambda_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ -\lambda_{r1} & -\lambda_{r2} & \cdots & 1 - \lambda_{rr} \end{pmatrix}.$$

Multiplying the above equation by $\mathrm{adj}(\alpha)$ we get $\det(\alpha)M = 0$. Since $\alpha = I_r$ modulo I, $\det(\alpha) = 1$ modulo I. So, there exists $a \in I$ such that $(1 - a)M = 0$. This proves the lemma. □

Lemma 1.3.4 (Second version of Nakayama Lemma) *Let A be a ring, M a finitely generated A-module and $I \subset A$ an ideal of A contained in Jacobson radical of A. Then $IM = M$ implies $M = 0$.*

Proof. By Lemma 1.3.3, there exists an element $a \in I$ such that $(1-a)M = 0$. Since I is contained in Jacobson radical of A, $(1-a)$ is a unit of A, so that $M = 0$. Hence the lemma. □

Corollary 1.3.5 *Let A be a ring, M a finitely generated A module, N an A-submodule of M. Let I be an ideal of A contained in Jacobson radical of A. If $M = N + IM$ then $M = N$.*

Proof. The proof follows by applying 1.3.5 to the module M/N. □

1.4 Noetherian Rings and Modules

In this section we prove some basic results on Noetherian rings and modules.

Let A be a ring and M be an A-module. Then the following statements are equivalent:

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

Definition 1.4.1 Let A be a ring. An A-module M is called **Noetherian** if it satisfies one of the above equivalent conditions.

Definition 1.4.2 A ring A is said to be Noetherian if A is Noetherian as an A-module.

Proposition 1.4.3 *Let A be 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.*

Proof. It is clear that if M is Noetherian then N and M/N are Noetherian. So, we prove the converse.

Assume N and M/N are Noetherian. Let K be any submodule of M. We show that K is finitely generated. Since $(N+K)/N$ is a submodule of M/N, it is finitely generated. Let bar denote the reduction modulo N. Let $\{\overline{k_1}, \ldots, \overline{k_n}\}$ be a generating set of $(N+K)/N$, where $k_i \in K$, $1 \leq i \leq n$. Let $N_1 = K \cap N$. Since N is Noetherian, N_1 is finitely generated. Let $q_1, \ldots, q_r$ generate N_1. Now, for $x \in K$, $\overline{x} = \sum_{i=1}^{n} \overline{\lambda_i k_i}$ for some $\lambda_i \in A$. Therefore, the element $x - \sum_{i=1}^{n} \lambda_i k_i$ belongs to $K \cap N$ and hence $x - \sum_{i=1}^{n} \lambda_i k_i = \sum_{j=1}^{r} \mu_j q_j$, $\mu_i \in A$. This implies that $K = \langle k_1, \ldots, k_n, q_1, \ldots, q_r \rangle$, proving the corollary. □

Corollary 1.4.4 *Let A be a ring and M_i, $1 \leq i \leq n$ be A-modules. Then the A-module $\oplus_{i=1}^{n} M_i$ is Noetherian $\Leftrightarrow$ each M_i is a Noetherian A-module.*

Corollary 1.4.5 *Any homomorphic image of a Noetherian ring is Noetherian.*

Corollary 1.4.6 *Let A be a Noetherian ring and M be a finitely generated A-module. Then M is Noetherian.*

Theorem 1.4.7 *Let A be a Noetherian ring. Then $A[X]$ is Noetherian.*

Proof. (See [33]) Let $I \subset A[X]$ be an ideal. We want to show that I is finitely generated. Let us choose $f_1(X) \in I$ of smallest degree. If $I = \langle f_1(X) \rangle$, we are through. If not, we choose $f_2(X) \in I$ such that $f_2(X) \notin \langle f_1(X) \rangle$ and is of smallest degree amongst all polynomials in I which are not in $\langle f_1(X) \rangle$. If $I = \langle f_1(X), f_2(X) \rangle$, then we are through as before. If not, we choose $f_3(X) \in I$ such that $f_3(X)$ has the smallest degree amongst all polynomials of I which are not in $\langle f_1(X), f_2(X) \rangle$. Proceeding in this way we can choose $f_i(X)$ for $i > 0$.

Let a_i be the leading coefficient of the polynomial $f_i(X)$. Since A is Noetherian, the increasing chain of ideals

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

terminates. Suppose $\langle a_1, \ldots, a_n \rangle = \langle a_1, \ldots, a_n, a_{n+1} \rangle = \cdots$ for some $n > 0$. We claim, $I = \langle f_1, \ldots, f_n \rangle$. Assume to the contrary that $f_{n+1}(X) = a_{n+1}X^m +$lower degree terms is not in the ideal generated by $f_1, \ldots, f_n$. Let $a_{n+1} = \sum_{i=1}^{n} \lambda_i a_i$. Let us define $g(X) = f_{n+1}(X) - \sum_{i=1}^{n} \lambda_i f_i(X) X^{\deg(f_{n+1}) - \deg(f_i)}$. Thus, $g(X)$ is a polynomial of degree less than that of $f_{n+1}(X)$ and is not in the ideal generated by $f_1, \ldots, f_n$. This contradicts the choice of $f_{n+1}(X)$. Hence the claim. This proves the theorem. □

Definition 1.4.8 Let A be a ring and I be an ideal of A. The set of all elements $\{x \in A \mid x^n \in I \text{ for some } n > 0\}$ is an ideal and is called the **radical of** I and is denoted by $\sqrt{I}$. The ideal $\sqrt{0}$ is called the **nil radical** of A and is denoted by $\text{nil}(A)$.

Remark 1.4.9 Let A be a Noetherian ring and $I \subset A$ be an ideal. Then, since $\sqrt{I}$ is finitely generated, there exists an integer $n > 0$ such that $(\sqrt{I})^n \subset I$.

Lemma 1.4.10 *Let A be a ring, S a multiplicative closed subset of A. If I is an ideal of A maximal with respect to the property that $I \cap S = \Phi$, then I is a prime ideal.*

Before we prove the lemma we make the following remark.

Remark 1.4.11 The ideal $\langle 0 \rangle$ satisfies the property that $\langle 0 \rangle \cap S = \Phi$. Therefore, by Zorn's lemma an ideal I with the above property exists.

Proof of Lemma 1.4.10. Suppose I is not prime. Then there exists $a, b \in A$ such that $a, b \notin I$ but $ab \in I$. By assumption, $\langle I, a \rangle \cap S \neq \Phi$ and $\langle I, b \rangle \cap S \neq \Phi$. Let us choose $x = \lambda + at \in \langle I, a \rangle \cap S$, where $\lambda \in I$, $t \in A$ and $y = \mu + br \in \langle I, b \rangle \cap S$, where $\mu \in I$, $r \in A$. Since $ab \in I$, the element $xy = (\lambda + at)(\mu + br) = \lambda\mu + \lambda br + \mu at + abrt \in I \cap S$. This is a contradiction. This proves the lemma. □

Lemma 1.4.12 *Let A be a ring and $I \subset A$ be an ideal. Then $\sqrt{I} = \cap \mathfrak{p}$, where intersection is taken over all prime ideals of A containing I.*

Proof. We prove this when $I = 0$, the general case being similar. Let $a \in \sqrt{0}$. Then $a^n = 0$ for some $n > 0$. Hence $a^n \in \mathfrak{p}$ for all $\mathfrak{p} \in \text{Spec}(A)$, so that $a \in \mathfrak{p}$ for all $\mathfrak{p} \in \text{Spec}(A)$.

Conversely, let $a \in \cap \mathfrak{p}$ for all $\mathfrak{p} \in \text{Spec } A$. Suppose a is not nilpotent. Let $S = \{1, a, a^2, \ldots\}$. Then S is a multiplicative closed subset of A and hence by Lemma 1.4.10, there exists a prime ideal $\mathfrak{q}$ of A such that $\mathfrak{q} \cap S = \Phi$. But $a \in \mathfrak{q} \cap S$ showing that $\mathfrak{q} \cap S \neq \Phi$, a contradiction. Hence the lemma follows. □

Proposition 1.4.13 *Let A be Noetherian ring, $I \subset A$ an ideal. Then $\sqrt{I}$ is a finite intersection of prime ideals of A.*

Proof. Suppose the proposition is false. Let **S** be the family of ideals I of A such that $\sqrt{I}$ is not a finite intersection of prime ideals.

Since A is Noetherian, S has a maximal element, say I_0. If I_0 is a prime ideal, then $I_0 = \sqrt{I_0}$ and hence the proposition follows. So we assume that I_0 is not prime. So, there exist $a, b \in A$ such that $a, b \notin I_0$ but $ab \in I_0$. Since $I_0 \subsetneq \langle I_0, a\rangle$ and $I_0 \subsetneq \langle I_0, b\rangle$, $\sqrt{\langle I_0, a\rangle}$ and $\sqrt{\langle I_0, b\rangle}$ are finite intersections of prime ideals.

We claim, $\sqrt{I_0} = \sqrt{\langle I_0, a\rangle} \cap \sqrt{\langle I_0, b\rangle}$. It would then follow that $\sqrt{I_0}$ is also a finite intersection of prime ideals. This contradicts the assumption on I_0.

Proof of the claim : Clearly, $\sqrt{I_0} \subset \sqrt{\langle I_0, a\rangle} \cap \sqrt{\langle I_0, b\rangle}$. To prove the other part let $x \in \sqrt{\langle I_0, a\rangle} \cap \sqrt{\langle I_0, b\rangle}$. Then $x^n \in \langle I_0, a\rangle$, $x^m \in \langle I_0, b\rangle$ for some $m, n > 0$. Since $ab \in I_0$, $x^{m+n} \in I_0$. This implies that $x \in \sqrt{I_0}$. Hence the claim. This completes the proof. □

Proposition 1.4.14 *Let A be a Noetherian ring, $I \subset A$ an ideal of A. If $\sqrt{I} = \cap_{i=1}^{n} \mathfrak{p}_i$ and n is the least integer with respect to this property, then the $\mathfrak{p}_i$'s are exactly those prime ideals of A which are minimal over I.*

Proof. Let n be the least integer with respect to the property that $\sqrt{I} = \cap_{i=1}^{n} \mathfrak{p}_i$. If for some i, $\mathfrak{p}_i$ is not minimal over I, then there exists a prime ideal $\mathfrak{q}$ of A such that $I \subset \mathfrak{q} \subsetneq \mathfrak{p}_i$. Taking radicals it follows that $\cap_{i=1}^{n} \mathfrak{p}_i \subset \mathfrak{q} \subset \mathfrak{p}_i$. Hence $\mathfrak{p}_r \subset \mathfrak{q} \subsetneq \mathfrak{p}_i$ for some r. This contradicts the minimality of n. Hence the $\mathfrak{p}_i$'s are minimal over I.

Conversely, let $\mathfrak{p} \in \mathrm{Spec}(A)$ be minimal over I. Then $I \subset \mathfrak{p}$ and taking radicals it follows that $I \subset \mathfrak{p}_j \subset \mathfrak{p}$ for some j, $1 \leq j \leq n$. Since $\mathfrak{p}$ is minimal over I, $\mathfrak{p} = \mathfrak{p}_j$. This proves the proposition. □

Corollary 1.4.15 For any ideal I of a Noetherian ring A there are only finitely many prime ideals of A minimal over I.

1.5 Artinian Rings and Modules

In this section we prove basic results about Artinian rings and modules.

Definition 1.5.1 Let A be a ring. An A-module M is said to be Artinian if one of the following equivalent conditions holds.

1. Any non empty collection of submodules of M has a minimal element.
2. Any descending chain of submodules of M is stationary.

Definition 1.5.2 A ring A is said to **Artinian** if it is Artinian as an A-module.

Some properties of Artinian Modules:

1. If M is an A-module and N is a submodule of M, then M is Artinian if and only if N and M/N are Artinian.
2. For A-modules $M_1, \ldots, M_n$, $\oplus_{i=1}^{n} M_i$ is Artinian if and only if each M_i is Artinian.
3. If A is a Artinian ring, then any finitely generated A-module is Artinian.

Proposition 1.5.3 *An Artinian domain is a field.*

Proof. Let A be an Artinian domain and $x \in A$ be a non zero element. Since A is Artinian, the decreasing chain of ideals $\langle x\rangle \supset \langle x^2\rangle \supset \cdots$, terminates *i.e.* there exists

an integer $n > 0$ such that $\langle x^n \rangle = \langle x^{n+1} \rangle \cdots$. Therefore, $x^n \in \langle x^{n+1} \rangle$ and hence there exists $y \in A$ such that $x^n = x^{n+1}y$. Since A is a domain, and $x \neq 0$, it follows that $xy = 1$, showing that x is a unit of A. Hence the proposition follows. □

Corollary 1.5.4 *In an Artinian ring every prime ideal is maximal.*

Proof. Let A be an Artinian ring, $\mathfrak{p}$ a prime ideal of A. Then $A/\mathfrak{p}$ is an Artinian domain and hence is a field. Therefore, $\mathfrak{p}$ is a maximal ideal of A. □

Proposition 1.5.5 *An Artinian ring is semilocal.*

Proof. Let A be an Artinian ring. Suppose to the contrary $\{\mathfrak{m}_i\}_{i\in\mathbb{N}}$, is an infinite set of distinct maximal ideals of A. Since A is a Artinian ring the decreasing chain of ideals

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \cdots$$

will stop, so that there exists a $n > 0$ such that $\cap_{i=1}^{n}\mathfrak{m}_i = \cap_{i=1}^{n+1}\mathfrak{m}_i$. This implies that $\cap_{i=1}^{n}\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$. Hence $\mathfrak{m}_k \subset \mathfrak{m}_{n+1}$ for some $k \leq n$. But $\mathfrak{m}_i$'s are maximal, so that $\mathfrak{m}_k = \mathfrak{m}_{n+1}$. This contradicts our assumption that the $\mathfrak{m}_i$'s are distinct. Therefore, A has only finitely many maximal ideals. This completes the proof. □

Proposition 1.5.6 *In an Artinian ring the nil radical is nilpotent.*

Proof. Let A be a Artinian ring and $\mathfrak{N}$ be the nil radical of A. Consider the decreasing chain $\mathfrak{N} \supset \mathfrak{N}^2 \supset \cdots$. Since A is Artinian, there exists an integer $k > 0$ such that $\mathfrak{N}^k = \mathfrak{N}^{k+1} = \cdots = \mathfrak{a}$ (say). If $\mathfrak{a} = \{0\}$, we are done. Assume that $\mathfrak{a} \neq \{0\}$. Let

$$S = \{\mathfrak{b} | \mathfrak{b} \text{ is an ideal of } A, \mathfrak{b}\mathfrak{a} \neq 0\}$$

Note that $\mathfrak{a}\mathfrak{a} = \mathfrak{N}^k\mathfrak{N}^k = \mathfrak{N}^{2k} \neq 0$. Hence $\mathfrak{a} \in S$, so that S is non empty and since A is Artinian, S has a minimal element, say I. Thus, there exists $x \in I$ such that $x\mathfrak{a} \neq \{0\}$. Now $\langle x \rangle \subset I$ and therefore, by the minimality of I it follows that $\langle x \rangle = I$. But $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$. Since $x\mathfrak{a} \subset I = \langle x \rangle$, by the minimality of I it follows that $x\mathfrak{a} = \langle x \rangle$, so that $x = xy$ for some $y \in \mathfrak{a}$. Therefore, $x = xy = xy^2 = \cdots = xy^n = \cdots$. Now, $y \in \mathfrak{a}$ implies that y is nilpotent. Therefore, $y^n = 0$ for some n. This implies $x = 0$. (Alternatively, $(1 - y)x = 0$. But, $1 - y$ is unit and hence $x = 0$). Now, since $x = 0$, $I = \{0\}$. This is a contradiction. Hence the proposition follows. □

Proposition 1.5.7 *For a vector space V over a field k the following are equivalent.*

1. *V is a finite dimensional vector space over k.*
2. *V is a Noetherian k-module.*
3. *V is an Artinian k-module.*

Proof. (1) ⇒ (2): Since V is a finite dimensional vector space over k, every subspace of V is finite dimensional. This implies that V is a Noetherian k-module.

(2) ⇒ (1): We assume to the contrary that V is Noetherian k-module but not finite dimensional. Then we can find an infinite set of linearly independent vectors $\{e_1, e_2, \ldots, e_n, \ldots\}$ of V. This gives a strictly increasing chain of subspaces of V *viz.* $ke_1 \subset ke_1 + ke_2 \subset ke_1 + ke_2 + ke_3 \subset \cdots$. This contradicts the fact that V is Noetherian. Hence V is finite dimensional.

(1) ⇒ (3): Suppose (1) is true but V is not Artinian. Let $W = W_0 \supset W_1 \supset W_2 \supset \cdots$ be a strictly decreasing chain of subspaces of V. Then $\dim(W_0) > \dim(W_1) > \cdots$. But, since V is finite dimensional, the chain stops, showing that V is Artinian.

(3) $\Rightarrow$ (1): If V is not finite dimensional, as before we can choose a linearly independent set of vectors $\{e_1, e_2, \ldots, e_n, \ldots\}$ of V. Then $\sum_{i=1}^{\infty} ke_i \supset \sum_{i=2}^{\infty} ke_i \supset \cdots$ is a strictly decreasing chain of subspaces of V, contradicting the fact that V is an Artinian k-module. Hence V is finite dimensional. $\square$

Lemma 1.5.8 *Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = \langle 0 \rangle$ be a filtration of A-modules. Then M is a Noetherian (Artinian) A-module if and only if each M_i/M_{i+1} is a Noetherian (Artinian) A-module for $0 \leq i \leq n-1$.*

Lemma 1.5.9 *Let A be a ring and $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ be maximal ideals of A (which are not necessarily distinct). Let M be an A-module. Suppose $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n M = \langle 0 \rangle$. Then M is a Noetherian A-module if and only if M is an Artinian A-module.*

Proof. Let M be a Noetherian A-module. We consider the filtration $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = \langle 0 \rangle$, where $M_i = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_i M$. Since M is Noetherian A-module M_i/M_{i+1} is a Noetherian A-module for every i. Hence M_i/M_{i+1} is a Noetherian $A/\mathfrak{m}_i$-module for every i. Using 1.5.7, it follows that M_i/M_{i+1} is an Artinian $A/\mathfrak{m}_i$-module for every i. Hence M_i/M_{i+1} is an Artinian A-module for all i. Therefore, M is an Artinian A-module. The other assertion can proved similarly. $\square$

Corollary 1.5.10 A ring A is Artinian if and only if it is Noetherian and $\dim(A) = 0$.

Proof. Suppose A is Artinian. By 1.5.4, every prime ideal of A is maximal. By 1.5.5, A has only finitely many maximal ideals. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ be the finitely many prime (maximal) ideals of A. Then by 1.5.6, there exists $n > 0$ such that $(\cap_{i=1}^{k} \mathfrak{m}_i)^n = \sqrt{0}^n = \langle 0 \rangle$. Now, by 1.5.9, A is Noetherian. The converse can be proved similarly. $\square$

Definition 1.5.11 Let A be a ring. An A-module M is said to be simple if $M \neq 0$ and the only submodules of M are $\langle 0 \rangle$ and M.

Remark 1.5.12 *A simple A-module is both Artinian and Noetherian.*

Remark 1.5.13 Let A be a ring and M be a simple A-module. Let m be a non zero element of M. We consider the A-linear map $g : A \to M$ which sends 1 to m. Since $\mathrm{Im}(g) \neq 0$ and M is simple, g is surjective. Since $A/\ker(g) \cong M$ is simple, $\ker(g)$ is a maximal ideal of A. Thus, a simple A-module is isomorphic to $A/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal of A.

Definition 1.5.14 Let A be a ring and M be an A-module. Then M is said to be of **finite length** if there exists a filtration $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = \langle 0 \rangle$, where M_i/M_{i+1} is a simple A-module for each i. In this case n is called the **length** of the filtration. Such a filtration is called a **Jordan Hölder series** or **composition series** of length n. An A-module M is said to be of finite length if it has a Jordan Hölder series.

Theorem 1.5.15 *Let A be a ring and M be an A-module. Suppose M has a composition series of length n. Then every composition series of M has length n.*

Proof. Let $l_A(M)$ = least length of a Jordan Hölder series of M.(Convention: $l_A(M) = \infty \Leftrightarrow M$ has no Jordan Hölder series.) We split the proof into two parts.

Step 1. We claim that if N is a A-submodule of M then $l_A(N) \leq l_A(M)$. Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ be a composition series of M of minimum length. Let $N_i = N \cap M_i$. Since $\frac{N_{i-1}}{N_i} \subset \frac{M_{i-1}}{M_i}$ and $\frac{M_{i-1}}{M_i}$ is a simple module, either $\frac{N_{i-1}}{N_i} = \frac{M_{i-1}}{M_i}$ or

$N_{i-1} = N_i$. Thus, removing repeated terms we obtain a composition series of N and we get $l_A(N) \leq l_A(M)$. Now, if $N \subsetneq M$, we show that the above inequality is actually strict. For, if $l_A(N) = l_A(M)$, then $\frac{N_{i-1}}{N_i} = \frac{M_{i-1}}{M_i}$ for all $i = 1, 2, \ldots, n$. Since $M_n = \langle 0 \rangle = N_n$, $M_{n-1} = N_{n-1}$ and hence $M_{n-2} = N_{n-2}$ and so on. Thus $M = N$, this is a contradiction. this proves the claim.

Step 2. Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r = \langle 0 \rangle$ be a chain of submodules of M of length r. Then from Step 1, it follows that $l_A(M) > l_A(M_1) > \cdots > l_A(M_r) = 0$. This implies that $l_A(M) \geq r$.

Step 3. It follows from Step 2, that for any composition series of M of length r, $r \leq l_A(M)$. Therefore, by the definition of $l_A(M)$, $l_A(M) = r$. Hence all composition series of M have the same length. □

Proposition 1.5.16 *An A-module M has a Jordan Hölder series if and only if M is both Noetherian and Artinian as an A-module.*

Proof. Let $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = \langle 0 \rangle$ be a Jordan Hölder series of M. Since M_i/M_{i+1} is simple A module it follows from 1.5.12 that M_i/M_{i+1} is both an Artinian and Noetherian A-module for $i = 1, \ldots, n$. So by 1.5.8, M is both Artinian and Noetherian.

Conversely, suppose M is both Artinian and Noetherian. Since A is Noetherian, M contains a maximal proper submodule, say M_1. But, since M_1 is also Noetherian it has a maximal proper submodule, say M_2. Iterating this process we get a descending chain $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq M_3 \cdots$ with M_i/M_{i+1} simple. Since M is an Artinian A-module this chain stops. Therefore, $M_n = \langle 0 \rangle$ for some $n > 0$. Hence M has a Jordan Hölder series. □

Proposition 1.5.17 *Let A be a ring, M an A-module and $N \subset M$ a submodule. Then M has finite length if and only if N and M/N have finite length and in this case $l_A(M) = l_A(N) + l_A(M/N)$.*

Proof. The first part of the proof follows from 1.5.16. The second part also follows easily. □

1.6 Krull's Principal Ideal Theorem and its Generalisation

In this section we prove Krull's Principal Ideal theorem.

Theorem 1.6.1 (Krull's Principal Ideal Theorem). *Let A be a Noetherian ring, $\mathfrak{p}$ a prime ideal of A such that $\mathfrak{p}$ is minimal over the ideal $\langle a \rangle$ for some $a \in A$. Then* $\mathrm{ht}(\mathfrak{p}) \leq 1$.

This theorem is an easy consequence of the next theorem.

Note 1.6.2 This theorem fails due to the deficiency of Noetherian property of the ring. For, consider the ring $A = \mathbb{Z}[2X, 2X^2, 2X^3, \ldots]$. Then A is a two dimentional ring as $A[1/2] = A[1/2, X]$ which is not Noetherian. The maximal ideal $\langle 2, 2X, 2X^2, \ldots \rangle$ is minimal over the principal ideal $\langle 2 \rangle$ and hence is of height 2. But it is not finitely generated.

Theorem 1.6.3 *Let $(A, \mathfrak{m})$ be a Noetherian local domain. Suppose $\mathfrak{m}$ is minimal over the ideal $\langle a \rangle$, where $a \neq 0$. Then* $\mathrm{ht}(\mathfrak{m}) = 1$, *i.e.* $\mathrm{Spec}(A) = \{\langle 0 \rangle, \mathfrak{m}\}$.

Motivation. If one knows that $\mathrm{Spec}(A) = \{\langle 0\rangle, \mathfrak{m}\}$, it would follow that for any non zero element $b \in \mathfrak{m}$, $\mathfrak{m}$ is the only prime ideal minimal over bA. It would hence follow that $\sqrt{bA} = \mathfrak{m}$. This implies that $\mathfrak{m}^n \subset bA$ for some natural number $n > 0$ and hence for any non zero element $a \in \mathfrak{m}$, $a^n \in bA$. This motivates the following assertion. Let $(A, \mathfrak{m})$ be a Noetherian local domain such that $\mathfrak{m}$ minimal over $\langle a\rangle$, where $a \neq 0$. Let $b \in \mathfrak{m}$ be a non zero element. Then for sufficiently large n, $\langle a^n, b\rangle A = \langle a^{n+1}, b\rangle A = bA$. We prove this assertion in 1.6.8 & 1.6.9 and deduce 1.6.3 as a consequence.

Lemma 1.6.4 *Let A be a ring and $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of A-modules. Suppose $I \subset A$ is an ideal. Then the following sequence of A-modules is exact:*

$$0 \longrightarrow \frac{M'}{IM \cap M'} \longrightarrow \frac{M}{IM} \longrightarrow \frac{M''}{IM''} \longrightarrow 0$$

Proof. By hypothesis, $M/M' \cong M''$. Therefore, using the fact $IM'' \cong I(M/M') \cong (IM + M')/M'$, we get

$$\frac{M/IM}{M'/IM \cap M'} \cong \frac{M/IM}{M' + IM/IM} \cong \frac{M}{M' + IM} \cong \frac{M/M'}{(M' + IM)/M'} \cong \frac{M''}{IM''}.$$

Hence the lemma follows. □

Note 1.6.5 Let A be a ring and M be a torsion free A-module. Let $c \in A$, $c \neq 0$ and N be a A-submodule of M. Then $M/N \simeq cM/cN$. The map sending $\overline{m}$ to $\overline{cm}$, is an isomorphism. Indeed, if $cm \in cN$, then $cm = cn$, where $n \in N \Rightarrow c(m - n) = 0 \Rightarrow m - n = 0$, as M is a torsion free A-module. This implies that $m = n \in N \Rightarrow \lambda_c$ is injective.

We state the following well known lemma, *cf.* [32].

Lemma 1.6.6 (Artin-Rees Lemma) *Let I, J be two ideals of a Noetherian ring A. Then there exists a natural number m such that for all $n \geq m$, $(I^{n+1} \cap J) = I(I^n \cap J)$.*

It is obvious that $I(I^n \cap J) \subset I^{n+1} \cap J$. The other inclusion is non trivial. We prove the following special case.

Lemma 1.6.7 *Let A be a Noetherian ring and $a, b \in A$. Then there exists a natural number m such that for all $n \geq m$, $a^{n+1}A \cap bA = a(a^nA \cap bA)$.*

Proof. Let $J_i = \{\mu \in A \,|\, \mu a^i \in bA\}$. Then $J_1 \subset J_2 \subset \cdots$ is an increasing chain of ideals of A. Since A is Noetherian, there exists an integer $m > 0$ such that $J_m = J_{m+1} = \cdots$. Let $n \geq m$ and $c \in a^{n+1}A \cap bA$. Then $c = \mu a^{n+1} \in bA$. This implies that $\mu \in J_{n+1} \Rightarrow \mu \in J_n \Rightarrow \mu a^n \in bA$. Therefore, $c = \mu a^{n+1} = a(\mu a^n) \in a(a^nA \cap bA)$. Hence the lemma follows. □

Theorem 1.6.8 *Let $(A, \mathfrak{m})$ be a Noetherian local domain, $\mathfrak{m}$ be minimal over the ideal $\langle a\rangle$, for some non zero element $a \in A$. Let $b \in \mathfrak{m}$ be a non zero element. Then for $n \geq 1$, the A-module $A/\langle a^n, b\rangle A$ has finite length and for sufficiently large n*

$$l_A\left(A/\langle a^n, b\rangle A\right) = l_A\left(A/\langle a^{n+1}, b\rangle A\right). \tag{1}$$

Proof. We first prove that $l_A(A/a^nA) < \infty$ for $n \geq 1$.

Since A is Noetherian, $A/\langle a^n\rangle$ is Noetherian. If $\mathfrak{p}$ is a prime ideal of A containing a^n, then $a \in \mathfrak{p} \subset \mathfrak{m}$. Since $\mathfrak{m}$ is minimal over $\langle a\rangle$, $\mathfrak{p} = \mathfrak{m}$. Thus $\mathrm{Spec}((A/a^nA)) = \{\overline{\mathfrak{m}}\}$. This

implies that every prime ideal of A/a^nA is maximal. Hence A/a^nA is both Artinian and Noetherian (see 1.5.10). Therefore, $l_A(A/a^nA) < \infty$.

Now we proceed to prove (1). Applying Lemma 1.6.4 to the exact sequence of A-modules

$$0 \longrightarrow bA \longrightarrow A \longrightarrow A/bA \longrightarrow 0$$

we get exact sequences

$$0 \longrightarrow \frac{bA}{bA \cap a^nA} \longrightarrow \frac{A}{a^nA} \longrightarrow \frac{A}{\langle a^n, b\rangle A} \longrightarrow 0$$

and

$$0 \longrightarrow \frac{bA}{bA \cap a^{n+1}A} \longrightarrow \frac{A}{a^{n+1}A} \longrightarrow \frac{A}{\langle a^{n+1}, b\rangle A} \longrightarrow 0.$$

Since $l_A\left(A/a^nA\right)$ is finite for all $n \geq 1$, we have

$$l_A\left(\frac{A}{a^nA}\right) = l_A\left(\frac{bA}{a^nA \cap bA}\right) + l_A\left(\frac{A}{\langle a^n, b\rangle A}\right)$$

and

$$l_A\left(\frac{A}{a^{n+1}A}\right) = l_A\left(\frac{bA}{a^{n+1}A \cap bA}\right) + l_A\left(\frac{A}{\langle a^{n+1}, b\rangle A}\right).$$

Therefore, we have

$$l_A\left(\frac{A}{\langle a^{n+1}, b\rangle A}\right) - l_A\left(\frac{A}{\langle a^n, b\rangle A}\right) = l_A\left(\frac{A}{a^{n+1}A}\right) - l_A\left(\frac{A}{a^nA}\right)$$

$$-l_A\left(\frac{bA}{a^{n+1}A \cap bA}\right) + l_A\left(\frac{bA}{a^nA \cap bA}\right) \tag{2}$$

In order to prove that the difference is zero for sufficiently large n, we consider the exact sequence

$$0 \longrightarrow \frac{a^nA}{a^{n+1}A} \longrightarrow \frac{A}{a^{n+1}A} \longrightarrow \frac{A}{a^nA} \longrightarrow 0$$

which shows that

$$l_A\left(\frac{A}{a^{n+1}A}\right) - l_A\left(\frac{A}{a^nA}\right) = l_A\left(\frac{a^nA}{a^{n+1}A}\right) = l_A\left(\frac{A}{aA}\right) \text{ by 1.6.5} \tag{3}$$

Also, we have the following exact sequence

$$0 \longrightarrow \frac{abA}{bA \cap a^{n+1}A} \longrightarrow \frac{bA}{bA \cap a^{n+1}A} \longrightarrow \frac{bA}{abA} \longrightarrow 0. \tag{4}$$

Using Lemma 1.6.7, we choose natural number m such that for all $n \geq m$,

$$a^{n+1}A \cap bA = a(a^nA \cap bA). \tag{5}$$

Therefore, for all $n \geq m$ we have,

$l_A\left(\frac{A}{\langle a^{n+1}, b\rangle A}\right) - l_A\left(\frac{A}{\langle a^n, b\rangle A}\right)$

$= l_A\left(\frac{A}{aA}\right) - \left[l_A\left(\frac{bA}{bA\cap a^{n+1}A}\right) - l_A\left(\frac{abA}{a(bA\cap a^nA)}\right)\right]$ by (2), (3) and 1.6.5

$= l_A\left(\frac{A}{aA}\right) - [l_A\left(\frac{bA}{bA\cap a^{n+1}A}\right) - l_A\left(\frac{abA}{bA\cap a^{n+1}A}\right)]$ by (5)

$= l_A\left(\frac{A}{aA}\right) - l_A\left(\frac{bA}{abA}\right)$ by (4)

$= l_A\left(\frac{A}{aA}\right) - l_A\left(\frac{A}{aA}\right)$ by 1.6.5

$= 0$

This proves the theorem. □

Corollary 1.6.9 *Let $(A, \mathfrak{m})$ be a Noetherian local domain such that $\mathfrak{m}$ is minimal over the ideal $\langle a\rangle$, for some non zero $a \in A$. If $b \in \mathfrak{m}$, $\neq 0$ then for sufficiently large n, $\langle a^n, b\rangle A = \langle a^{n+1}, b\rangle A = bA$.*

Proof. The sequence $0 \longrightarrow \frac{\langle a^n,b\rangle A}{\langle a^{n+1},b\rangle A} \longrightarrow \frac{A}{\langle a^{n+1},b\rangle A} \longrightarrow \frac{A}{\langle a^n,b\rangle A} \longrightarrow 0$ is exact and hence by 1.6.8, $l_A\left(\frac{\langle a^n,b\rangle A}{\langle a^{n+1},b\rangle A}\right) = 0$ for sufficiently large n. That is, for sufficiently large n, we get $\langle a^n, b\rangle A = \langle a^{n+1}, b\rangle A$. Therefore, we can write $a^n = \mu a^{n+1} + \lambda b$. Hence $a^n(1 - \mu a) = \lambda b$. Since $a \in \mathfrak{m}$, $1 - \mu a$ is unit. This implies that $a^n \in bA$. Hence $\langle a^n, b\rangle A = bA$.

(Alternatively, in the local ring A/bA, $\langle \overline{a^n}\rangle = \langle \overline{a^{n+1}}\rangle$. By Nakayama, it follows that $\langle \overline{a^n}\rangle = 0$. This implies that $a^n \in bA$.) □

Proof of Theorem 1.6.3. Since $\mathfrak{m}$ is minimal over $\langle a\rangle$, $\sqrt{aA} = \mathfrak{m}$. Let $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{p} \neq 0$. We show that $\mathfrak{p} = \mathfrak{m}$. Let $b \in \mathfrak{p}$ be non zero and n be a positive integer such that $a^n \in bA$. Since $\mathfrak{m}^k \subset aA$ for some $k \geq 0$, we get $\mathfrak{m}^{kn} \subset a^nA \subset bA \subset \mathfrak{p}$. This implies that $\mathfrak{m} \subset \mathfrak{p} \subset \mathfrak{m}$. Hence $\mathfrak{p} = \mathfrak{m}$. □

Proof of Theorem 1.6.1. If $a = 0$, then $\mathfrak{p}$ is minimal prime ideal of A and hence $\mathrm{ht}(\mathfrak{p}) = 0$. Assume $a \neq 0$. Suppose to the contrary that $\mathrm{ht}(\mathfrak{p}) \geq 2$. Let $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2$ be a chain of prime ideals of A. Going modulo $\mathfrak{p}_2$ we may assume A is a domain. Localising at $\mathfrak{p}$ we may assume that A is a local domain. Applying 1.6.3, we get a contradiction. This proves the lemma. □

Theorem 1.6.10 (Krull's dimension Theorem). *Let A be a Noetherian ring. Suppose $\mathfrak{p} \in \mathrm{Spec}(A)$ be such that $\mathfrak{p}$ is minimal over $\langle a_1, \ldots, a_n\rangle$. Then $\mathrm{ht}(\mathfrak{p}) \leq n$.*

Proof. We prove the theorem by induction on n. The case $n = 1$ follows from 1.6.1. We assume the result is true for all positive integers $k < n$. Assume to the contrary suppose that $\mathrm{ht}(\mathfrak{p}) > n$ and $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_{n+1}$ is a chain of prime ideals of A such that there is no prime ideal between $\mathfrak{p}_0$ and $\mathfrak{p}_1$. Localising at $\mathfrak{p}$, we may assume that A is local with maximal ideal $\mathfrak{p}$. Since $\mathfrak{p} = \mathfrak{p}_\circ$ is minimal over $\langle a_1, \ldots, a_n\rangle$, it follows that $a_i \notin \mathfrak{p}_\imath$ for some i. Without any loss of generality we assume that $a_1 \notin \mathfrak{p}_\imath$. Since there is no prime ideal of A between $\mathfrak{p}_\circ$ and $\mathfrak{p}_\imath$ and $\langle A, \mathfrak{p}_0\rangle$ is local, $\mathfrak{p}_\circ$ is the only prime ideal of A minimal over $\langle a_1, \mathfrak{p}_\imath\rangle$. Therefore, $\sqrt{\langle a_1, \mathfrak{p}_\imath\rangle} = \mathfrak{p}_\circ$. Thus, there exists an integer $t > 0$ such that $a_i^t = c_ia_1 + b_i$, where $c_i \in A$ and $b_i \in \mathfrak{p}_1$, $2 \leq i \leq n$.

Let $J = \langle b_2, \ldots, b_n\rangle$. Clearly, $\mathfrak{p}_\imath$ contains J, but it is not minimal over J. For, if so, then by the induction hypothesis $\mathrm{ht}(\mathfrak{p}_\imath) \leq n - 1$. But $\mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_{n+1}$ is a chain of prime ideals of length n. Thus, there exists $\mathfrak{q} \in \mathrm{Spec}(A)$ such that $J = \langle b_2, \ldots, b_n\rangle \subset \mathfrak{q} \subsetneq \mathfrak{p}_\imath$.

Let bar denote the reduction modulo $\mathfrak{q}$. We claim that $\overline{\mathfrak{p}}$ is minimal over $\langle \overline{a_1}\rangle$. It suffices to show that $\mathfrak{p}$ is the unique prime ideal of A containing $\langle a_1, \mathfrak{q}\rangle$. If $\widetilde{\mathfrak{p}} \in \mathrm{Spec}(A)$

is such that $\widetilde{\mathfrak{p}} \supset \langle a_1, \mathfrak{q} \rangle$, then $\widetilde{\mathfrak{p}} \supset \langle a_1, J \rangle$. Since $b_i \in J$, $a_i^t \in \widetilde{\mathfrak{p}}$, and hence $a_i \in \widetilde{\mathfrak{p}}$ for $2 \leq i \leq n$. This implies that $\langle a_1, \ldots, a_n \rangle \subset \widetilde{\mathfrak{p}} \subset \mathfrak{p}$. Therefore, $\widetilde{\mathfrak{p}} = \mathfrak{p}$. This proves the claim. Now, we have a chain of prime ideals $\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{q}$ in A which gives a chain of prime ideals $\overline{\mathfrak{p}} \supsetneq \overline{\mathfrak{p}_1} \supsetneq \overline{0}$ of length 2 in $A/\mathfrak{q}$. But, since $\overline{\mathfrak{p}}$ is minimal over $\langle \overline{a_1} \rangle$, by 1.6.1, $\mathrm{ht}(\overline{\mathfrak{p}}) \leq 1$. This is a contradiction. Hence the theorem follows. □

1.7 Converse of Krull's Theorem

Theorem 1.7.1 *Let A a Noetherian ring and $\mathfrak{p}$ be a prime ideal of A. If $\mathrm{ht}(\mathfrak{p}) = r \geq 1$, then there exist r elements $a_1, \ldots, a_r$ in $\mathfrak{p}$ such that $\mathfrak{p}$ is minimal over the ideal $\langle a_1, \ldots, a_r \rangle$.*

Proof. Since $\mathrm{ht}(\mathfrak{p}) \geq 1$, $\mathfrak{p}$ is not a minimal prime of A. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ be the minimal prime ideals of A. By Lemma 1.2.1, $\mathfrak{p} \nsubseteq \cup_{i=1}^{l} \mathfrak{p}_i$. We choose $a_1 \in \mathfrak{p}$, $a_1 \notin \cup_{i=1}^{l} \mathfrak{p}_i$. Then $\mathrm{ht}\langle a_1 \rangle \geq 1$.

Having chosen $a_1, a_2, \ldots, a_j \in \mathfrak{p}$, $j < r$, we choose a_{j+1} in the following manner. Let us suppose that $\mathfrak{q}_1', \ldots, \mathfrak{q}_m' \in \mathrm{Spec}(A)$ are the minimal prime ideals of A containing $\langle a_1, \ldots, a_j \rangle$. Then $\mathrm{ht}(\mathfrak{q}_k') \leq j$ and hence $\mathfrak{p} \nsubseteq \mathfrak{q}_k'$ for $k = 1, \ldots, m$. We choose $a_{j+1} \in \mathfrak{p}$ such that $a_{j+1} \notin \cup_{k=1}^{m} \mathfrak{q}_k'$.

We prove by induction that $\mathrm{ht}\langle a_1, \ldots, a_i \rangle \geq i$ for all i, $1 \leq i \leq r$. The case $i = 1$ follows as above. Assume by induction that $\mathrm{ht}\langle a_1, \ldots, a_i \rangle \geq i$. Now, let $\mathfrak{q} \in \mathrm{Spec}(A)$ such that $\mathfrak{q} \supset \langle a_1, \ldots, a_{i+1} \rangle$. We show that $\mathrm{ht}(\mathfrak{q}) \geq i + 1$. Since $\mathfrak{q} \supset \langle a_1, \ldots, a_i \rangle$, by induction $\mathrm{ht}(\mathfrak{q}) \geq i$. If $\mathrm{ht}(\mathfrak{q}) > i$ we are done. Assume $\mathrm{ht}(\mathfrak{q}) = i$. Then we claim that $\mathfrak{q}$ is minimal over $\langle a_1, \ldots, a_i \rangle$. For, suppose there exists prime ideal $\mathfrak{q}'$ of A such that $\mathfrak{q} \supset \mathfrak{q}' \supset \langle a_1, \ldots, a_i \rangle$. Then by induction $\mathrm{ht}(\mathfrak{q}') \geq i$. Since $\mathrm{ht}(\mathfrak{q}) = i$, it follows that $\mathfrak{q}' = \mathfrak{q}$. This proves that $\mathfrak{q}$ is minimal over $\langle a_1, \ldots, a_i \rangle$. Now, by the choice of a_{i+1}, $a_{i+1} \notin \mathfrak{q}$. This contradicts the fact that $\mathfrak{q} \supset \langle a_1, \ldots, a_{i+1} \rangle$. Hence $\mathrm{ht}(\mathfrak{q}) \geq i + 1$, proving the claim.

Therefore, $\mathrm{ht}\langle a_1, \ldots, a_r \rangle \geq r$. Since $\mathrm{ht}(\mathfrak{p}) = r$, $\mathfrak{p}$ is minimal over $\langle a_1, \ldots, a_r \rangle$. This completes the proof. □

1.8 Dimension of Polynomial Algebras

In this section we prove that if A is a Noetherian ring, then $\dim(A[X]) = \dim(A) + 1$.

Notation. 1.8.1 Let A be a ring, $I \subset A$ an ideal. We denote the extension of I in the polynomial ring $A[X]$ by $I[X]$.

Lemma 1.8.2 *Let A be ring and $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3$ be a chain of prime ideals in $A[X]$. Then we cannot have $\mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A = \mathfrak{p}_3 \cap A$.*

Proof. Assume to the contrary that a chain of prime ideals $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3$ exists with the above property. By going modulo $\mathfrak{p}_1 \cap A$ we may assume that A is a domain and $\mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A = \mathfrak{p}_3 \cap A = 0$. Let $S = A - \{0\}$. Since there is a one-to-one correspondence between prime ideals of $S^{-1}A[X]$ and prime ideals of $A[X]$ which do not meet S, we have $S^{-1}\mathfrak{p}_1 \subsetneq S^{-1}\mathfrak{p}_2 \subsetneq S^{-1}\mathfrak{p}_3$. However, since $S^{-1}A$ is a field, $S^{-1}A[X]$ is a PID, and hence is of dimension 1. Hence the lemma follows. □

Lemma 1.8.3 *Let A be a Noetherian ring and I be an ideal of $A[X]$ with $\mathrm{ht}(I) = n$. Then $\mathrm{ht}(I \cap A) \geq n - 1$.*

Proof. We split the proof in two cases.

Case 1. I is a prime ideal. Let $I = \mathfrak{p} \in \text{Spec}(A[X])$. We claim that $\text{ht}(\mathfrak{p}) = \text{ht}(\mathfrak{p} \cap A)$ if $\mathfrak{p} = (\mathfrak{p} \cap A)[X]$ and $\text{ht}(\mathfrak{p}) = \text{ht}(\mathfrak{p} \cap A) + 1$ if $\mathfrak{p} \supsetneq (\mathfrak{p} \cap A)[X]$. It is clear that any chain of prime ideals $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_s \subsetneq (\mathfrak{p} \cap A)$ in A can be extended to a chain of prime ideals

$$\mathfrak{q}_0[X] \subsetneq \mathfrak{q}_1[X] \subsetneq \cdots \subsetneq \mathfrak{q}_s[X] \subsetneq (\mathfrak{p} \cap A)[X] \subset \mathfrak{p} \tag{6}$$

in $A[X]$. Let $\text{ht}(\mathfrak{p} \cap A) = r$. By Theorem 1.7.1, $(\mathfrak{p} \cap A)$ is minimal over an ideal J which is generated by r elements.

We claim that $(\mathfrak{p} \cap A)[X]$ is minimal over $J[X]$, which is also generated by r elements. For, if there exists a prime ideal $\mathfrak{q}$ in $A[X]$ such that $J[X] \subset \mathfrak{q} \subset (\mathfrak{p} \cap A)[X]$, then $J \subset J[X] \cap A \subset \mathfrak{q} \cap A \subset \mathfrak{p} \cap A$, and hence $\mathfrak{p} \cap A = \mathfrak{q} \cap A$. This implies that $\mathfrak{q} \subset (\mathfrak{p} \cap A)[X] = (\mathfrak{q} \cap A)[X] \subseteq \mathfrak{q}$. Therefore, $\mathfrak{q} = (\mathfrak{p} \cap A)A[X]$, yielding the claim. Hence by Theorem 1.6.10, $\text{ht}(\mathfrak{p} \cap A)[X] \leq r$. Therefore, if $\mathfrak{p} = (\mathfrak{p} \cap A)[X]$, then $\text{ht}(\mathfrak{p}) \leq r$. But $\text{ht}(\mathfrak{p} \cap A) = r$, so that $\text{ht}(\mathfrak{p}) \geq r$ by (6). Therefore, it follows that $\text{ht}(\mathfrak{p}) = r$.

On the other hand if $(\mathfrak{p} \cap A)[X] \subsetneq \mathfrak{p}$, then there exists $f(X) \in \mathfrak{p}$, $f(X) \notin (\mathfrak{p} \cap A)[X]$. Since J is generated by r elements, $I_1 = \langle J[X], f \rangle$ is generated by $r + 1$ elements. We claim that $\mathfrak{p}$ is minimal over I_1. Assuming the claim it follows by Krull's theorem that $\text{ht}(\mathfrak{p}) \leq r + 1$. Now, by (6), we have $\text{ht}(\mathfrak{p}) > \text{ht}(\mathfrak{p} \cap A)[X] = \text{ht}(\mathfrak{p} \cap A) = r$. Thus, $\text{ht}(\mathfrak{p}) \geq r + 1$. Hence $\text{ht}(\mathfrak{p}) = r + 1$, proving the first assertion.

Proof of the claim: Suppose $I_1 \subset \mathfrak{p}' \subsetneq \mathfrak{p}$ for some $\mathfrak{p}' \in \text{Spec } A[X]$. Then $J \subset (\mathfrak{p}' \cap A) \subset (\mathfrak{p} \cap A)$. Since $(\mathfrak{p} \cap A)$ is minimal over J, $(\mathfrak{p}' \cap A) = (\mathfrak{p} \cap A)$. Since $f \notin (\mathfrak{p} \cap A)[X]$, $(\mathfrak{p} \cap A)[X] \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p}$. But, $(\mathfrak{p} \cap A) = (\mathfrak{p} \cap A)[X] \cap A = \mathfrak{p}' \cap A = \mathfrak{p} \cap A$, contradicting 1.8.2. This proves the claim.

Case 2. I is any ideal of $A[X]$. By the Noetherian property of A, $\sqrt{I} = \cap_{i=1}^{r} \mathfrak{p}_i$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the minimal primes over I. Then $\sqrt{I \cap A} = \sqrt{I} \cap A = \cap_{i=1}^{r} (\mathfrak{p}_i \cap A)$. Therefore, from 1.4.14 and the definition of height, $\text{ht}(I \cap A) = \text{ht}(\mathfrak{p}_i \cap A)$ for some $i = 1, 2, \ldots, n$. Using Case 1, $\text{ht}(I \cap A) = \text{ht}(\mathfrak{p}_i \cap A) \geq \text{ht}(\mathfrak{p}_i) - 1 \geq \text{ht}(I) - 1$. This completes the proof. □

Corollary 1.8.4 *If A is a Noetherian ring then* $\dim(A[X]) = \dim(A) + 1$.

Proof. Note that for a maximal ideal $\mathfrak{m}$ of A, $\frac{A[X]}{\mathfrak{m}[X]} \simeq \frac{A}{\mathfrak{m}}[X]$ is not a field. Since every strictly increasing chain of prime ideals of A gives a strictly increasing chain of prime ideals in $A[X]$, and for a maximal ideal $\mathfrak{m}$ of A, $\mathfrak{m}[X]$ is prime but not a maximal ideal of $A[X]$, it follows that $\dim(A[X]) \geq \dim(A) + 1$.

Let $\dim(A) = d$. We may assume that d is finite. Otherwise there is nothing to prove. Assume that $\dim(A[X]) > \dim(A) + 1$. Let M be a maximal ideal of $A[X]$ of height $> d + 1$. Then by 1.8.3, $\text{ht}(M \cap A) > d$. This contradicts the fact that $\dim(A) = d$. Hence the result follows. □

1.9 Integral Extensions

In this section we prove some basic results on integral extensions.

Definition 1.9.1 Let A be a ring and $f(X) \in A[X]$. Then $f(X)$ is said to be a **monic polynomial** if the coefficient of the leading term of $f(X)$ is 1.

Definition 1.9.2 Let $A \hookrightarrow B$ be a ring extension. An element $x \in B$ is said to be integral over A if $f(x) = 0$, where $f(X) \in A[X]$ is a monic polynomial *i.e.* if $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, where $a_i \in A$, and $n > 0$.

Proposition 1.9.3 *Let $A \hookrightarrow B$ be a ring extension. Then the following are equivalent.*

1. *$x \in B$ is integral over A.*
2. *$A[x]$ is a finitely generated A-module.*
3. *$A[x]$ is contained in a subring C such that C is a finitely generated A-module.*

Proof. (1) $\Rightarrow$ (2): If x is integral over A, then $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some $n > 0$ and $a_i \in A\,(1 \leq i \leq n)$. Therefore, all powers of x lie in the A-module generated by $1, x, \ldots, x^{n-1}$. Hence $A[x]$ is generated by $1, x, \ldots, x^{n-1}$ as an A-module.

(2) $\Rightarrow$ (3): Taking $C = A[x]$, the result follows.

(3) $\Rightarrow$ (1): Let $c_1, \ldots, c_r$ generate C as an A-module. Let $xc_i = \sum_{j=1}^{r} \lambda_{ij}c_j$, where $\lambda_{ij} \in A$. Let

$$\alpha = \begin{pmatrix} x - \lambda_{11} & -\lambda_{12} & \cdots & -\lambda_{1n} \\ -\lambda_{21} & x - \lambda_{22} & \cdots & -\lambda_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ -\lambda_{n1} & -\lambda_{n2} & \cdots & x - \lambda_{nn} \end{pmatrix}.$$

As in the proof of Nakayama Lemma we get $\det(\alpha)C = 0$. Since $1 \in C$, $\det \alpha = 0$. Expanding the determinant, we see that x is integral over A. □

Example 1.9.4 Let A be a ring and $I \subset A[X]$ be an ideal containing a monic polynomial and $J = I \cap A$. Then the extension $A/J \hookrightarrow A[X]/I$ is integral.

Proposition 1.9.5 *Let $A \hookrightarrow B$ be a ring extension. If $x_1, \ldots, x_n \in B$ are integral over A, then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

Proof. The proof follows by induction on n. □

Proposition 1.9.6 *Let $A \hookrightarrow B$ be a ring extension. The set of all elements of B which are integral over A is a subring of B containing A.*

Proof. Let C be the set of all elements of B which are integral over A. Let $x, y \in C$. Then $A[x, y]$ is a finitely generated A-module. Since $A[x \pm y] \subset A[x, y]$ and $A[xy] \subset A[x, y]$, it follows that $A[x \pm y]$ and $A[xy]$ are contained in a ring $A[x, y]$, which is a finitely generated A-module. Therefore, by 1.9.5, $x \pm y$ and xy are integral over A and hence are in C. □

Definition 1.9.7 The Subring C defined in 1.9.6 is called the **integral closure** of A in B.

Let the notation be as in 1.9.6 and 1.9.7.

1. If B=C, then $A \hookrightarrow B$ said to be an integral extension. The ring B is said to be integral over A. We say that B/A is integral.
2. If A=C, then A is said to be integrally closed in B.
3. If A=C is a domain and B is the quotient field of A, then A is said to be integrally closed.

Proposition 1.9.8 *If $A \hookrightarrow B$ and $B \hookrightarrow C$ are integral extensions, then so is $A \hookrightarrow C$.*

Proof. Let $x \in C$. Since C is integral over B, $x^n + b_1x^{n-1} + \cdots + b_n = 0$, where $b_i \in B$ $(1 \leq i \leq n)$. Therefore, x is integral over $A[b_1, \ldots, b_n]$. Since $A \hookrightarrow B$ is an integral extension, each b_i is integral over A. Therefore, $A[b_1, \ldots, b_n]$ is a finitely generated A-module. But as x is integral over $A[b_1, \ldots, b_n]$, $A[b_1, \ldots, b_n][x]$ is a finitely generated $A[b_1, \ldots, b_n]$-module. This implies that $A[b_1, \ldots, b_n][x]$ is a finitely generated A-module. Therefore, x is contained in a ring *viz.* $A[b_1, \ldots, b_n][x]$, which is finitely generated as an A-module. By 1.9.3, it follows that x is integral over A. □

Proposition 1.9.9 *Let $A \hookrightarrow B$ be an integral extension. Let I be an ideal of B and $J = I \cap A$. Then $A/J \hookrightarrow B/I$ is an integral extension.*

Proof. Let $\overline{x} \in B/I$, where bar denotes reduction modulo J. Since B is integral over A, x satisfies a monic polynomial *i.e.*, $x^n + a_1x^{n-1} + \cdots + a_n = 0$, where $a_i \in A$, $1 \leq i \leq n$. It follows that $\overline{x}$ is integral over A/J. □

Proposition 1.9.10 *Let $A \hookrightarrow B$ be an integral extension. Let S be a multiplicative closed subset of A. Then $S^{-1}A \hookrightarrow S^{-1}B$ is an integral extension.*

Proof. Let $x/s \in S^{-1}B$, where $x \in B$, $s \in S$. Since $A \hookrightarrow B$ is integral, $x^n + a_1x^{n-1} + \cdots + a_n = 0$, where $a_i \in A$, $1 \leq i \leq n$. Dividing both sides by s^n, we get

$$\left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0.$$

Thus, x/s is integral over $S^{-1}A$. This proves the proposition. □.

Proposition 1.9.11 *Let $A \hookrightarrow B$ be an integral extension of domains. Then A is a field if and only if B is a field.*

Proof. Suppose A is a field and $x \in B$ be a non zero element. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$, where $a_i \in A$, $1 \leq i \leq n$, be a polynomial of least degree such that $f(x) = 0$. Since B is a domain, it follows that $a_n \neq 0$. As A is a field, $a_n^{-1} \in A$ and hence the element $(-a_n)^{-1}(x^{n-1} + a_1x^{n-2} + \cdots + a_{n-1})$ is inverse of x in B, proving that B is a field.

Conversely, let B be a field and $y \in A$ be a non zero element. Let $x = y^{-1}$. Then $x^m + a_1'x^{m-1} + \cdots + a_n' = 0$, where $a_i' \in A$, $1 \leq i \leq n$. Multiplying by y^m, we get $1 + a_1'y + \cdots + a_m'y^m = 0$, *i.e.* y is invertible in A. Hence A is a field. □

Corollary 1.9.12 *Let $A \hookrightarrow B$ be an integral extension. Let $\mathfrak{p}$ be a prime ideal of A and $\mathfrak{q}$ be a prime ideal of B be such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then $\mathfrak{p}$ is a maximal ideal of A if and only if $\mathfrak{q}$ is a maximal ideal of B.*

Proof. The proof follows from 1.9.9 and 1.9.11. □

Theorem 1.9.13 *Let $A \hookrightarrow B$ be integral extension of rings and $\mathfrak{p}$ be a prime ideal of A. Then there exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Motivation for the proof. If such a prime ideal $\mathfrak{q}$ exists, then $\mathfrak{q} \supset \mathfrak{p}B$ and $\mathfrak{q} \cap (A - \mathfrak{p}) = \Phi$. This implies that $\mathfrak{p}B \cap (A - \mathfrak{p}) = \Phi$. Assuming that the extension $A \hookrightarrow B$ is integral, we first show that $\mathfrak{p}B \cap (A - \mathfrak{p}) = \Phi$ and then use this to prove Theorem 1.9.13.

Lemma 1.9.14 *Let $A \hookrightarrow B$ be an integral extension, $\mathfrak{p}$ a prime ideal of A. Then any element $x \in \mathfrak{p}B$ satisfies an equation $x^n + a_1x^{n-1} + \cdots + a_n = 0$, where $a_i \in \mathfrak{p}$, $1 \leq i \leq n$.*

Proof. Let $x \in \mathfrak{p}B$. Then $x = \sum_{i=1}^n p_ib_i$, where $p_i \in \mathfrak{p}$ and $b_i \in B$. Since B is integral over A, $A[b_1, \ldots, b_n] = S$ (say) is a finitely generated A-module. Let $S = Aw_1 + \cdots + Aw_r$, where $w_j \in S$, $1 \leq j \leq r$.

Since $b_i \in S$, $b_iw_j = \sum_{k=1}^r \lambda_{ik}w_k$, where $\lambda_{ik} \in A$. Since $x = \sum_{i=1}^n p_ib_i$ and $p_i \in \mathfrak{p}$, we have $xw_j = \sum_{k=1}^r g_{jk}w_k$, where $g_{jk} \in \mathfrak{p}$, $1 \leq k \leq r$. Now the proof follows as in the proof of (3) ⇒ (1) of 1.9.3. □

Lemma 1.9.15 *Let $A \hookrightarrow B$ be an integral extension of rings. If $\mathfrak{p}$ is any prime ideal of A, then $\mathfrak{p}B \cap (A - \mathfrak{p}) = \Phi$.*

Proof. Suppose to the contrary let $x \in \mathfrak{p}B \cap (A - \mathfrak{p})$. Since $x \in \mathfrak{p}B$, by Lemma 1.9.14, it follows that $x^n + a_1x^{n-1} + \cdots + a_n = 0$, where $a_i \in \mathfrak{p}$, $1 \leq i \leq n$. This implies that $x^n \in \mathfrak{p}$ and hence $x \in \mathfrak{p}$, contradicting the fact that $x \in A - \mathfrak{p}$. Hence the lemma. □

Proof of Theorem 1.9.13. In view of Lemma 1.4.10, we can extend $\mathfrak{p}B$ to a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap (A - \mathfrak{p}) = \Phi$. This implies that $\mathfrak{q} \cap A \subseteq \mathfrak{p}$. Also, $\mathfrak{p} \subseteq \mathfrak{p}B \cap A \subseteq \mathfrak{q} \cap A$, showing that $\mathfrak{p} = \mathfrak{q} \cap A$. Hence the theorem. □

Theorem 1.9.16 *Let $A \hookrightarrow B$ be an integral extension of rings. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2$ be prime ideals of A and $\mathfrak{q}_1$ prime ideal of B such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there exists a prime ideal $\mathfrak{q}_2$ of B such that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ and $\mathfrak{q}_1 \subset \mathfrak{q}_2$.*

Proof. Since $A \hookrightarrow B$ is an integral extension, by 1.9.9 it follows that $A/\mathfrak{p}_1 \hookrightarrow B/\mathfrak{q}_1$ is an integral extension. Let us consider the following commutative diagram :

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} \\ A/\mathfrak{p}_1 & \longrightarrow & B/\mathfrak{q}_1 \end{array}$$

Since $\overline{\mathfrak{p}_2}$ is a prime ideal of $A/\mathfrak{p}_1$ by Theorem 1.9.13, there exists a prime ideal, say $\overline{\mathfrak{q}_2}$, in $B/\mathfrak{q}_1$ such that $\overline{\mathfrak{q}_2} \cap (A/\mathfrak{p}_1) = \overline{\mathfrak{p}_2}$. Then $\psi^{-1}(\overline{\mathfrak{q}_2}) = \mathfrak{q}_2$ (say) is a prime ideal. Since the above diagram is commutative, $\mathfrak{q}_2 \cap A = \phi^{-1}(\overline{\mathfrak{p}_2}) = \mathfrak{p}_2$. This completes the proof. □

Theorem 1.9.17 (Going-up Theorem) *Let $A \hookrightarrow B$ be an integral extension of rings. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \cdots \subset \mathfrak{q}_m$ $(m \leq n)$ be a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ $(1 \leq i \leq m)$. Then the chain $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \cdots \subset \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \cdots \subset \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.*

Corollary 1.9.18 *If $A \hookrightarrow B$ is an integral extension of rings then* $\dim(A) = \dim(B)$.

Theorem 1.9.19 *Let $A \hookrightarrow B$ be an integral extension of domains with A integrally closed. Suppose $\mathfrak{p}_1 \subsetneq \mathfrak{p}_0$ are prime ideals of A such that there exists a prime ideal $\mathfrak{q}_0$ of B with the property that $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$. Then there exists a prime ideal $\mathfrak{q}_1$ of B such that $\mathfrak{q}_1 \subsetneq \mathfrak{q}_0$, and $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.*

Motivation for the proof of 1.9.19. Suppose we have $\mathfrak{p}_1 \subsetneq \mathfrak{p}_0$ prime ideals of A and there exists a prime ideal $\mathfrak{q}_0$ of B with the property that $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$. We want a prime ideal $\mathfrak{q}_1$ of B such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$ and $\mathfrak{q}_1 \subset \mathfrak{q}_0$.

If such a prime ideal exists, then $\mathfrak{q}_1 \cap (B - \mathfrak{q}_0) = \Phi$, $\mathfrak{q}_1 \cap (A - \mathfrak{p}_1) = \Phi$ and $\mathfrak{q}_1 \supset \mathfrak{p}_1B$. In that case it would follow that $\mathfrak{q}_1 \cap (B - \mathfrak{q}_0)(A - \mathfrak{p}_1) = \Phi$ and hence $\mathfrak{p}_1B \cap (B - \mathfrak{q}_0)(A - \mathfrak{p}_1) = \Phi$. We show that if $A \hookrightarrow B$ is an integral extension of domains and A is integrally closed, then this is the case and then use this to prove Theorem 1.9.19.

Lemma 1.9.20 *Let $A \hookrightarrow B$ be an integral extension of domains, where A is integrally closed with quotient field K. Then if $b \in B$, the minimal monic polynomial of b over K belongs to $A[X]$.*

Proof. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be the minimal monic polynomial of b over K, where $a_i \in K$, $1 \leq i \leq n$. We show that $a_i \in A$ for $1 \leq i \leq n$. Let $d_1, \ldots, d_n$ be the roots of $f(X)$ in some algebraic extension L of K, where $B \subset K$. Note that we can choose such a field L, as the quotient field of B is algebraic over K, B being

integral over A. Since b is integral over A, b satisfies a monic polynomial, say $\phi(X)$ over A. Since $f(X)$ is the minimal polynomial of b, it follows that $f(X)|\phi(X)$ in $K[X]$, so that $\phi(d_i) = 0$, $1 \leq i \leq n$. Hence the d_i's are integral over A for $1 \leq i \leq n$. Since $(X - d_1)(X - d_2)\cdots(X - d_n) = X^n + a_1X^{n-1} + \cdots + a_n$, the a_i are integral over A, $1 \leq i \leq n$. But, since A is integrally closed, it follows that $a_i \in A$, $1 \leq i \leq n$. This completes the proof. □

Lemma 1.9.21 *Let $A \hookrightarrow B$ be an integral extension of domains, where A integrally closed with quotient field K. Let $\mathfrak{p}$ be a prime ideal of A and $b \in \mathfrak{p}B$. Let $f(X) = X^m + c_1X^{m-1} + \cdots + c_m$ be the minimal polynomial of b over K. Then $c_i \in \mathfrak{p}$ for $1 \leq i \leq n$.*

Proof. Since $b \in \mathfrak{p}B$, it follows from 1.9.14 that b satisfies a monic polynomial $g(X) = X^n + a_1X^{n-1} + \cdots + a_n$, where $a_i \in \mathfrak{p}$, $1 \leq i \leq n$. Let $f(X) = X^m + c_1X^{m-1} + \cdots + c_m$ be the minimal polynomial of b over K. By 1.9.20, $c_i \in A$ for $1 \leq i \leq m$. Since $f(X)$ is monic, $\underline{g(X) = f(X)h(X)}$, where $\underline{h(X)} \in \underline{A[X]}$. Let bar denote the reduction modulo $\mathfrak{p}$. Since $g(X) = \overline{X^n} = \overline{f(X)h(X)}$, $\overline{f(X)} = \overline{X^m}$, where $m \leq n$. This means $c_i \in \mathfrak{p}$ for $1 \leq i \leq m$. Hence the lemma follows. □

Lemma 1.9.22 *Let $A \hookrightarrow B$ be an integral extension of domains with A integrally closed and $\mathfrak{p}_1 \subsetneq \mathfrak{p}_0$ prime ideals of A such that there exists a prime ideal $\mathfrak{q}_0$ of B with the property that $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$. Then $\mathfrak{p}_1B \cap (B - \mathfrak{q}_0)(A - \mathfrak{p}_1) = \Phi$.*

Proof. Let $a \in (A - \mathfrak{p}_1)$, $b \in (B - \mathfrak{q}_0)$ and $c = ab$. Suppose to the contrary that $c \in \mathfrak{p}_1B$. Let $f(X) = X^n + \lambda_1X^{n-1} + \cdots + \lambda_n$ be the minimal polynomial of c over the quotient field of A. From 1.9.21, it follows that $\lambda_i \in \mathfrak{p}_1$. Since $a \in A$, the minimal polynomial of b over the quotient field of A is $X^n + (\lambda_1/a)X^{n-1} + \cdots + (\lambda_n/a^n)$. Since A is integrally closed, by 1.9.20, $\lambda_i/a^i \in A$ for $1 \leq i \leq n$. Let $\mu_i = \lambda_i/a^i$. Then as $a \notin \mathfrak{p}_1$, $\lambda_i = a^i\mu_i$ and $\lambda_i \in \mathfrak{p}_1$, it follows that $\mu_i \in \mathfrak{p}_1$. Since $b^n + \mu_1b^{n-1} + \cdots + \mu_n = 0$, $b^n \in \mathfrak{p}_1B \subset \mathfrak{q}_0$, implying that $b \in \mathfrak{q}_0$. This yields a contradiction. Hence the lemma. □

Proof of the Theorem 1.9.19. By Lemma 1.9.22 we get $\mathfrak{p}_1B \cap (B - \mathfrak{q}_0)(A - \mathfrak{p}_1) = \Phi$. Using 1.4.10, enlarge $\mathfrak{p}_1B$ to a prime ideal $\mathfrak{q}_1$ of B such that $\mathfrak{q}_1 \cap (B - \mathfrak{q}_0)(A - \mathfrak{p}_1) = \Phi$. Then $\mathfrak{p}_1B \subset \mathfrak{q}_1$ implies that $\mathfrak{p}_1 \subset \mathfrak{q}_1 \cap A$. Also $\mathfrak{q}_1 \cap (A - \mathfrak{p}_1) = \Phi$ implies that $\mathfrak{q}_1 \cap A \subset \mathfrak{p}_1$, so that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Moreover, $\mathfrak{q}_1 \cap (B - \mathfrak{q}_0) = \Phi$ implying that $\mathfrak{q}_1 \subset \mathfrak{q}_0$. □

Theorem 1.9.23 (Going-down Theorem) *Let $A \hookrightarrow B$ be an integral extension of domains where A is integrally closed. Let $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be a decreasing chain of prime ideals of A and $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ $(m \leq n)$ be a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$. Then the chain $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ $(m \leq n)$ can be extended to a chain $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.*

Corollary 1.9.24 *Let $A \hookrightarrow B$ be an integral extension of domains with A integrally closed. Let $\mathfrak{p}$ be a prime ideal of B. Then* $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p} \cap A)$.

Lemma 1.9.25 *Let A be a ring and J be an ideal of A. If $f(X) \in A[X]$ is monic then $\langle JA[X], f(X)\rangle \cap A = J$.*

Proof. The proof is an easy checking. □

1.10 Dimension of Affine Algebras

Definition 1.10.1 Let k be a field, $I \subset k[X_1, \ldots, X_n]$ an ideal and $A = k[X_1, \ldots, X_n]/I$. Then A is said to be an **affine k-algebra**. If A is a domain, then we say that A is an **affine domain** over k.

In this section we prove the following theorem.

Theorem 1.10.2 *Let A be an affine domain over a field k and $\mathfrak{p}$ be a prime ideal of A. Then* $\mathrm{ht}(\mathfrak{p}) + \dim\left(\frac{A}{\mathfrak{p}}\right) = \dim(A)$.

Before proving the theorem we first prove some lemmas.

Lemma 1.10.3 *Let k be a field, $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ 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 $\varphi|_k = \mathrm{Id}$, $\varphi(X_i) = X_i + X_n^{c_i}$ for $1 \leq i \leq n-1$ and $\varphi(X_n) = X_n$, then $\varphi(f(X_1, \ldots X_n))$ is monic in X_n (after multiplying an element of k^*).*

Proof. We have

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

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

$$c_1\beta_1 + \cdots + c_{n-1}\beta_{n-1} + \beta_n \neq c_1\gamma_1 + \cdots + c_{n-1}\gamma_{n-1} + \gamma_n. \tag{7}$$

For, we choose $t > \max(\gamma_i, \beta_j)$ $(1 \leq i, j \leq n)$. Let $c_1 = t^{n-1}, c_2 = t^{n-2}, \ldots, c_{n-1} = t$. We claim these c_i's satisfy equation (7). This follows by considering t-adic expansions. It is now clear that if t is suitably chosen, then $\varphi(f(X_1, \ldots, X_n))$ is monic. □

Lemma 1.10.4 (Noether Normalization) *Let $k[X_1, \ldots, X_n]$ be a polynomial ring in n variables over a field k, $I \subset k[X_1, \ldots, X_n]$ an ideal and $A = k[X_1, \ldots, X_n]/I$ be an affine algebra over k. Then there exists a polynomial subring $B = k[Z_1, \ldots, Z_m]$ of A such that $B \hookrightarrow A$ is an integral extension.*

Proof. We prove the lemma by induction on the number of variables n. If $I = 0$, we choose $B = k[X_1, \ldots, X_n]$. So, we assume that $I \neq 0$.

Suppose $n = 1$. Since I contains a monic polynomial, using 1.9.4, $k \hookrightarrow k[X_1]/I$ is an integral extension. Taking $B = k$, the result follows.

Assume $n > 1$. Let $f(X_1, \ldots, X_n) \in I$, $f \neq 0$. Applying the automorphism φ in 1.10.3, *viz.* $\varphi|_k = \mathrm{Id}$, $\varphi(X_i) = X_i + X_n^{c_i}$ for $1 \leq i \leq n-1$ and $\varphi(X_n) = X_n$, we may assume that $\varphi(f)$ is monic in X_n. Let $J = \varphi(I)$. Then J contains a monic polynomial *viz.* $\varphi(f)$. Hence using 1.9.4, $k[X_1, \ldots, X_{n-1}]/J \cap k[X_1, \ldots, X_{n-1}] \hookrightarrow k[X_1, \ldots, X_n]/J$ is an integral extension. We claim that $k[X_1, \ldots, X_n]/I$ is integral over the image of $k[X_1 - X_n^{c_1}, \ldots, X_{n-1} - X_n^{c_{n-1}}]$ in $k[X_1, \ldots, X_n]/I$. Let

$$\varphi(f) = X_n^r + g_{i-1}(X_1, \ldots, X_{n-1})X_n^{r-1} + \cdots + g_0(X_1, \ldots, X_{n-1}) \in J.$$

Since $\varphi^{-1}(J) = I$, we have $\varphi^{-1}(f) = X_n^r + g_{i-1}(X_1 - X_n^{c_1}, \ldots, X_{n-1} - X_n^{c_{n-1}})X_n^{r-1} + \cdots + g_0(X_1 - X_n^{c_1}, \ldots, X_{n-1} - X_n^{c_{n-1}}) \in I$. This proves the claim.

The image C of $k[X_1 - X_n^{c_1}, \ldots, X_{n-1} - X_n^{c_{n-1}}]$ in $k[X_1, \ldots, X_n]/I$ is an affine k-algebra in $n-1$ variables. By induction there exists a polynomial subring $B = k[Z_1, \ldots, Z_m]$ of C such that $B \hookrightarrow C$ is an integral extension. Since $C \hookrightarrow A$ is integral, $B \hookrightarrow A$ is integral, proving the lemma. □

Lemma 1.10.5 *A Noetherian integral domain A is a UFD if and only if every height one prime ideal of A is principal.*

Proof. Let A be a Noetherian UFD and $\mathfrak{p} \in \mathrm{Spec}(A)$ with $\mathrm{ht}(\mathfrak{p}) = 1$. Let $a \in \mathfrak{p}$, $a \neq 0$. Since A is a Noetherian, a can be expressed as $a = \Pi_{i=1}^{n} d_i$ with $d_i \in A$, d_i irreducible. Since $\mathfrak{p}$ is prime ideal, $d_i \in \mathfrak{p}$ for some i. Since A is a UFD, $\langle d_i \rangle$ is a (non zero) prime ideal of A. As $\mathrm{ht}(\mathfrak{p}) = 1$, $\mathfrak{p} = \langle d_i \rangle$. Thus, $\mathfrak{p}$ is a principal ideal.

Conversely, assume that every height one prime ideal of A is principal. Since A is Noetherian, any non-zero, non-unit element of A can be expressed as a product of finitely many irreducible elements. So, it is enough to show that every irreducible element of A is prime. Let $a \in A$ be irreducible and $\mathfrak{p}$ be a minimal prime over $\langle a \rangle$. Since A is a domain, by Krull's theorem $\mathrm{ht}(\mathfrak{p}) = 1$. Therefore, by hypothesis $\mathfrak{p} = \langle b \rangle$ for some $b \in A$, and hence $a = bc$ for some $c \in A$. Then c is a unit as a is irreducible. Thus, $\langle a \rangle = \langle b \rangle = \mathfrak{p}$, so that a is a prime element of A. □

Lemma 1.10.6 *Let A be a UFD. Then A is integrally closed.*

Proof. Let K be the quotient field of A. Let $c, d \in A$ and $c/d \in K$ be integral over A. We show that $c/d \in A$. We may assume without loss of generality that c and d do not have any common prime factors. Since c/d is integral over A, we have

$$\left(\frac{c}{d}\right)^n + \lambda_1 \left(\frac{c}{d}\right)^{n-1} + \cdots + \lambda_n = 0,$$

where $\lambda_i \in A$, $1 \leq i \leq n$. Multiplying this equation by d^n, we see that d divides c^n. Hence d is a unit of A (otherwise d and c have a common prime factor). This is proves the lemma. □

Corollary 1.10.7 *If k is a field and $A = k[X_1, \ldots, X_n]$ then A is integrally closed.*

Lemma 1.10.8 *Let $A = k[X_1, \ldots, X_n]$, $\mathfrak{p} \in \mathrm{Spec}(A)$. Then* $\mathrm{ht}(\mathfrak{p}) + \dim\left(\frac{A}{\mathfrak{p}}\right) = \dim(A)$.

Proof. We prove the lemma by induction on number of variables n. It is clear that the lemma is true for $n = 1$. Since the lemma is vacuously true for $\mathrm{ht}(\mathfrak{p}) = 0$, we assume $\mathrm{ht}(\mathfrak{p}) = r > 0$. Let $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_{r-1} \supsetneq \mathfrak{p}_r = \langle 0 \rangle$ be a chain of prime ideals of length r. Then $\mathrm{ht}(\mathfrak{p}_{r-1}) = 1$. By Lemma 1.10.5, $\mathfrak{p}_{r-1} = \langle f \rangle$ for some $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$. By an automorphism of $k[X_1, \ldots, X_n]$ (see 1.10.3), we may assume that f is monic in X_n. Thus,

$$B = k[X_1, \ldots, X_{n-1}] \hookrightarrow \frac{k[X_1, \ldots, X_n]}{\langle f \rangle} = C$$

is an integral extension with B integrally closed. Let bar denote the reduction modulo $\langle f \rangle$. Then $\overline{\mathfrak{p}} = \overline{\mathfrak{p}_0} \supsetneq \cdots \supsetneq \langle \overline{f} \rangle = \langle \overline{0} \rangle$ is a chain of prime ideals in C of length $r - 1$. Let $\overline{\mathfrak{p}} \cap B = \mathfrak{q}$. Since $\mathrm{ht}(\mathfrak{p}) = r$, $\mathrm{ht}(\overline{\mathfrak{p}}) = r - 1$. Now, from Corollary 1.9.24, we get $\mathrm{ht}(\overline{\mathfrak{p}}) = \mathrm{ht}(\mathfrak{q})$. Also, using 1.9.9 and 1.9.18, we see that $\dim(C/\overline{\mathfrak{p}}) = \dim(B/\mathfrak{q})$. This implies that $\mathrm{ht}(\overline{\mathfrak{p}}) + \dim(C/\overline{\mathfrak{p}}) = \mathrm{ht}(\mathfrak{q}) + \dim(B/\mathfrak{q})$. But, by induction, $\mathrm{ht}(\mathfrak{q}) + \dim(B/\mathfrak{q}) = n - 1$, so that $r + \dim(C/\overline{\mathfrak{p}}) = n$. But, $\dim(C/\overline{\mathfrak{p}}) = \dim(A/\mathfrak{p})$, hence the result follows. □

Proof of Theorem 1.10.2. By Theorem 1.10.4, there exists a polynomial subalgebra B of A such that the extension $B \hookrightarrow A$ is integral. Let $\mathfrak{p} \cap B = \mathfrak{q}$. By 1.9.9 and 1.9.18, $\dim(A/\mathfrak{p}) = \dim(B/\mathfrak{q})$ and by 1.9.24, $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q})$. Thus, by Lemma 1.10.8, $\mathrm{ht}(\mathfrak{q}) + \dim(B/\mathfrak{q}) = \dim(B)$. Hence it follows that $\mathrm{ht}(\mathfrak{p}) + \dim\left(\frac{A}{\mathfrak{p}}\right) = \dim(A)$. □

2 Unimodular Rows

In this section we prove a few basic results on unimodular rows.

2.1 Completability condition for a Unimodular Row over a Ring

$$\begin{aligned}
A &= \text{commutative ring with identity element} \\
A^* &= \text{group of invertible elements of } A \\
A[X_1, X_2, \ldots, X_n] &= \text{polynomial ring in } n \text{ variables } X_1, X_2, \ldots, X_n \\
&\quad \text{over the ring } A \\
\langle a_1, a_2, \ldots, a_n \rangle &= \text{ideal generated by } a_1, a_2, \ldots, a_n \\
[a_1, a_2, \ldots, a_n] &= \text{row with } n \text{ entries } a_1, a_2, \ldots, a_n \\
(a_1, a_2, \ldots, a_n) &= 1 \times n \text{ matrix with } n \text{ entries } a_1, a_2, \ldots, a_n
\end{aligned}$$

We recall that the set of all $n \times n$ matrices over a ring A is a ring under matrix addition and matrix multiplication and is denoted by $M_n(A)$.

A matrix $\alpha \in M_n(A)$ is said to be invertible if there exists $\beta \in M_n(A)$ such that $\alpha\beta = \beta\alpha = I_n$. If $\alpha \in M_n(A)$ is invertible, then it follows that $\det(\alpha)$ is a unit of A. Conversely, if $\det(\alpha)$ is a unit of A, it follows from the identity $\alpha\,\mathrm{adj}(\alpha) = \mathrm{adj}(\alpha)\,\alpha = \det(\alpha)I_n$ that α is invertible. The set of invertible matrices belonging to $M_n(A)$ form a group under matrix multiplication and this group is denoted by $GL_n(A)$. Elements of $GL_n(A)$ give rise to automorphisms of the free module A^n.

The subgroup of $SL_n(A)$ of $GL_n(A)$ consists of all matrices with determinant 1.

Let $E_{ij}(\lambda)$, $i \neq j$, $\lambda \in A$, denote the matrix $I_n + \lambda e_{ij}$, where e_{ij} is the matrix with 1 in the (i, j) th position and zeroes elsewhere. The subgroup of $SL_n(A)$ generated by $E_{ij}(\lambda)$, $\lambda \in A$, is denoted by $E_n(A)$.

Definition 2.1.1 Let A be a ring. A row $[a_1, a_2, \ldots, a_n] \in A^n$ is said to be **unimodular** (of length n) if the ideal $\langle a_1, a_2, \ldots, a_n \rangle = A$. The set of unimodular rows of length n is denoted by $\mathrm{Um}_n(A)$.

A unimodular row $[a_1, a_2, \ldots, a_n]$ is said to be completable if there is a matrix in $GL_n(A)$ whose first row is $[a_1, a_2, \ldots, a_n]$.

Notation. 2.1.2 Let $[a_1, a_2, \ldots, a_n], [b_1, b_2, \ldots, b_n] \in A^n$. We write,

$$(a_1, a_2, \ldots, a_n) \overset{GL_n(A)}{\sim} (b_1, b_2, \ldots, b_n)$$

if there exists a matrix $M \in GL_n(A)$ such that

$$M \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_n \end{pmatrix}.$$

Remark 2.1.3 Let the notation be as in 2.1.2. Assume that

$$M \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_n \end{pmatrix}$$

where $M \in GL_n(A)$. It follows that $\langle b_1, b_2, \ldots, b_n \rangle \subset \langle a_1, a_2, \ldots, a_n \rangle$. Further, since

$$M^{-1} \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix}$$

it follows then that $\langle a_1, a_2, \ldots, a_n \rangle \subset \langle b_1, b_2, \ldots, b_n \rangle$. Hence if

$$(a_1, a_2, \ldots, a_n) \overset{GL_n(A)}{\sim} (b_1, b_2, \ldots, b_n),$$

then $\langle a_1, a_2, \ldots, a_n \rangle = \langle b_1, b_2, \ldots, b_n \rangle$. In particular, $GL_n(A)$ acts on the set of unimodular rows of length n.

Remark 2.1.4 It is easy to show that a unimodular row $[a_1, a_2, \ldots, a_n] \in A^n$ is completable if and only if $(a_1, a_2, \ldots, a_n) \overset{GL_n(A)}{\sim} (1, 0, \ldots, 0)$. Similarly, one can define the relations $\overset{SL_n(A)}{\sim}$ and $\overset{E_n(A)}{\sim}$. The relations $\overset{GL_n(A)}{\sim}$, $\overset{SL_n(A)}{\sim}$, $\overset{E_n(A)}{\sim}$ are equivalence relations on $\mathrm{Um}_n(A)$.

Example 2.1.5 If $[a_1, \ldots, a_n] \in \mathrm{Um}_n(A)$, then $(a_1, \ldots, a_n) \overset{E_n(A)}{\sim} (a_1 + \lambda_2 a_2, a_2, \ldots, a_n)$ and $(a_1, \ldots, a_n) \overset{E_n(A)}{\sim} (a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n, a_2, \ldots, a_n)$.

Theorem 2.1.6 *Let A be a ring and $[b_1, b_2, \ldots, b_n] \in A^n$ be a unimodular row of length n which contains a unimodular row of shorter length. Then the row $[b_1, b_2, \ldots, b_n]$ is completable. In fact; $(b_1, b_2, \ldots, b_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0)$.*

Proof. Without loss of generality we assume that the row $[b_1, b_2, \ldots, b_{n-1}]$ is unimodular. Hence we can find $a_1, a_2, \ldots, a_{n-1} \in A$ such that $1 - b_n = a_1 b_1 + \cdots + a_{n-1} b_{n-1}$ *i.e.* $a_1 b_1 + \cdots + a_{n-1} b_{n-1} + b_n = 1$. Now, the result follows from the following steps: $(b_1, b_2, \ldots, b_n) \overset{E_n(A)}{\sim} (b_1, b_2, \ldots, b_{n-1}, 1) \overset{E_n(A)}{\sim} (0, 0, \ldots, 0, 1) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0, 1) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0, 0)$. □

Remark 2.1.7 It is clear that if A is a local ring, then any unimodular row is completable. For, suppose $[a_1, a_2, \ldots, a_n] \in A^n$ is a unimodular row in a local ring $(A, \mathfrak{m})$. If none of the a_i's are units, then $\langle a_1, a_2, \ldots, a_n \rangle \subseteq \mathfrak{m}$. Hence at least one of the elements a_i is a unit. Thus, $[a_1, a_2, \ldots, a_n]$ contains a unimodular row of shorter length. Therefore, by Theorem 2.1.6, we have $(a_1, a_2, \ldots, a_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0, 0)$.

The following theorem shows that this is also true if A is a semilocal ring.

Theorem 2.1.8 *In a semilocal ring A any unimodular row $[a_1, \ldots, a_n]$ of length $n \geq 2$ is completable. In fact; $(a_1, a_2, \ldots, a_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0, 0)$.*

Proof. Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_r$ be all maximal ideals of A. Using 1.2.2, we can find $b_2, \ldots, b_n \in A$, so that the element $d = a_1 + a_2 b_2 + \cdots + a_n b_n \notin \cup_{i=1}^{r} \mathfrak{m}_i$. This implies that d is a unit in A and therefore, using 2.1.6,

$$(a_1, a_2, \ldots, a_n) \overset{E_n(A)}{\sim} (d, a_2, \ldots, a_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0).$$

Hence $[a_1, a_2, \ldots, a_n]$ is completable. □

Convention. Let A be a Noetherian ring. Then $\mathrm{ht}(A) = \infty$.

Lemma 2.1.9 *Let A be a Noetherian ring and I be an ideal generated by n elements $a_1, a_2, \ldots, a_n$ such that $\mathrm{ht}(I) \geq n$, $n \geq 1$. Then there exists $\theta \in E_n(A)$ such that*

$$(a_1, a_2, \ldots, a_n)\,\theta = (d_1, d_2, \ldots, d_n),$$

where $d_1, \ldots, d_n$ generate I and $\mathrm{ht}\langle d_1, d_2, \ldots, d_i\rangle \geq i$ for $1 \leq i \leq n$.

Proof. Since A is Noetherian, there are only finitely many minimal prime ideals of A. By hypothesis $\mathrm{ht}(I) \geq n \geq 1$, so that I is not contained in any of the minimal prime ideals of A. Therefore, by 1.2.2, we can find $b_2, \ldots, b_n$ in A such that the element $d_1 = a_1 + a_2b_2 + \cdots + a_nb_n$ does not belong to any minimal prime ideal of A. Therefore, $\mathrm{ht}\langle d_1\rangle \geq 1$. If d_1 is a unit, then by the above convention the elements $d_1, a_2, \ldots, a_n$ will serve our purpose. So we assume that d_1 is not unit.

Assume, by induction we have chosen $\sigma \in E_n(A)$ such that $(a_1, \ldots, a_n)\sigma = (g_1, \ldots, g_n)$, where $g_1, \ldots, g_n$ generate I and $\mathrm{ht}\langle g_1\rangle \geq 1, \ldots, \mathrm{ht}\langle g_1, \ldots, g_i\rangle \geq i$, $i < n$.

If $\langle g_1, \ldots, g_i\rangle = A$, then we set $d_j = g_j$ for $1 \leq j \leq n$. So, we assume that $\langle g_1, \ldots, g_i\rangle \neq A$. Let $\mathfrak{p}_{i1}, \ldots, \mathfrak{p}_{ir}$ be the minimal primes over $\langle g_1, \ldots, g_i\rangle$. By Krull's theorem $\mathrm{ht}(\mathfrak{p}_{ij}) \leq i$ for $1 \leq j \leq r$. Since $\mathrm{ht}(I) = n > i$, it follows that $I \nsubseteq \mathfrak{p}_{ij}$ for all j, $1 \leq j \leq r$. Using 1.2.2, we choose $c_1, \ldots, c_i, c_{i+2}, \ldots, c_n \in A$ such that

$$g'_{i+1} = c_1g_1 + \cdots + c_ig_i + g_{i+1} + c_{i+2}g_{i+2} + \cdots + c_ng_n \notin \cup_{j=1}^{r}\mathfrak{p}_{ij}.$$

Let $g'_j = g_j$ for $j \neq i+1$. Then $I = \langle g'_1, \ldots, g'_n\rangle$ and $\mathrm{ht}\langle g'_1, \ldots, g'_{i+1}\rangle \geq i+1$. Indeed; recall that $\mathrm{ht}\langle g'_1, \ldots, g'_i\rangle \geq i$ and if $\mathfrak{p}$ is minimal over the ideal $\langle g'_1, \ldots, g'_i\rangle$, then $g'_{i+1} \notin \mathfrak{p}$.

Let $\mathfrak{q}_{i1}, \ldots, \mathfrak{q}_{is}$ be the minimal primes over $\langle g'_1, \ldots, g'_{i+1}\rangle$. We claim that $\mathrm{ht}(\mathfrak{q}_{ij}) \geq i+1$ for $1 \leq j \leq s$. Let us assume to the contrary that $\mathrm{ht}(\mathfrak{q}_{ij}) < i+1$ for some j. Since $\langle g'_1, \ldots, g'_i\rangle \subset \mathfrak{q}_{ij}$ and by induction $\mathrm{ht}\langle g'_1, \ldots, g'_i\rangle \geq i$, we have $\mathrm{ht}(\mathfrak{q}_{ij}) = i$. We show that $\mathfrak{q}_{ij}$ is minimal over $\langle g'_1, \ldots, g'_i\rangle$. Assume to the contrary, suppose that $\mathfrak{q} \in \mathrm{Spec}(A)$ is such that $\langle g'_1, \ldots, g'_i\rangle \subset \mathfrak{q} \subsetneq \mathfrak{q}_{ij}$. Since $\mathrm{ht}\langle g'_1, \ldots, g'_i\rangle \geq i$, $\mathrm{ht}(\mathfrak{q}) \geq i$, so that $\mathrm{ht}(\mathfrak{q}_{ij}) \geq i+1$. This contradicts our assumption. Therefore, it follows that $\mathfrak{q}_{ij}$ is minimal over $\langle g'_1, \ldots, g'_i\rangle$. By construction this implies that $g'_{i+1} \notin \mathfrak{q}_{ij}$. This contradicts the fact that $\langle g'_1, \ldots, g'_{i+1}\rangle \subset \mathfrak{q}_{ij}$. Therefore, $\mathrm{ht}\langle g'_1, \ldots, g'_{i+1}\rangle \geq i+1$. Hence by induction the lemma follows. □

The proof of the following theorem follows ([16], Theorem 7.3, pg. 74).

Theorem 2.1.10 *Let A be a Noetherian ring with $\dim(A) = d$. Then for $n \geq d+2$, $E_n(A)$ acts transitively on $\mathrm{Um}_n(A)$. In other words, any unimodular row of length n over A is completable if $n \geq d+2$.*

Proof. Suppose $[a_1, a_2, \ldots, a_n] \in A^n$ is a unimodular row of length n, where $n \geq d+2$. By 2.1.9, we can find $b_1, b_2 \ldots, b_n$ in A such that $(a_1, a_2, \ldots, a_n) \overset{E_n(A)}{\sim} (b_1, b_2, \ldots, b_n)$, where $\mathrm{ht}\langle b_1, b_2, \ldots, b_i\rangle \geq i$ for $1 \leq i \leq n$. It follows that $\mathrm{ht}\langle b_1, b_2, \ldots, b_{d+1}\rangle \geq d+1$. But $\dim(A) = d$, hence $[b_1, b_2, \ldots, b_{d+1}]$ is unimodular. Thus, $[b_1, b_2, \ldots, b_n]$ contains a unimodular row of shorter length, and so by Theorem 2.1.6, $[b_1, b_2, \ldots, b_n]$ is completable. In fact; $(b_1, b_2, \ldots, b_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0)$. Hence $(a_1, a_2, \ldots, a_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0)$. This proves the theorem. □

Example 2.1.11 If $[a_1, a_2, \ldots, a_n]$ is a unimodular row with integer entries, then it follows by using the Euclidean algorithm that there exists a matrix in $\sigma \in E_n(\mathbb{Z})$ such that $(a_1, a_2, \ldots, a_n)\,\sigma = (1, 0 \ldots, 0)$.

Lemma 2.1.12 *For any ring A and for any ideal I of A the following diagram is commutative (where the maps are the natural ones):*

$$\begin{array}{ccc} M_n(A) \times A^n & \longrightarrow & M_n(A/I) \times (A/I)^n \\ \downarrow & & \downarrow \\ A^n & \longrightarrow & (A/I)^n \end{array}$$

Lemma 2.1.13 *Let A be a ring and I be an ideal of A. Then the map $E_n(A) \to E_n(A/I)$ is surjective.*

Proof. The proof follows from the fact that the generators $E_{ij}(\overline{\lambda})$ of $E_n(A/I)$ can be lifted to generators $E_{ij}(\lambda)$ of $E_n(A)$. □

Definition 2.1.14 Let A be a Noetherian ring. We define the **Jacobson radical** of A (denoted by $\mathrm{Jac}(A)$) to be the intersection of all maximal ideals of A.

The following theorem generalises 2.1.8 and 2.1.10.

Theorem 2.1.15 *Let A be a Noetherian ring and $[a_1, \ldots, a_n] \in \mathrm{Um}_n(A)$. Suppose $n \geq \dim(A/\mathrm{Jac}(A)) + 2$. Then $(a_1, \ldots, a_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0)$.*

Proof. Since $[a_1, \ldots, a_n] \in \mathrm{Um}_n(A)$, the row $[\overline{a_1}, \ldots, \overline{a_n}]$ is unimodular in $A/\mathrm{Jac}(A)$. Since $n \geq \dim(A/\mathrm{Jac}(A)) + 2$, by Theorem 2.1.10, $[\overline{a_1}, \ldots, \overline{a_n}]$ is completable. In fact; $(\overline{a_1}, \ldots, \overline{a_n}) \overset{E_n(A/\mathrm{Jac}(A))}{\sim} (\overline{1}, \overline{0}, \ldots, \overline{0})$. Then $(a_1, \ldots, a_n) \overset{E_n(A)}{\sim} (1 + c_1, c_2, \ldots, c_n)$, by 2.1.12 and 2.1.13, where $c_i \in \mathrm{Jac}(A)$. But, since $c_1 \in \mathrm{Jac}(A)$, $1 + c_1$ is unit of A. Therefore, by Theorem 2.1.6, $(1 + c_1, c_2, \ldots, c_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0)$. Hence $(a_1, \ldots, a_n) \overset{E_n(A)}{\sim} (1, 0, \ldots, 0)$. □

2.2 Horrocks' Theorem

The aim of this section is to prove the following theorem of Horrocks (*cf.* [12]). We give two proofs due to Suslin, *cf.* ([16], pgs. 87 - 90).

Theorem 2.2.1 (Horrocks) *Let $(A, \mathfrak{m})$ be a local ring and $[f_1(X), f_2(X), \ldots, f_n(X)]$ be a unimodular row in $A[X]$ with one entry monic. Then $[f_1(X), f_2(X), \ldots, f_n(X)]$ is completable.*

We need

Lemma 2.2.2 *Let k be a field and B be a ring containing k such that B is a finite dimensional k-vector space having dimension l say. Then the number of maximal ideals of $B \leq l$.*

Proof. If possible, let us assume that $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_{l+1}$ are $l+1$ distinct maximal ideals of B. Then we have

$$\mathfrak{m}_i + \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_{i-1}\mathfrak{m}_{i+1} \ldots \mathfrak{m}_{l+1} = B$$

Therefore, we can choose $c_i \in \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_{i-1}\mathfrak{m}_{i+1} \ldots \mathfrak{m}_{l+1}$ such that $c_i - 1 \in \mathfrak{m}_i$. We claim that $c_1, \ldots, c_{l+1} \in B$ are linearly independent over k. Suppose to the contrary that $\sum_{i=1}^{l+1} a_i c_i = 0$ in B, where $a_i \in k$ and not all a_i are zero. Without loss of generality

we may assume that $a_1 \neq 0$, so that $c_1 = -\sum_{i=2}^{l+1} a_1^{-1} a_i c_i$, showing that $c_1 \in \mathfrak{m}_1$. Since $c_1 - 1 \in \mathfrak{m}_1$, it follows that $1 \in \mathfrak{m}_1$, a contradiction. Therefore, the elements $c_1, \ldots, c_{l+1}$ in B are linearly independent, yielding a contradiction. Hence the lemma follows. □

Now, we give the proof of the Theorem 2.2.1.

Proof 1. Clearly, any unimodular row of length 2 is completable. Let us consider the case where $n \geq 3$. Without loss of generality we may assume that $f_1(X)$ is monic. Let $\deg(f_1(X)) = n$ and $B = A[X]/\langle f_1(X)\rangle$. Then B is finitely generated A-module, generated by the images of $1, X, \ldots, X^{n-1}$. Hence $A \hookrightarrow B$ is an integral extension. We now split the proof of the theorem into two parts.

Step 1. In this step we show that B is semilocal. First of all $\mathfrak{m}B \neq B$. This follows from Nakayama lemma, since B is finitely generated A-module. Hence $B/\mathfrak{m}B$ is a finite dimensional $A/\mathfrak{m}$-vector space. Since $A \hookrightarrow B$ is an integral extension, maximal ideals of B contract to the unique maximal ideal $\mathfrak{m}$ of A. Therefore, maximal ideals of B are in one-to-one correspondence with maximal ideals of $B/\mathfrak{m}B$. So, it suffices to show that the number of maximal ideals of $B/\mathfrak{m}B$ is finite. This follows from Lemma 2.2.2 as the number of maximal ideals of $B/\mathfrak{m}B \leq l$, where $l = \dim_{A/\mathfrak{m}} B/\mathfrak{m}B$. This proves that B is semilocal.

Step 2. By Step 1, $B = A[X]/\langle f_1(X)\rangle$ is semilocal. Since $n \geq 3$, $n - 1 \geq 2$. Let bar denote the reduction modulo $\langle f_1(X)\rangle$. Using Theorem 2.1.8, we have

$$(\overline{f_2(X)}, \ldots, \overline{f_n(X)}) \overset{E_{n-1}(B)}{\sim} (\overline{1}, \overline{0}, \ldots, \overline{0}).$$

So, there exists $\alpha \in E_{n-1}(B)$ such that

$$\alpha \begin{pmatrix} \overline{f_2(X)} \\ \overline{f_3(X)} \\ . \\ . \\ \overline{f_n(X)} \end{pmatrix} = \begin{pmatrix} \overline{1} \\ \overline{0} \\ . \\ . \\ \overline{0} \end{pmatrix}$$

where bar denotes the reduction modulo $f_1(X)$. Applying Lemma 2.1.13, to the surjective map $A[X] \to A[X]/\langle f_1(X)\rangle$, we can lift α to $\sigma \in E_{n-1}(A[X])$ and by 2.1.12 we get

$$\sigma \begin{pmatrix} f_2(X) \\ f_3(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 + f_1(X)h_1(X) \\ f_1(X)h_2(X) \\ . \\ . \\ f_1(X)h_{n-1}(X) \end{pmatrix}$$

where $h_i(X) \in A[X]$, $1 \leq i \leq n-1$. Therefore,

$$\begin{pmatrix} 1 & 0 \\ 0 & \sigma \end{pmatrix} \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} f_1(X) \\ 1 + f_1(X)h_1(X) \\ . \\ . \\ f_1(X)h_{n-1}(X) \end{pmatrix} \overset{E_n(A[X])}{\sim} \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

This completes the proof. □

Proof 2. Let $[f_1(X), \ldots, f_n(X)] \in \mathrm{Um}_n(A[X])$ with $f_1(X)$ monic and $r_2(X), \ldots, r_n(X)$ be the remainders obtained after dividing $f_2(X), \ldots, f_n(X)$ by $f_1(X)$. Then

$$(f_1(X), f_2(X), \ldots, f_n(X)) \overset{E_n(A[X])}{\sim} (f_1(X), r_2(X), \ldots, r_n(X))$$

and $\deg(r_i) < \deg(f_1)$ for $2 \leq i \leq n$. Therefore, we may assume that $\deg(f_i) < \deg(f_1)$ if $i > 1$. We split the proof into two parts.

Case 1. $\deg(f_1) = 1$. Then $f_1(X) = X - a_1$ for some $a_1 \in A$ and the unimodular row $[f_1(X), f_2(X), \ldots, f_n(X)]$ is of the form $[X - a_1, a_2, \ldots, a_n]$, where $a_2, \ldots, a_n \in A$. If $a_i \in \mathfrak{m}$ for all $i = 2, \ldots, n$, then by going modulo $\mathfrak{m}$, the row $[\overline{X - a_1}, \overline{0}, \ldots, \overline{0}]$ is unimodular in $k[X]$, where $k = A/\mathfrak{m}$. But this is a contradiction, as $\overline{X - a_1}$ is not unit of $k[X]$. Hence $a_i \notin \mathfrak{m}$ for some i, $2 \leq i \leq n$ and for that i, a_i is a unit. Therefore, the row $[X - a_1, a_2, \ldots, a_n]$ contains a unimodular row of shorter length and hence is completable by Theorem 2.1.6, showing that $[f_1(X), f_2(X), \ldots, f_n(X)]$ is completable. Therefore, the theorem is proved in this special case.

Case 2. $\deg(f_1) = l > 1$. As before we may assume $\deg(f_i) < \deg(f_1)$ for $2 \leq i \leq n$. Our aim is to transform the unimodular row to another row with one of the entries monic with degree less than $\deg(f_1)$ and appeal to induction. Since $[f_1(X), \ldots, f_n(X)]$ is a unimodular row, we have $\sum_{i=1}^{n} f_i(X)g_i(X) = 1$, where $g_i(X) \in A[X]$. If all the coefficients of each f_i for $2 \leq i \leq n$, belong to $\mathfrak{m}$, we get $\overline{f_1(X)}\,\overline{g_1(X)} = \overline{1}$ in $(A/\mathfrak{m})[X]$. This implies that $\overline{f_1(X)}$ is unit in $k[X]$, where $k = A/\mathfrak{m}$. But this is impossible as $f_1(X)$ is monic. Hence, without loss of generality, we may assume that not all coefficients of $f_2(X)$ are in $\mathfrak{m}$. We show that the ideal $\langle f_1(X), f_2(X) \rangle$ contains a monic polynomial of degree $\leq \deg(f_1) - 1$. Suppose $f_1(X) = X^l + a_{l-1}X^{l-1} + \cdots + a_0$ and $f_2(X) = b_kX^k + b_{k-1}X^{k-1} + \cdots + b_0$. Note that by assumption $\deg(f_2) < \deg(f_1)$ *i.e.* $k < l$. We define $h_1(X) = X^{l-k}f_2(X) - b_kf_1(X)$. Then $\deg(h_1) < \deg(f_1)$ and

$$h_1(X) = (b_{k-1} - a_{l-1}b_k)X^{l-1} + \text{ lower degree terms .}$$

If $b_k \notin \mathfrak{m}$, then b_k is a unit and multiplying f_2 by b_k^{-1} we obtain the required polynomial. We assume therefore that $b_k \in \mathfrak{m}$ and hence on going modulo $\mathfrak{m}$, we get $\overline{h_1(X)} = \overline{b_{k-1}X^{l-1}} + \overline{b_{k-2}X^{l-2}} + \cdots$ in $(A/\mathfrak{m})[X]$. If $b_{k-1} \notin \mathfrak{m}$, $b_{k-1} - a_{l-1}b_k \notin \mathfrak{m}$, as $b_k \in \mathfrak{m}$. Thus, in this case we have produced a polynomial $h_1(X)$ in $\langle f_1(X), f_2(X) \rangle$ such that $\deg(h_1) = \deg(f_1) - 1$ and the leading coefficient of $h_1(X)$ is a unit of A.

Otherwise, since by assumption not all coefficients of $f_2(X)$ are in $\mathfrak{m}$, let t be the smallest natural number such that $b_{k-t} \notin \mathfrak{m}$. Assume by induction that we have constructed for $i < t$ a polynomial $h_i(X) = c_{l-1}X^{l-1} + \cdots + c_0 \in \langle f_1(X), f_2(X) \rangle$ such that $\overline{h_i(X)} = \overline{b_{k-i}X^{l-1}} + \overline{b_{k-i-1}X^{l-2}} + \cdots$ in $(A/\mathfrak{m})[X]$. Note that we can start the induction for $i = 1$ as above. Having constructed $h_i(X)$ we define, $h_{i+1}(X) = Xh_i(X) - c_{l-1}f_1(X)$. Thus, if $h_{t-1}(X) = d_{l-1}X^{l-1} + \cdots + d_0$ is such that $\overline{h_{t-1}(X)} = \overline{b_{k-(t-1)}X^{l-1}} + \overline{b_{k-t}X^{l-2}} + \cdots$ in $(A/\mathfrak{m})[X]$. Then $h_t(X) = Xh_{t-1}(X) - d_{l-1}f_1(X)$. The coefficient c (say) of X^{l-1} in $h_t(X)$ is congruent to b_{k-t} modulo $\mathfrak{m}$. But, by assumption $b_{k-t} \notin \mathfrak{m}$, and hence $c^{-1}h_t(X)$ is monic of degree $l - 1$. Thus we have constructed a polynomial $h(X) = c^{-1}h_t(X)$ in $\langle f_1(X), f_2(X) \rangle$ such that $h(X)$ is monic and $\deg(h) = \deg(f_1) - 1$.

The assumption $\deg(f_i) < \deg(f_1)$ for $i > 1$ implies that $\deg(h) \geq \deg(f_3)$. If $\deg(h) > \deg(f_3)$, then $h + f_3$ is monic. Suppose $\deg(h) = \deg(f_3)$. Since f_3 is not monic (otherwise we are through), the leading coefficient of $f_3 = a$ (say), is in $\mathfrak{m}$. Hence $1 + a$ is a unit of A and $h + f_3 = (1 + a)X^{l-1} + \text{ lower degree terms .}$

Let $h(X) = g_1(X)f_1(X) + g_2(X)f_2(X)$ for some $g_1(X), g_2(X) \in A[X]$. By considering

$$\sigma = \begin{pmatrix} 1 & 0 & . & . & . & . & \\ 0 & 1 & 0 & . & . & . & . \\ g_1 & g_2 & 1 & 0 & . & . & . \\ 0 & 0 & 0 & 1 & 0 & . & . \\ . & . & . & . & . & . & 1 \end{pmatrix}$$

we get

$$\sigma \begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ . \\ . \\ f_n \end{pmatrix} = \begin{pmatrix} f_1 \\ f_2 \\ h + f_3 \\ . \\ . \\ f_n \end{pmatrix}.$$

Therefore, multiplying $h + f_3$ by $(1 + a)^{-1}$, we have produced an equivalent unimodular row to the given unimodular row with a monic entry of degree $l - 1$. Proceeding inductively we can produce an equivalent unimodular row to the given one with a monic entry of degree 1. In that case the proof follows from Case 1. Hence the theorem. □

2.3 Local-Global Principle

The aim of this section is to prove following Local-Global Principle due to D. Quillen, *cf.* [29]. The proof we give is due to Vaserstein. We follow ([17], pg. 848).

Theorem 2.3.1 (Local-Global Principle for $GL_n(A[X])$) *Suppose A is a ring and $[f_1(X), \ldots, f_n(X)]$ is a unimodular row. If*

$$(f_1(X), \ldots, f_n(X)) \overset{GL_n(A_{\mathfrak{m}}[X])}{\sim} (f_1(0), \ldots, f_n(0))$$

for all maximal ideals $\mathfrak{m}$ of A, then

$$(f_1(X), \ldots, f_n(X)) \overset{GL_n(A[X])}{\sim} (f_1(0), \ldots, f_n(0)).$$

We will prove the theorem when A is a domain.

Remark 2.3.2 In order to check that $(f_1(X), \ldots, f_n(X)) \overset{GL_n(A_{\mathfrak{m}}[X])}{\sim} (f_1(0), \ldots, f_n(0))$, it is enough to check that $(f_1(X), \ldots, f_n(X)) \overset{GL_n(A_{\mathfrak{m}}[X])}{\sim} (1, 0, \ldots, 0)$. For, we have $[f_1(0), \ldots, f_n(0)]$ is a unimodular row in a local ring $A_{\mathfrak{m}}$ and hence is elementary equivalent to $[1, 0, \ldots, 0]$ by 2.1.7.

To prove the theorem we first prove the following lemma.

Lemma 2.3.3 *Let A be an integral domain, S a multiplicative closed subset of A. If*

$$(f_1(X), \ldots, f_n(X)) \overset{GL_n(S^{-1}A[X])}{\sim} (f_1(0), \ldots, f_n(0))$$

then there exists $c \in S$ such that

$$(f_1(X + cY), \ldots, f_n(X + cY)) \overset{GL_n(A[X,Y])}{\sim} (f_1(X), \ldots, f_n(X)).$$

Proof. Let $f(X) = [f_1(X), \ldots, f_n(X)]$ and $f(0) = [f_1(0), \ldots, f_n(0)]$. By hypothesis it follows that there exists a matrix, say $\sigma(X)$, in $GL_n(S^{-1}A[X])$ such that $f(X) = \sigma(X)f(0)$. Therefore, $f(0) = \sigma(X)^{-1}f(X)$ is constant and hence invariant under the translation $X \mapsto X+Y$, *i.e.* $\sigma(X)^{-1}f(X) = \sigma(X+Y)^{-1}f(X+Y) = f(0)$. Let $\tau(X, Y) = \sigma(X)\sigma(X + Y)^{-1}$. Then

$$\tau(X, Y)f(X + Y) = \sigma(X)\sigma(X + Y)^{-1}f(X + Y) = \sigma(X)f(0) = f(X).$$

Since $\tau(X,0) = I_n$, we can find $c \in S$ such that $\tau(X,cY) \in M_n(A[X,Y])$. Further, as $\det(\sigma(X))$ is a unit of $S^{-1}A$ (since $\sigma(X) \in GL_n(S^{-1}A[X])$), we get $\det(\sigma(X)) = \det(\sigma(X+cY))$. Therefore, $\det(\tau(X,cY)) = \det(\sigma(X))\det(\sigma(X+cY)^{-1}) = 1$. This implies that $\tau(X,cY) \in SL_n(A[X,Y])$ and

$$\tau(X,cY)f(X+cY) = \sigma(X)\sigma(X+cY)^{-1}f(X+cY) = \sigma(X)f(0) = f(X).$$

This completes the proof. □

Proof of Theorem 2.3.1. Let $f(X)$ be as above and

$$J = \{c \in A \,|\, (f_1(X+cY),\ldots,f_n(X+cY)) \overset{GL_n(A[X,Y])}{\sim} (f_1(X),\ldots,f_n(X))\}.$$

We first show that J is an ideal.

Let $c_1, c_2 \in J$. Then there exist matrices $\sigma_1(X,Y)$ and $\sigma_2(X,Y)$ in $GL_n(A[X,Y])$ such that $\sigma_1(X,Y)f(X+c_1Y) = f(X)$ and $\sigma_2(X,Y)f(X+c_2Y) = f(X)$. Hence we get $\sigma_2(X+c_1Y,Y)f(X+(c_1+c_2)Y) = f(X+c_1Y)$. This gives

$$(f_1(X+(c_1+c_2)Y),\ldots,f_n(X+(c_1+c_2)Y) \overset{GL_n(A[X,Y])}{\sim} (f_1(X),\ldots,f_n(X)).$$

Therefore, $c_1+c_2 \in J$. Similarly, if $c \in J$ and $\lambda \in A$ by considering the substitutions $X \mapsto X$ and $Y \mapsto \lambda Y$ it follows that $c\lambda \in J$ and hence J is an ideal.

We claim that $J = A$. Suppose not, then $J \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of A. By hypothesis, $(f_1(X),\ldots,f_n(X)) \overset{GL_n(A_{\mathfrak{m}}[X])}{\sim} (f_1(0),\ldots,f_n(0))$, so by Lemma 2.3.3, there exists $c \in S = A - \mathfrak{m}$ such that

$$(f_1(X+cY),\ldots,f_n(X+cY)) \overset{GL_n(A[X,Y])}{\sim} (f_1(X),\ldots,f_n(X)).$$

This implies that $c \in J$, but $c \notin \mathfrak{m}$. This is a contradiction and hence the claim. Now, since $1 \in J$, we have $(f_1(X+Y),\ldots,f_n(X+Y)) \overset{GL_n(A[X,Y])}{\sim} (f_1(X),\ldots,f_n(X))$. So there exists $\sigma(X,Y) \in GL_n(A[X,Y])$ such that

$$\sigma(X,Y)\begin{pmatrix} f_1(X+Y) \\ f_2(X+Y) \\ . \\ . \\ f_n(X+Y) \end{pmatrix} = \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix}.$$

Let us consider the homomorphism $\psi : A[X,Y] \to A[Y]$, sending $X \to 0$ and $Y \to Y$. Then we obtain a matrix $\sigma(0,Y) \in GL_n(A[Y]) \subset GL_n(A[X,Y])$ such that

$$\sigma(0,Y)\begin{pmatrix} f_1(Y) \\ f_2(Y) \\ . \\ . \\ f_n(Y) \end{pmatrix} = \begin{pmatrix} f_1(0) \\ f_2(0) \\ . \\ . \\ f_n(0) \end{pmatrix}.$$

Replacing Y by X it follows that $(f_1(X),\ldots,f_n(X)) \overset{GL_n(A[X])}{\sim} (f_1(0),\ldots,f_n(0))$. □

2.4 Generalisation of Horrocks' Theorem

The aim of this section is to prove the following generalisation due to Quillen (*cf.*[29]) and Suslin (*cf.*[39]) of Horrocks theorem. We give two proofs one following Ravi Rao (*cf.*[31]) and another proof using a trick of Mandal.

Theorem 2.4.1 (Quillen-Suslin) *Let A be a domain and $[f_1(X), \ldots, f_n(X)]$ be a unimodular row in $A[X]$ with one entry, say $f_1(X)$, monic. Then the row $[f_1(X), \ldots, f_n(X)]$ is completable.*

Proof. We write

$$\begin{array}{lllll} f_1(X) = X^{r_1} + a_{1r_1-1}X^{r_1-1} + \cdots + a_{10} & & & & \\ f_2(X) = a_{2r_2}X^{r_2} + a_{2(r_2-1)}X^{r_2-1} + \cdots + a_{20} & & & & \\ \cdots \quad \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots \quad \cdots & \cdots & \cdots & \cdots & \cdots \\ f_n(X) = a_{nr_n}X^{r_n} + a_{n(r_n-1)}X^{r_n-1} + \cdots + a_{n0}. & & & & \end{array}$$

Now, consider polynomials $g_1, \ldots, g_n$ defined as follows:

$$\begin{array}{lll} g_1(X) = a_{10}X^{r_1} + a_{11}X^{r_1-1} + \cdots + 1 & & \\ g_2(X) = a_{20}X^{r_2} + a_{21}X^{r_2-1} + \cdots + a_{2r_2} & & \\ \cdots \quad \cdots & \cdots & \\ \cdots \quad \cdots & \cdots & \\ g_n(X) = a_{n0}X^{r_n} + a_{n1}X^{r_n-1} + \cdots + a_{nr_n}. & & \end{array}$$

We claim that the new row $[g_1(X), \ldots, g_n(X)]$ is unimodular in $A[X]$. To prove the claim let us first show that, $[g_1(X), \ldots, g_n(X)] \in \mathrm{Um}_n(A[X, X^{-1}])$. By hypothesis, $[f_1(X), \ldots, f_n(X)] \in \mathrm{Um}_n(A[X])$. Hence $[f_1(X^{-1}), \ldots, f_n(X^{-1})] \in \mathrm{Um}_n(A[X^{-1}])$. Further, $f_i(X^{-1}) = X^{-\deg(f_i)}g_i(X)$ for all $i,\ 1 \leq i \leq n$. So

$$[X^{-\deg(f_1)}g_1(X), \ldots, X^{-\deg(f_n)}g_n(X)] \in \mathrm{Um}_n(A[X^{-1}]).$$

Thus, there exist $h_1(X), \ldots, h_n(X) \in A[X]$ such that $\sum_{i=1}^{n} X^{-\deg(f_i)}g_i(X)h_i(X^{-1}) = 1$. Multiplying both sides by X^d, for sufficiently large d, we get $X^d \in \langle g_1(X), \ldots, g_n(X)\rangle$. Now, if $\langle g_1(X), \ldots, g_n(X)\rangle \neq A[X]$ then there exists some maximal ideal $\mathfrak{M}$ of $A[X]$ such that, $\langle g_1(X), \ldots, g_n(X)\rangle \subseteq \mathfrak{M}$. Since $X^d \in \mathfrak{M}$, $X \in \mathfrak{M}$ and since $g_1(0) = 1$, $1 \in \mathfrak{M}$. This is a contradiction. Hence $[g_1(X), \ldots, g_n(X)] \in \mathrm{Um}_n(A[X])$. Since the row $[f_1(X), \ldots, f_n(X)]$ is unimodular, setting $X = 0$, it follows that $\langle a_{10}, \ldots, a_{n0}\rangle = A$. Let $\mathfrak{m}$ be a maximal ideal of A. Then at least one of the $a_{i0}\,(1 \leq i \leq n)$ is not in $\mathfrak{m}$ and for that i, $g_i(X)$ has leading coefficient a unit of $A_{\mathfrak{m}}$. So localising at $\mathfrak{m}$ and applying Horrocks' theorem we have $(g_1(X), \ldots, g_n(X)) \overset{GL_n(A_{\mathfrak{m}}[X])}{\sim} (1, 0, \ldots, 0)$ for all maximal ideals $\mathfrak{m}$ of A. Hence by Quillen's Local-Global Principle we have $(g_1(X), \ldots, g_n(X)) \overset{GL_n(A[X])}{\sim} (g_1(0), \ldots, g_n(0))$. But, $g_1(0) = 1$, so by Theorem 2.1.6, $(g_1(0), \ldots, g_n(0)) \overset{GL_n(A)}{\sim} (1, 0, \ldots, 0)$, hence $(g_1(X), \ldots, g_n(X)) \overset{GL_n(A[X])}{\sim} (1, 0, \ldots, 0)$. Setting $X = 1$, we get $(g_1(1), \ldots, g_n(1)) \overset{GL_n(A)}{\sim} (1, 0, \ldots, 0)$. Again by applying Horrocks' theorem we have $(f_1(X), \ldots, f_n(X)) \overset{GL_n(A_{\mathfrak{m}}[X])}{\sim} (1, 0, \ldots, 0)$ for all maximal ideals $\mathfrak{m}$ of A and hence by Quillen's Local-Global Principle

$$(f_1(X), \ldots, f_n(X)) \overset{GL_n(A[X])}{\sim} (f_1(0), \ldots, f_n(0)).$$

In particular, setting $X = 1$, $(f_1(1), \ldots, f_n(1)) \overset{GL_n(A)}{\sim} (f_1(0), \ldots, f_n(0))$. Combining these it follows that,

$$\begin{aligned}(f_1(X), \ldots, f_n(X)) &\overset{GL_n(A[X])}{\sim} (f_1(0), \ldots, f_n(0)) \\ &\overset{GL_n(A[X])}{\sim} (f_1(1), \ldots, f_n(1)) = (g_1(1), \ldots, g_n(1)) \\ &\overset{GL_n(A[X])}{\sim} (1, 0, \ldots. \ldots \ldots, 0).\end{aligned}$$

Hence $[f_1(X), \ldots, f_n(X)]$ is completable. This completes the proof. □

The following proof is based on a trick of Mandal, *cf.* ([18], Remark 1.3).

Proof 2. Let $[f_1(X), \ldots, f_n(X)] \in \mathrm{Um}_n(A[X])$ with $f_1(X)$ monic. We define polynomials $h_i(X, T)$ as follows: $h_i(X, T) = T^{\deg(f_i)} f_i(X - T + T^{-1})$. It then follows that for $f_1(X) = X^r + a_1 X^{r-1} + \cdots + a_r$,

$$T^r f_1(X - T + T^{-1}) = (TX - T^2 + 1)^r + a_1 T(TX - T^2 + 1)^{r-1} + \cdots + a_r T^r.$$

i.e., $h_i(X, T)$ is monic in T and $h_1(X, 0) = 1$. We claim that $[h_1(X, T), \ldots, h_n(X, T)] \in \mathrm{Um}_n(A[X, T, T^{-1}])$.

By hypothesis, there exist $g_1(X), \ldots, g_n(X) \in A[X]$ such that $\sum_{i=1}^n f_i(X) g_i(X) = 1$. Hence we have $\sum_{i=1}^n f_i(X - T + T^{-1}) g_i(X - T + T^{-1}) = 1$. This implies that

$$\sum_{i=1}^{n} T^{-\deg(f_i)} h_i(X, T) g_i(X - T + T^{-1}) = 1. \tag{8}$$

This proves the claim. Now, we show that $I = \langle h_1(X, T), \ldots, h_n(X, T) \rangle = A[X, T]$. For, if $I \neq A[X, T]$, then $I \subset \mathfrak{M}$ for some maximal ideal $\mathfrak{M}$ of $A[X, T]$. Multiplying equation (8) by large power of T we get, $T^s \in \mathfrak{M}$ for some natural number $s > 0$, hence $T \in \mathfrak{M}$. But $h_1(X, 0) = 1$, so that $1 \in \mathfrak{M}$, a contradiction.

Now take $B = A[X]$. Since $h_1(X, T)$ is monic in T, by Horrocks' theorem

$$(h_1(X, T), \ldots, h_n(X, T)) \overset{GL_n(B_{\mathfrak{m}}[T])}{\sim} (1, 0, \ldots, 0)$$

for every maximal ideals $\mathfrak{m}$ of B. Therefore, by Quillen's Local-Global Principle

$$(h_1(X, T), \ldots, h_n(X, T)) \overset{GL_n(B[T])}{\sim} (h_1(X, 0), \ldots, h_n(X, 0)).$$

In particular, $(h_1(X, 1), \ldots, h_n(X, 1)) \overset{GL_n(B)}{\sim} (h_1(X, 0), \ldots, h_n(X, 0))$. As $h_1(X, 0) = 1$, it follows that $[h_1(X, 0), \ldots, h_n(X, 0)]$ contains a unimodular row of shorter length and hence by Theorem 2.1.6, $(h_1(X, 0), \ldots, h_n(X, 0)) \overset{E_n(B)}{\sim} (1, 0, \ldots, 0)$. Therefore, we have

$$\begin{aligned}(f_1(X), \ldots, f_n(X)) &= (h_1(X, 1), \ldots, h_n(X, 1)) \\ &\overset{GL_n(B)}{\sim} (h_1(X, 0), \ldots, h_n(X, 0)) \\ &\overset{E_n(B)}{\sim} (1, 0, \ldots, 0).\end{aligned}$$

This completes the proof. □

Corollary 2.4.2 (Quillen-Suslin). *Let k be a field and $A = k[X_1, \ldots, X_d]$. Then any unimodular row of length n over A is completable.*

Proof. The proof follows from 1.10.3 and 2.4.1.

Remark 2.4.3 The following principle is implicitly used in the proof of 2.4.1. Let A be ring. If $[f_1(X), \ldots, f_n(X)] \in \mathrm{Um}_n(A[X])$ and suppose $(f_1(X), \ldots, f_n(X)) \overset{GL_n(A[X])}{\sim} (f_1(0), \ldots, f_n(0))$. Then for any specialisation $X \mapsto a \in A$ $(f_1(a), \ldots, f_n(a)) \overset{GL_n(A)}{\sim} (f_1(0), \ldots, f_n(0))$. Hence $(f_1(X), \ldots, f_n(X)) \overset{GL_n(A[X])}{\sim} (f_1(a), \ldots, f_n(a))$ for every $a \in A$.

2.5 A Theorem of Suslin

The aim of this section is to apply Quillen's local-global principle to give a partial proof (assuming 2.5.4) of the following theorem of Suslin, *cf.* [39].

Theorem 2.5.1 *Let A be a ring, $[a_0, \ldots, a_n] \in \mathrm{Um}_{n+1}(A)$. Then the row $[a_0^{r_0}, \ldots, a_n^{r_n}]$ is completable if $n! \mid r_0 \cdots r_n$, where $r_0, \ldots, r_n$ are natural numbers.*

The following lemma is based on an unpublished remark of Mohan Kumar.

Lemma 2.5.2 *Let A be a local domain, $[a_0, \ldots, a_n] \in \mathrm{Um}_{n+1}(A)$ and $r > 0$ an integer. Then $[a_0^r, a_1 + a_0X, a_2, \ldots, a_n] \in \mathrm{Um}_n(A[X])$ and $(a_0^r, a_1 + a_0X, a_2, \ldots, a_n) \overset{GL_{n+1}(A[X])}{\sim} (1, 0, \ldots, 0)$.*

Proof. It is easy to check that $[a_0^r, a_1 + a_0X, a_2, \ldots, a_n] \in \mathrm{Um}_{n+1}(A[X])$. If $a_i \notin \mathfrak{m}$ for some $i \in \{0, 2, 3, \ldots, n\}$, then by Theorem 2.1.6, the row $[a_0^r, a_1 + a_0X, a_2, \ldots, a_n]$ is completable and the lemma is true in this case. So we assume that $a_i \in \mathfrak{m}$ for all $i \in \{0, 2, 3, \ldots, n\}$. Since $[a_0^r, a_1, a_2, \ldots, a_n]$ is a unimodular row, it follows that a_1 is a unit of A. Hence $[a_0^r, a_1 + a_0X] \in \mathrm{Um}_2(A[X])$ (since any maximal ideal of $A[X]$ containing $\langle a_0^r, a_1 + a_0X \rangle$ has to contain a_1, which is a unit). Therefore, the unimodular row $[a_0^r, a_1 + a_0X, a_2, \ldots, a_n]$ contains a unimodular row of shorter length and hence $(a_0^r, a_1 + a_0X, a_2, \ldots, a_n) \overset{GL_{n+1}(A[X])}{\sim} (1, 0, \ldots, 0)$. □

Lemma 2.5.3 *Let A be a domain, $r > 0$ a natural number and $[a_0, a_1, \ldots, a_n]$ a unimodular row of length $n + 1$. Then, there exists $\alpha \in GL_{n+1}(A)$ such that*

$$(a_0^r, a_1, \ldots, a_n)\alpha = (a_0, a_1^r, \ldots, a_n).$$

Proof. By 2.5.2, we can apply Quillen's localization theorem to the unimodular row $[a_0^r, a_1 + a_0X, a_2, \ldots, a_n]$. Setting $X = 0$ and $X = -1$, we obtain

$$(a_0^r, a_1, a_2, \ldots, a_n) \overset{GL_{n+1}(A)}{\sim} (a_0^r, a_1 - a_0, a_2, \ldots, a_n).$$

Moreover, $a_1^r - a_0^r = \lambda(a_1 - a_0)$ for some $\lambda \in A$, *i.e* $a_1^r = a_0^r + \lambda(a_1 - a_0)$, so that

$$(a_0^r, a_1 - a_0, a_2, \ldots, a_n) \overset{E_{n+1}(A)}{\sim} (a_1^r, a_1 - a_0, a_2, \ldots, a_n).$$

Hence $(a_0^r, a_1, a_2, \ldots, a_n) \overset{GL_{n+1}(A)}{\sim} (a_1^r, a_1 - a_0, a_2, \ldots, a_n)$. Now, repeating the above process with unimodular row $[a_1^r, a_1 - a_0, a_2, \ldots, a_n]$, we get $(a_1^r, a_1 - a_0, a_2, \ldots, a_n) \overset{GL_{n+1}(A)}{\sim} (a_1^r, a_1 - a_0 - a_1, a_2, \ldots, a_n) = (a_1^r, -a_0, a_2, \ldots, a_n)$. Hence $(a_0^r, a_1, a_2, \ldots, a_n) \overset{GL_{n+1}(A)}{\sim} (a_1^r, -a_0, a_2, \ldots, a_n)$. *i.e.* $(a_0^r, a_1, a_2, \ldots, a_n) \overset{GL_{n+1}(A)}{\sim} (a_0, a_1^r, a_2, \ldots, a_n)$. □

Theorem 2.5.4 (Suslin). (*cf.* [39]) *Let A be a domain and $[a_0, \ldots, a_n] \in \mathrm{Um}_{n+1}(A)$. Then the row $[a_0, a_1, a_2^2 \ldots, a_n^n]$ is completable.*

Corollary 2.5.5 *Let A be a domain and $[a_0, a_1, a_2, \ldots, a_n] \in \mathrm{Um}_{n+1}(A)$. Then the row $[a_0, a_1, a_2, \ldots, a_{n-1}, a_n^{n!}]$ is completable.*

Proof. The proof follows from 2.5.4 and 2.5.3. □

Proof of Theorem 2.5.1. The proof follows from 2.5.3 and 2.5.5. □

2.6 Quillen's Decomposition

The aim of this section is to prove a splitting lemma of Quillen (*cf.* [29]) and deduce some consequences which will be used later. We follow the proof given in [11].

Let A be a domain and s be a non zero element of A. Suppose $\sigma(X) \in GL_n(A_s[X])$ is such that $\sigma(0) = I_n$. Then there exists a positive integer N such that for all $n_1 \geq N$ and for all $\lambda \in A$, $\sigma(\lambda s^{n_1} X) \in M_n(A[X])$. Further, $\det(\sigma(X))$ is a unit of $A[X]$ and hence unit of A. Therefore, $\det(\sigma(X)) = \det(\sigma(0)) = 1$. Hence $\det(\sigma(\lambda s^{n_1} X)) = 1$ and therefore, $\sigma(\lambda s^{n_1} X) \in GL_n(A[X])$.

Lemma 2.6.1 (Quillen) *Let A be a domain and $s, t \in A$ be such that $sA + tA = A$. Suppose there exists $\sigma(X) \in GL_n(A_{st}[X])$ with the property that $\sigma(0) = I_n$. Then there exists $\psi_1(X) \in GL_n(A_s[X])$ with $\psi_1(0) = I_n$ and $\psi_2(X) \in GL_n(A_t[X])$ with $\psi_2(0) = I_n$ such that $\sigma(X) = (\psi_1(X))_t(\psi_2(X))_s$.*

(Here $(\psi_1(X))_t$ is the image of $\psi_1(X)$ in $GL_n(A_{st}[X])$ and $(\psi_2(X))_s$ is the image of $\psi_2(X)$ in $GL_n(A_{st}[X])$.)

Proof. Since $\sigma(0) = I_n$, $\sigma(X) = I_n + X\tau(X)$, where $\tau(X) \in M_n(A_{st}[X])$. So, we can choose a large integer N_1 such that $\sigma(\lambda s^k X) \in GL_n(A_t[X])$ for all $\lambda \in A$ and for all $k \geq N_1$. We define a matrix $\beta(X, Y, Z) \in GL_n(A_{st}[X, Y, Z])$ as follows:

$$\beta(X, Y, Z) = \sigma((Y + Z)X)\sigma(YX)^{-1}. \tag{9}$$

Then $\beta(X, Y, 0) = I_n$, and hence there exists large integer N_2 such that for all $k \geq N_2$ and for all $\mu \in A$ we have $\beta(X, Y, \mu t^k Z) \in GL_n(A_s[X, Y, Z])$. That means,

$$\beta(X, Y, \mu t^k Z) = (\sigma_1(X, Y, Z))_t, \tag{10}$$

where $\sigma_1(X, Y, Z) \in GL_n(A_s[X, Y, Z])$ with $\sigma_1(X, Y, 0) = I_n$.

Let $N = \max(N_1, N_2)$. By hypothesis, it follows that $\langle s^N \rangle + \langle t^N \rangle = 1$. Thus, there exist $\lambda, \mu \in A$ such that $\lambda s^N + \mu t^N = 1$. Setting $Y = \lambda s^N$, $Z = \mu t^N$, we get from (9), $\beta(X, \lambda s^N, \mu t^N) = \sigma(X)\sigma(\lambda s^N X)^{-1}$. Setting $Z = 1$, $Y = \lambda s^N$ in (10), we get $\beta(X, \lambda s^N, \mu t^N) = (\sigma_1(X, \lambda s^N, \mu t^N))_t = (\psi_1(X))_t$, where $\psi_1(X) \in GL_n(A_s[X])$. Therefore, $\sigma(X)\sigma(\lambda s^N X)^{-1} = (\psi_1(X))_t$. Let $\sigma(\lambda s^N X) = (\psi_2(X))_s$, where $\psi_2(X) \in GL_n(A_t[X])$. Since $\sigma(0) = I_n$, $\psi_1(0) = \psi_2(0) = I_n$. Now, the result follows by using the identity, $\sigma(X) = \sigma(X)\sigma(\lambda s^N X)^{-1}\sigma(\lambda s^N X)$. □

Remark 2.6.2 Let the notation be as in 2.6.1 By interchanging the roles of s and t we can write $\sigma(X) = (\tau_1(X))_s(\tau_2(X))_t$, where $\tau_1(X) \in GL_n(A_t[X])$ with $\tau_1(0) = \mathrm{Id}$ and $\tau_2(X) \in GL_n(A_s[X])$ with $\tau_2(0) = \mathrm{Id}$.

Definition 2.6.3 Any two matrices α and β in $GL_n(A)$ are said to be **connected** if there exists $\sigma(X) \in GL_n(A[X])$ such that $\sigma(0) = \alpha$ and $\sigma(1) = \beta$. By considering the matrix $\sigma(1 - X)$, it follows that if α is connected to β, then β is connected to α.

Lemma 2.6.4 *Let A be a ring. Then any matrix in $E_n(A)$ can be connected to the identity matrix.*

Proof. Let $\alpha \in E_n(A)$ be any matrix. Then, $\alpha = \Pi_{i=1}^r E_{ij}(\lambda)$. We define $\sigma(X) = \Pi_{i=1}^r E_{ij}(\lambda X)$. Then $\sigma(X) \in GL_n(A[X])$, $\sigma(0) = I_n$ and $\sigma(1) = \alpha$. This proves the lemma. □

Corollary 2.6.5 *Let A be a domain, $s, t \in A$ be such that $sA + tA = A$ and $\tau \in GL_n(A_{st})$ be such that τ can be connected to the identity matrix. Then $\tau = \tau_1\tau_2$ for some $\tau_1 \in GL_n(A_s)$ and $\tau_2 \in GL_n(A_t)$.*

Proof. The proof follows by applying 2.6.1, and setting $X = 1$.

Lemma 2.6.6 *Let A be a domain. If $\sigma_1 \in E_n(A_s)$, $\sigma_2 \in E_n(A_t)$, then $\sigma_1\sigma_2 = \beta_1\beta_2$, where $\beta_1 \in GL_n(A_t)$ and $\beta_2 \in GL_n(A_s)$.*

Proof. Since $\sigma_1\sigma_2 \in E_n(A_{st})$, there exists $\alpha(X) \in GL_n(A_{st}[X])$ such that $\alpha(0) = I_n$ and $\alpha(1) = \sigma_1\sigma_2$. By remark 2.6.2, $\alpha(X) = \delta_1(X)\delta_2(X)$, where $\delta_1(X) \in GL_n(A_t[X])$ and $\delta_2(X) \in GL_n(A_s[X])$. Setting $X = 1$, we get $\sigma_1\sigma_2 = \beta_1\beta_2$, where $\beta_1 = \delta_1(1)$ and $\beta_2 = \delta_2(1)$. This proves the lemma. □

Lemma 2.6.7 *Let A be a domain. If $\sigma_1 \in GL_n(A_s), \sigma_2 \in E_n(A_t)$, then $\sigma_1\sigma_2 = \beta_1\beta_2$, where $\beta_1 \in GL_n(A_t)$ and $\beta_2 \in GL_n(A_s)$.*

Proof. We can write $\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1^{-1}\sigma_1$. Therefore, it suffices to show that $\sigma_1\sigma_2\sigma_1^{-1} = \gamma_1\gamma_2$, where $\gamma_1 \in GL_n(A_t)$ and $\gamma_2 \in Gl_n(A_s)$. Then the result follows by setting $\beta_1 = \gamma_1, \beta_2 = \gamma_2\sigma_1$. Since any elementary matrix can be connected to the identity matrix, we can find $\alpha(X) \in GL_n(A_t[X])$ such that $\alpha(0) = I_n$ and $\alpha(1) = \sigma_2$. Let $\delta(X) = \sigma_1\alpha(X)\sigma_1^{-1}$. Then $\delta(1) = \sigma_1\sigma_2\sigma_1^{-1}$. Since $\delta(X) \in GL_n(A_{st}[X])$ and $\delta(0) = I_n$, by 2.6.2, $\delta(X) = \delta_1(X)\delta_2(X)$, where $\delta_1(X) \in GL_n(A_t[X])$ and $\delta_2(X) \in GL_n(A_s[X])$. Let $\gamma_1 = \delta_1(1)$ and $\gamma_2 = \delta_2(1)$. Now, the lemma follows. □

Remark 2.6.8 Proceeding similarly one can prove that if $\sigma_1 \in E_n(A_s)$ and $\sigma_2 \in GL_n(A_t)$, then $\sigma_1\sigma_2 = \beta_1\beta_2$, where $\beta_1 \in GL_n(A_t)$ and $\beta_2 \in GL_n(A_s)$.

2.7 On a Theorem of Ravi.A.Rao

In this section we prove a weaker version of the following theorem of Ravi.A.Rao. For details see [31].

Theorem 2.7.1 *Let A be a ring and $[f_1(X), \ldots, f_n(X)]$ be a unimodular row in $A[X]$ with $f_1(X)$ monic. Then if $n \geq 3$, there exists an elementary matrix which transforms $(f_1(X), \ldots, f_n(X))^t$ to $(1, 0, \ldots, 0)^t$.*

Proof. *cf.* [31].

In view of Lemma 2.6.4, the following theorem is a special case of Ravi's Theorem.

Theorem 2.7.2 *Let A be a domain and $[f_1(X), \ldots, f_n(X)] \in \mathrm{Um}_n(A[X])$ with $f_1(X)$ monic. Then there exists a matrix $\alpha(X, W) \in GL_n(A[X, W])$ such that $\alpha(X, 0) = I_n$ and*

$$\alpha(X,1)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

i.e. we can find a matrix which can be connected to the identity matrix taking the column $(f_1, f_2, \ldots, f_n)^t$ to $(1, 0, \ldots, 0)^t$.

Proof. Case 1. Suppose

$$(f_1(0), \ldots, f_n(0)) = (1, 0, \ldots, 0). \tag{11}$$

By 2.4.1 there exists $\beta(X) \in GL_n(A[X])$ such that

$$\beta(X) \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

So, we have following:

$$\beta(0) \begin{pmatrix} f_1(0) \\ f_2(0) \\ . \\ . \\ f_n(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}$$

$$\Rightarrow \beta(0) \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix} \text{ (using (11))}$$

$$\Rightarrow \beta(0)^{-1}\beta(X) \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Let $\sigma(X) = \beta(0)^{-1}\beta(X)$. Then $\sigma(0) = I_n$ and

$$\sigma(X) \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}$$

We set $\alpha(X, W) = \sigma(XW)$, proving the result in this case.

Case 2. To establish the result in general we apply the trick of Mandal used earlier. We introduce a new variable T and consider the ring $A[X, T, T^{-1}]$. Let

$$h_1(X, T) = T^{\deg(f_1)} f_1(X - T + T^{-1})$$

$$h_i(X, T) = T^{\deg(f_i)+1} f_i(X - T + T^{-1})$$

for $i = 2, \ldots, n$. Then as in 2.4.1, we get (1) $h_1(X, T)$ is monic in T and $h_1(X, 0) = 1$, (2) $[h_1(X, T), \ldots, h_n(X, T)] \in \mathrm{Um}_n(R[X, T])$, (3) $h_i(X, 0) = 0$ for $i > 1$ and (4) $h_i(X, 1) = f_i(X)$.

Therefore, $[h_1(X,0),\ldots,h_n(X,0)] = [1,0,\ldots,0]$ and hence by Case 1, there exists $\beta(X,T,W) \in GL_n(A[X,T,W])$ such that $\beta(X,T,0) = I_n$ and

$$\beta(X,T,1)\begin{pmatrix} h_1(X,T) \\ h_2(X,T) \\ . \\ . \\ h_n(X,T) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Let $\alpha(X,W) = \beta(X,1,W)$. Then $\alpha(X,0) = \beta(X,1,0) = I_n$. Since $\alpha(X,1) = \beta(X,1,1)$ and $h_i(X,1) = f_i(X)$ for $1 \leq i \leq n$, we have

$$\alpha(X,1)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

This completes the proof of the theorem. □

Lemma 2.7.3 *Let $[f_1(X), f_2(X)] \in \mathrm{Um}_2(A[X])$. Then there exists a matrix $\tau(X) \in GL_2(A[X])$ such that $\tau(0) = I_2$ and*

$$\tau(X)\begin{pmatrix} f_1(X) \\ f_2(X) \end{pmatrix} = \begin{pmatrix} f_1(0) \\ f_2(0) \end{pmatrix}.$$

Proof. Since any row of length 2 is completable, there exists a matrix $\sigma(X) \in GL_2(A[X])$ such that

$$\sigma(X)\begin{pmatrix} f_1(X) \\ f_2(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Hence

$$\sigma(0)\begin{pmatrix} f_1(0) \\ f_2(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Therefore,

$$\sigma(0)^{-1}\sigma(X)\begin{pmatrix} f_1(X) \\ f_2(X) \end{pmatrix} = \begin{pmatrix} f_1(0) \\ f_2(0) \end{pmatrix}.$$

Setting $\tau(X) = \sigma(0)^{-1}\sigma(X)$, the lemma follows. □

Lemma 2.7.4 *Let A be a ring and $[f_1(X),\ldots,f_n(X)] \in \mathrm{Um}_n(A[X])$ with $f_1(X)$ monic. Then there exists a matrix $\tau(X) \in GL_n(A[X])$ such that $\tau(0) = I_n$ and*

$$\tau(X)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} f_1(0) \\ f_2(0) \\ . \\ . \\ f_n(0) \end{pmatrix}.$$

Proof. Since $f_1(X)$ is monic, by Horrocks' theorem and Quillen's localisation theorem there exists $\sigma(X) \in GL_n(A[X])$ such that

$$\sigma(X)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} f_1(0) \\ f_2(0) \\ . \\ . \\ f_n(0) \end{pmatrix}.$$

Hence

$$\sigma(0)^{-1}\sigma(X)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \sigma(0)^{-1}\begin{pmatrix} f_1(0) \\ f_2(0) \\ . \\ . \\ f_n(0) \end{pmatrix} = \begin{pmatrix} f_1(0) \\ f_2(0) \\ . \\ . \\ f_n(0) \end{pmatrix}.$$

Setting $\tau(X) = \sigma(0)^{-1}\sigma(X)$, the lemma follows. □

2.8 Suslin's Monic Polynomial Theorem

The aim of this section is to prove a simpler version 2.8.4 of Suslin's monic polynomial theorem, *cf.* ([16], pg. 93).

Lemma 2.8.1 *Let A be a Noetherian ring with $\dim(A) = d$. Suppose $\mathfrak{M}$ is a maximal ideal of $A[X]$ such that $\mathrm{ht}(\mathfrak{M}) = d+1$. Then $\mathfrak{M} \cap A$ is also a maximal ideal of A.*

Proof. From Lemma 1.8.3, it follows that $\mathrm{ht}(\mathfrak{M} \cap A) \geq d$. But, as $\dim(A) = d$, $\mathrm{ht}(\mathfrak{M} \cap A) = d$ and hence $\mathfrak{M} \cap A$ is a maximal ideal of A. □

Lemma 2.8.2 *Let A be a Noetherian ring, $\mathfrak{M} \subset A[X]$ a maximal ideal of height $d+1$. Then $\mathfrak{M}$ contains a monic polynomial.*

Proof. Suppose $\mathfrak{M} \cap A = \mathfrak{m}$. It follows from Lemma 2.8.1 that $\mathfrak{m}$ is maximal ideal in A. The isomorphism

$$\frac{A[X]}{\mathfrak{m}A[X]} \cong \frac{A}{\mathfrak{m}}[X]$$

implies that the ideal $\mathfrak{m}A[X]$ of $A[X]$ is not maximal. Note that $\mathfrak{M}$ contains $\mathfrak{m}A[X]$. Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial of smallest degree in $\mathfrak{M} - \mathfrak{m}A[X]$. If $a_n \in \mathfrak{m}$, then $a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \in \mathfrak{M} - \mathfrak{m}A[X]$. This is impossible by the choice of $f(X)$. Hence $a_n \notin \mathfrak{m}$, so that there exists $b_n \in A$ such that $a_nb_n - 1 \in \mathfrak{m}$. Therefore, $b_nf(X) - (a_nb_n - 1)X^n \in \mathfrak{M}$ is the required monic polynomial. □

Lemma 2.8.3 *Let A be a Noetherian ring with $\dim(A) = d$ and I be an ideal of $A[X]$ such that $\mathrm{ht}(I) = d+1$. Then I contains a monic polynomial.*

Proof. By 1.4.13, it follows that $\sqrt{I} = \cap_{i=1}^{n}\mathfrak{p}_i$ where, the prime ideals $\mathfrak{p}_i$ are minimal over I. But, $\mathrm{ht}(I) = d+1$ implies that $\mathrm{ht}(\mathfrak{p}_i) \geq d+1$. Since $\dim(A[X]) = d+1$, $\mathrm{ht}(\mathfrak{p}_i) = d+1$, and the prime ideals $\mathfrak{p}_i$ are maximal. Hence by Lemma 2.8.2, each $\mathfrak{p}_i$ contains a monic polynomial. So, by taking the product of the monic polynomials belonging to $\mathfrak{p}_i$ for each i, we get a monic polynomial in $\sqrt{I}$. By taking some large power of that polynomial we get a monic polynomial belonging to I. □

Theorem 2.8.4 *Let A be a Noetherian domain of dimension d and $[f_1(X), f_2(X), \ldots, f_n(X)] \in \mathrm{Um}_n(A[X])$, where $n \geq d+2$. Then we can find a matrix $\beta(X) \in GL_n(A[X])$ such that $\beta(X)$ can be connected to the identity matrix and*

$$\beta(X)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Proof. Since any elementary matrix can be connected to the identity matrix [*cf.* 2.6.4], the result follows from 2.1.10, if $n \geq d+3$. So we assume that $n = d+2$. By Lemma 2.1.9, we can find $\sigma(X) \in E_n(A[X])$ such that

$$\sigma(X) \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} g_1(X) \\ g_2(X) \\ . \\ . \\ g_n(X) \end{pmatrix}$$

and $\mathrm{ht}(g_1(X), \ldots, g_i(X)) \geq i$ for $1 \leq i \leq n$. Since $\mathrm{ht}\big\langle g_1(X), \ldots, g_{n-1}(X)\big\rangle \geq n-1 = d+1$, it follows from Lemma 2.8.3 that the ideal $\big\langle g_1(X), \ldots, g_{n-1}(X)\big\rangle$ contains a monic polynomial, say $h(X)$. By adding a large power of $h(X)$ to $g_n(X)$, we may assume that g_n is monic. Now, by adding a large power of $g_n(X)$ to $g_1(X)$, we may assume that $g_1(X)$ is monic. Hence by Theorem 2.7.2, there exists a matrix $\delta(X,T) \in GL_n(A(X,T)$ such that $\delta(X,0) = I_n$ and

$$\delta(X,1) \begin{pmatrix} g_1(X) \\ g_2(X) \\ . \\ . \\ g_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Now, $\sigma(X)$ is elementary and hence can be connected to the identity matrix. Hence there exists $\delta'(X,T) \in GL_n(A[X,T])$ such that $\delta'(X,0) = I_n$ and $\delta'(X,1) = \sigma(X)$. Let $\alpha(X,T) = \delta(X,T)\delta'(X,T)$. Then $\alpha(X,0) = I_n$ and

$$\alpha(X,1) \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Setting $\beta(X) = \alpha(X,1)$, the result follows. □

3 On Forster's Conjecture

The aim of this section is to give a proof of Forster's conjecture 3.3.3, *viz.*

Theorem. Let k be a field and $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ be a prime ideal such that $k[X_1, \ldots, X_n]/\mathfrak{p}$ is regular. Then $\mathfrak{p}$ is generated by n elements.

The proof we give is based on a theorem of Satya Mandal 3.3.2. We also use the theorem of Mandal to prove some addition principles (see 3.4).

3.1 Conditions for Efficient Generation of Ideals

Let A be a ring and M an A-module. Then we define $\mu(M)$ to be the minimum number of elements of M needed to generate M.

Definition 3.1.1 An ideal I of a ring A is said to be **efficiently generated** if $\mu(I) = \mu(I/I^2)$.

In this section we give necessary conditions for an ideal I to be efficiently generated. The results proved in this section are in a certain sense the analogues of the results proved in Sections 2.1 and 2.2.

Theorem 3.1.2 *Let $(A, \mathfrak{m})$ be a Noetherian local ring and $I \subset A$ be an ideal. Suppose there exist $f_1, f_2, \ldots, f_n$ in I such that their images generate I/I^2, then I is generated by $f_1, f_2, \ldots, f_n$.*

Proof. Since $\mathfrak{m}$ is the unique maximal ideal of A, $I \subseteq \mathfrak{m}$. Since A is Noetherian, I is finitely generated. Let J be the ideal of A generated by $f_1, \ldots, f_n$. Then $I = J + I^2$. Using Corollary 1.3.5, $I = J$. This proves the lemma. □

The following lemma is based on a result of Kronecker (*cf.*[14]).

Lemma 3.1.3 *Let A be a Noetherian ring with $\dim(A) = d$ and $I \subset A$ be an ideal. Then there exist $f_1, f_2, \ldots, f_{d+1} \in I$ such that $V(I) = V(f_1, f_2, \ldots, f_{d+1})$.*

Proof. We split the proof into six steps.

Step 1. If I is contained in every minimal prime ideal of A, then $V(I) = \mathrm{Spec}(A)$, and we may choose $f_1 = f_2 = \cdots = f_{d+1} = 0$.

Step 2. We may therefore assume that I is not contained in every minimal prime ideal of A. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ be the minimal prime ideals of A which do not contain I. Since $I \nsubseteq \mathfrak{p}_i$ for $1 \leq i \leq r$, by 1.2.1, it follows that $I \nsubseteq \cup_{i=1}^{r} \mathfrak{p}_i$. Hence we can choose $f_1 \in I$ such that $f_1 \notin \cup_{i=1}^{r} \mathfrak{p}_i$.

Step 3. Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_s \in \mathrm{Spec}(A)$ be the minimal prime ideals containing $\langle f_1 \rangle$ but not containing I. If no such prime ideals exist we choose $f_2 = 0$. Otherwise, as in Step 2, we choose $f_2 \in I$ such that $f_2 \notin \cup_{i=1}^{s} \mathfrak{q}_i$.

Step 4. Having chosen $f_1, f_2, \ldots, f_j \in I$ for $1 \leq j \leq d$, in the above way, let $\mathfrak{p}_1', \mathfrak{p}_2', \ldots, \mathfrak{p}_l' \in \mathrm{Spec}(A)$ be the minimal prime ideals of A containing $\langle f_1, f_2, \ldots, f_j \rangle$ but not containing I. If no such prime ideals exist, we choose $f_{j+1} = 0$ and $f_i = 0$ for $j+1 \leq i \leq d+1$. Otherwise, we choose $f_{j+1} \in I$ such that $f_{j+1} \notin \cup_{i=1}^{l} \mathfrak{p}_i'$.

Step 5. We claim that if $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_i \rangle$ and $\mathfrak{p} \not\supseteq I$, then $\mathrm{ht}(\mathfrak{p}) \geq i$ for $1 \leq i \leq d+1$. We prove the claim by induction on i. The case $i = 1$, follows from Step 2. Assume, by induction, the assertion of the claim holds for $i = j$. Suppose $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_{j+1} \rangle$, $\mathfrak{p} \not\supseteq I$. We will prove that $\mathrm{ht}(\mathfrak{p}) \geq j+1$. Assume that $\mathrm{ht}(\mathfrak{p}) \leq j$. We will derive a contradiction.

Since $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_j \rangle$ and $\mathfrak{p} \not\supseteq I$, it follows from the induction hypothesis that $\mathrm{ht}(\mathfrak{p}) \geq j$. By assumption, we have $\mathrm{ht}(\mathfrak{p}) \leq j$. It therefore follows that $\mathrm{ht}(\mathfrak{p}) = j$.

We next prove that $\mathfrak{p}$ is minimal over $\langle f_1, f_2, \ldots, f_j \rangle$. Let $\mathfrak{p}' \in \mathrm{Spec}(A)$ be such that $\mathfrak{p} \supsetneq \mathfrak{p}' \supset \langle f_1, f_2, \ldots, f_j \rangle$. Since $\mathfrak{p} \not\supseteq I$, $\mathfrak{p}' \not\supseteq I$. This implies that $\mathrm{ht}(\mathfrak{p}') \geq j$ by the induction hypothesis. Hence $\mathrm{ht}(\mathfrak{p}) \geq j+1$, which is a contradiction. Therefore, $\mathfrak{p}$ is minimal over $\langle f_1, f_2, \ldots, f_j \rangle$. Since $\mathfrak{p} \not\supseteq I$, it follows from Step 4, that $f_{j+1} \notin \mathfrak{p}$. This contradicts the assumption that $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_{j+1} \rangle$. Hence the claim.

Step 6. By Step 5, if $\mathfrak{p} \in \mathrm{Spec}(A)$ is such that $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_{d+1} \rangle$ and $\mathfrak{p} \not\supseteq I$, then $\mathrm{ht}(\mathfrak{p}) \geq d+1$. Since $\dim(A) = d$, it follows that any prime ideal containing $\langle f_1, f_2, \ldots, f_{d+1} \rangle$ has to contain I. Therefore, $V(f_1, f_2, \ldots, f_{d+1}) \subset V(I)$. On the other hand $\langle f_1, f_2, \ldots, f_{d+1} \rangle \subset I$, so that $V(I) \subset V(f_1, f_2, \ldots, f_{d+1})$. Therefore, $V(I) = V(f_1, f_2, \ldots, f_{d+1})$. □

We can ask, what additional hypothesis are necessary to conclude that I is generated by $d+1$ elements. If I is generated by $d+1$ elements, then so is I/I^2. It turns out that this additional condition is sufficient to ensure that I is generated by $d+1$ elements.

We prove the following theorem due to N. Mohan Kumar, *cf.* [23], Lemma 4.

Theorem 3.1.4 *Let A be Noetherian ring with $\dim(A) = d$, and $I \subset A$ be an ideal such that I/I^2 is generated by $d+1$ elements. Then I is generated by $d+1$ elements.*

Before proving Theorem 3.1.4, we prove the following theorem.

Theorem 3.1.5 *Let A be a Noetherian ring and I be an ideal of A. Then I will be generated by n elements $f_1, f_2, \ldots, f_n$ provided $f_1, f_2, \ldots, f_n$ generate I modulo I^2 and $V(f_1, f_2, \ldots, f_n) = V(I)$.*

To prove this Theorem we need the following lemmas.

Lemma 3.1.6 *Let A be a Noetherian ring and $I \subset A$ be an ideal such that $I = I^2$. Then I is generated by an idempotent element.*

Proof. Since A is Noetherian, I is finitely generated. By 1.3.3, there exists $a \in I$ such that $(1-a)I = 0$. We claim that $I = \langle a \rangle$. Clearly, $\langle a \rangle \subset I$. Let $b \in I$. Then $(1-a)b = 0$. Since $ab \in \langle a \rangle$, $b \in \langle a \rangle$. Hence the claim. Now, since $(1-a)a = 0$, $a = a^2$. Hence a is an idempotent element. □

Corollary 3.1.7 *Let A be a Noetherian ring and $I \subset A$ be an ideal. Suppose $I = \langle a_1, a_2, \ldots, a_n \rangle + I^2$. Then $I = \langle a_1, a_2, \ldots, a_n, e \rangle$, where $e(1-e) \in \langle a_1, a_2, \ldots, a_n \rangle$.*

Proof. Let $a_1, a_2, \ldots, a_n \in I$ be such that their images generate I/I^2. Then $I = \langle a_1, a_2, \ldots, a_n \rangle + I^2$. Suppose $\bar{I} = I/\langle a_1, a_2, \ldots, a_n \rangle$, where bar denotes reduction modulo $\langle a_1, a_2, \ldots, a_n \rangle$. Then $\bar{I} = \bar{I}^2$. By Lemma 3.1.6, $\bar{I} = \langle \bar{e} \rangle$ for some idempotent element $\bar{e} \in \bar{I}$. Let $e \in I$ be any preimage of $\bar{e}$. Then $I = \langle a_1, a_2, \ldots, a_n, e \rangle$ and $e(1-e) \in \langle a_1, a_2, \ldots, a_n \rangle$. □

Lemma 3.1.8 *Let A be a ring and $e \in A$ be an idempotent element. Then*

$$\langle e \rangle \cap \langle 1-e \rangle = \{0\}.$$

Proof. Let $x \in \langle e \rangle \cap \langle 1-e \rangle$. Then $x = \lambda e = \mu(1-e)$ for some $\lambda, \mu \in A$. This implies that $\lambda e^2 = \mu e(1-e)$. Since $e = e^2$, it follows that $x = \lambda e = \lambda e^2 = \mu e(1-e) = 0$. □

Lemma 3.1.9 (*cf.* [5], Lemma 2.11) *Let A be a Noetherian ring and $J \subset A$ be an ideal. Let $J_1 \subset J$ and $J_2 \subset J^2$ be two ideals of A such that $J_1 + J_2 = J$. Then $J = J_1 + \langle e \rangle$ for some $e \in J_2$ and $J_1 = J \cap J'$, where $J_2 + J' = A$.*

Proof. We claim that $(J/J_1)^2 = J/J_1$. Clearly, $(J/J_1)^2 \subset J/J_1$. Conversely, we know that $(J/J_1)^2 = (J^2 + J_1)/J_1$. But, $J^2 + J_1 \supset J_2 + J_1 \supset J$ implying that $(J/J_1)^2 \supset J/J_1$. Hence the claim.

Let bar denote reduction modulo J_1. By Lemma 3.1.6, it follows that $J/J_1 = \langle \overline{e} \rangle$ for some idempotent element $\overline{e} \in J/J_1$. Since the map $J_2 \to J/J_1$ is surjective, we may assume that $e \in J_2$. Let $J' = J_1 + \langle 1-e \rangle$. Then $e \in J_2$ implies $1 = e + (1-e) \in J_2 + J'$, showing that $J_2 + J' = A$.

Lastly to show that $J \cap J' = J_1$. It suffices to show that $\overline{J} \cap \overline{J}' = \langle \overline{0} \rangle$. But, this is clear by 3.1.8, since $\overline{J} = \langle \overline{e} \rangle$ and $\overline{J'} = \langle \overline{1-e} \rangle$. Hence the lemma follows. □

Lemma 3.1.10 *Let A be a ring, M an A-module and N be an A-submodule of M. Then following three statements are equivalent. (i) $M = N$. (ii) $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Spec}(A)$. (iii) $M_{\mathfrak{m}} = N_{\mathfrak{m}}$ for every $\mathfrak{m} \in \operatorname{Max}(A)$.*

Proof. Let us consider the A-module $L = M/N$. Then $L = 0 \Leftrightarrow M = N$ and $L_{\mathfrak{p}} = 0 \Leftrightarrow M_{\mathfrak{p}} = N_{\mathfrak{p}}$ (see 1.1.16). Therefore, it suffices to show the equivalence of the following three statements. (i) $M = 0$. (ii) $M_{\mathfrak{p}} = 0$ for every $\mathfrak{p} \in \mathrm{Spec}(A)$. (iii) $M_{\mathfrak{m}} = 0$ for every $\mathfrak{m} \in \mathrm{Max}(A)$.

Clearly, $(i) \Rightarrow (ii) \Rightarrow (iii)$. Now, we show that $(iii) \Rightarrow (i)$. Let (iii) be true and suppose $M \neq 0$. Then there exists $x \in M$ such that $x \neq 0$. If $I = \mathrm{ann}(x) = \{\lambda \in A \,|\, \lambda x = 0\}$, then $I \neq A$, as $x \neq 0$. Thus, I is contained in some maximal ideal $\mathfrak{m}$ of A. Now, $\frac{x}{1} \in M_{\mathfrak{m}} = 0$ implying that there exists $s \in A - \mathfrak{m}$ such that $sx = 0$. But $s \in \mathrm{ann}(x) = I \subset \mathfrak{m}$. This is a contradiction, hence $(iii) \Rightarrow (i)$. □

Proof of Theorem 3.1.5.

Proof 1. Let $J = \langle f_1, f_2, \ldots, f_n \rangle$. In order to check that $J = I$, by Lemma 3.1.10, it is enough to check that $I_{\mathfrak{p}} = J_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$. If $\mathfrak{p} \not\supseteq J$, then $\mathfrak{p} \not\supseteq I$ and hence $I_{\mathfrak{p}} = J_{\mathfrak{p}} = A_{\mathfrak{p}}$. If $\mathfrak{p} \supset J$, then by hypothesis $\mathfrak{p} \supset I$. Since $f_1, f_2, \ldots, f_n$ generate I modulo I^2, and $A_{\mathfrak{p}}$ is local, by Lemma 3.1.2, $I_{\mathfrak{p}} = J_{\mathfrak{p}}$. This proves the lemma. □

Proof 2. Since $\langle f_1, f_2, \ldots, f_n \rangle + I^2 = I$, by Lemma 3.1.9, $\langle f_1, f_2, \ldots, f_n \rangle = I \cap I'$ for some ideal I' of A such that $I + I' = A$. It follows that no prime ideal of A can contain both I and I'. We claim that $I' = A$. Take $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $\mathfrak{p} \supset I'$. Then $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_n \rangle$ and hence by hypothesis $\mathfrak{p} \supset I$. This is a contradiction. Hence the claim. Therefore, $\langle f_1, f_2, \ldots, f_n \rangle = I$. □

We now proceed to the proof of Theorem 3.1.4. Its proof is similar to that of Lemma 3.1.3. The idea of the proof is to start with a set of generators $g_1, g_2, \ldots, g_{d+1}$ of I modulo I^2 and modify them by elements of I^2 to obtain $f_1, f_2, \ldots, f_{d+1}$, so that $V(f_1, f_2, \ldots, f_{d+1}) = V(I)$ and appeal to 3.1.5.

Proof of Theorem 3.1.4. We split the proof into five steps.

Step 1. If I is contained in every minimal prime ideal of A, then $V(I) = \mathrm{Spec}(A)$. Therefore, $V(g_1, g_2, \ldots, g_{d+1}) = \mathrm{Spec}(A) = V(I)$ and by 3.1.5, $I = \langle g_1, g_2, \ldots, g_{d+1} \rangle$.

Step 2. We may therefore assume that I is not contained in every minimal prime ideal of A. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the minimal prime ideals of A which do not contain I. Since $I \not\subseteq \mathfrak{p}_i$, $I^2 \not\subseteq \mathfrak{p}_i$ $(1 \leq i \leq r)$. We choose $y_1 \in I^2$ such that $y_1 \notin \cup_{i=1}^r \mathfrak{p}_i$. Suppose that $g_1 \in \mathfrak{p}_i$ for $1 \leq i \leq l$ and $g_1 \notin \mathfrak{p}_i$ for $l+1 \leq i \leq r$. We choose $a_1 \in \cap_{i=l+1}^r \mathfrak{p}_i - \cup_{i=1}^l \mathfrak{p}_i$. The element $f_1 = g_1 + a_1 y_1 \notin \cup_{i=1}^r \mathfrak{p}_i$ and $f_1 = g_1$ modulo I^2.

Step 3. Having chosen $f_1, f_2, \ldots, f_j$ we choose f_{j+1} in the following manner. Let $\mathfrak{p}'_1, \mathfrak{p}'_2 \ldots, \mathfrak{p}'_m$ be the minimal prime ideals containing $\langle f_1, f_2, \ldots, f_j \rangle$ and not containing I. If no such prime ideals exist, we choose $f_i = g_i$ for all $i \geq j+1$. Otherwise, as in Step 2, we choose $y_{j+1} \in I^2$, $y_{j+1} \notin \cup_{i=1}^m \mathfrak{p}'_i$. Suppose $g_{j+1} \in \mathfrak{p}_i{}'$ for $1 \leq i \leq s$ and $g_{j+1} \notin \mathfrak{p}_i{}'$ for $s+1 \leq i \leq m$. We choose $a_{j+1} \in \cap_{i=s+1}^m \mathfrak{p}'_i - \cup_{i=1}^s \mathfrak{p}'_i$. The element $f_{j+1} = g_{j+1} + a_{j+1} y_{j+1}$ satisfies the property that $f_{j+1} \notin \cup_{i=1}^m \mathfrak{p}'_i$ and $f_{j+1} = g_{j+1}$ modulo I^2.

Step 4. As in 3.1.3, it follows that if $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_i \rangle$ and $\mathfrak{p} \not\supseteq I$, then $\mathrm{ht}(\mathfrak{p}) \geq i$, $1 \leq i \leq d+1$.

Step 5. By Step 4, if $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{p} \supset \langle f_1, f_2, \ldots, f_{d+1} \rangle$ and $\mathfrak{p} \not\supseteq I$, then $\mathrm{ht}(\mathfrak{p}) \geq d+1$. Since $\dim(A) = d$, it follows that any prime ideal containing $\langle f_1, f_2, \ldots, f_{d+1} \rangle$ contains I. Therefore, $V(f_1, f_2, \ldots, f_{d+1}) = V(I)$. Further, since $f_i = g_i \bmod I^2$ and $g_1, g_2, \ldots, g_{d+1}$ generate I modulo I^2, it follows from 3.1.5 that $f_1, f_2, \ldots, f_{d+1}$ generate I. This completes the proof of the theorem. □.

Theorem 3.1.11 *Let A be a Noetherian ring with $\dim(A) = d$, $I \subset A$ an ideal of A such that I/I^2 is generated by n elements, where $n \geq d+1$. Then I is generated by n elements.*

Proof. We choose $g_1, g_2, \ldots, g_n \in I$ which generate I modulo I^2. As in the proof of Theorem 3.1.4, we choose $f_1, f_2, \ldots, f_{d+1} \in I$ such that $f_i = g_i$ modulo I^2 for $i = 1, 2, \ldots, d+1$ and $V(I) = V(f_1, f_2, \ldots, f_{d+1})$. Since $g_i = f_i$ modulo I^2 and $g_1, g_2, \ldots, g_n$ generate I modulo I^2, it follows that $f_1, \ldots, f_{d+1}, g_{d+2}, \ldots, g_n$ generate I modulo I^2. Since $V(I) = V(f_1, \ldots, f_{d+1})$, we have $V(I) = V(f_1, \ldots, f_{d+1}, g_{d+2}, \ldots, g_n)$. Thus, by Lemma 3.1.5, $f_1, \ldots, f_{d+1}, g_{d+2}, \ldots, g_n$ generate I. This proves the theorem. □

The following lemma is special case of a result of Eisenbud-Evans. For details see ([8], Theorem A).

Lemma 3.1.12 *Let A be a Noetherian ring and $[a_1, \ldots, a_n, a] \in A^{n+1}$. Then there exists $[b_1, \ldots, b_n] \in A^n$ such that if $I = \langle a_1 + ab_1, \ldots, a_n + ab_n \rangle$, then $\mathrm{ht}(I_a) \geq n$, i.e. if $\mathfrak{p} \in \mathrm{Spec}(A)$, $I \subset \mathfrak{p}$ and $a \notin \mathfrak{p}$, then $\mathrm{ht}(\mathfrak{p}) \geq n$.*

Proof. If a belongs to every minimal prime ideal of A, then a belongs to every prime ideal of A and there is nothing to prove.

Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ be the minimal prime ideals of A which do not contain a. Since $a \notin \mathfrak{p}_i$, $\langle a_1, a \rangle \not\subseteq \mathfrak{p}_i$. Hence by Lemma 1.2.1, $\langle a_1, a \rangle \not\subseteq \cup_{i=1}^r \mathfrak{p}_i$. Using 1.2.2, we choose $b_1 \in A$ such that $a_1 + b_1 a \notin \cup_{i=1}^r \mathfrak{p}_i$. Having chosen $b_1, b_2, \ldots, b_k$ for $k < n$, we choose b_{k+1} as follows. Suppose that $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_s \in \mathrm{Spec}(A)$ are the minimal prime ideals containing the ideal $\langle a_1 + b_1 a, \ldots, a_k + b_k a \rangle$ but $a \notin \mathfrak{q}_i$, $1 \leq i \leq s$. If no such prime ideal with the above property exists, we choose $b_{k+1} = 0$ and $b_i = 0$ for $i \geq k+1$. Otherwise, since $a \notin \mathfrak{q}_i$, $\langle a_{k+1}, a \rangle \not\subseteq \cup_{i=1}^s \mathfrak{q}_i$. We choose $b_{k+1} \in A$ such that $a_{k+1} + b_{k+1} a \notin \cup_{i=1}^s \mathfrak{q}_i$. It is easy to check that the elements $b_1, \ldots, b_n$ satisfy the required property. □

Lemma 3.1.13 *Let A be a Noetherian ring and $I \subset A$ be an ideal of A. If $f_1, f_2, \ldots, f_n \in I$ generate I modulo I^2 and every maximal ideal containing $\langle f_1, f_2, \ldots, f_n \rangle$ contains I then $f_1, f_2, \ldots, f_n$ generate I.*

Proof. The proof is along the lines of 3.1.5. □

The next two results are in [26].

Theorem 3.1.14 *Let A be a Noetherian semilocal ring, $I \subset A$ an ideal. If I/I^2 generated by n elements, then I generated by n elements.*

Proof. Let $a_1, \ldots, a_n \in I$ generate I/I^2. Then $\langle a_1, \ldots, a_n \rangle + I^2 = I$. Suppose every maximal ideal containing $\langle a_1, \ldots, a_n \rangle$ contains I. Then by Lemma 3.1.13, I is generated by the n elements $a_1, \ldots, a_n$. Assume otherwise. Since A is semilocal, it has only finitely many maximal ideals. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_l$ be the maximal ideals of A such that $\mathfrak{m}_i \not\supseteq I$, $\mathfrak{m}_i \supset \langle a_1, \ldots, a_n \rangle$. We are going to change a_1 so that $l = 0$. Enumerating all the maximal ideals of A and classifying them, it follows that A has the following three types of maximal ideals. (i) $a_1 \in \mathfrak{m}'_1, \ldots, \mathfrak{m}'_s$, where $\mathfrak{m}'_i \supset I$. (ii) $a_1 \in \mathfrak{m}_1, \ldots, \mathfrak{m}_l$, where $\mathfrak{m}_i \not\supseteq I$. (iii) $a_1 \notin \mathfrak{m}''_1, \ldots, \mathfrak{m}''_q$. It is clear that $I^2 \cap \mathfrak{m}'_1 \cap \cdots \cap \mathfrak{m}'_s \cap \mathfrak{m}''_1 \cap \cdots \cap \mathfrak{m}''_q \not\subseteq \mathfrak{m}_i$ for all $i = 1, 2, \ldots, l$.

We choose, $b \in I^2 \cap \mathfrak{m}'_1 \cap \cdots \cap \mathfrak{m}'_s \cap \mathfrak{m}''_1 \cap \cdots \cap \mathfrak{m}''_q$ such that $b \notin \cup_{i=1}^l \mathfrak{m}_i$. Let $a'_1 = a_1 + b$. Since $b \in I^2$, $\langle a'_1, a_2, \ldots, a_n \rangle + I^2 = I$. We shall show that any maximal ideal of A containing the ideal $\langle a'_1, a_2, \ldots, a_n \rangle$ contains I. Let $\mathfrak{m}$ be a maximal ideal of A such that $\mathfrak{m} \supset \langle a'_1, a_2, \ldots, a_n \rangle$. Then $a'_1 = a_1 + b \in \mathfrak{m}$, where $b \notin \cup_{i=1}^l \mathfrak{m}_i$.

If $\mathfrak{m} = \mathfrak{m}_i$ for some $i = 1, 2, \ldots, l$, then $a'_1 \in \mathfrak{m}_i$. But, since $a_1 \in \mathfrak{m}_i$, $b \in \mathfrak{m}_i$, which is not true. Further, if $\mathfrak{m} = \mathfrak{m}''_j$, then $\mathfrak{m}$ contains a'_1 as well as b, so that it contains a_1. But $\mathfrak{m}''_j$ does not contain a_1. This implies, $\mathfrak{m} \neq \mathfrak{m}''_j$ for $j = 1, 2, \ldots, q$.

Therefore, $\mathfrak{m} = \mathfrak{m}'_r$ for some $r \in \{1, 2, \ldots, s\}$. This implies that $\mathfrak{m}$ contains I. Hence the assertion. Using Lemma 3.1.13, it follows that $I = \langle a'_1, a_2, \ldots, a_n \rangle$.

□

As a direct consequence of Theorem 3.1.14, we have the following theorem.

Theorem 3.1.15 *Let A be a Noetherian local ring. Let $I \subset A[X]$ be an ideal containing a monic polynomial. Suppose I/I^2 is generated by n elements. Then I is generated by n elements.*

Proof. Let $f(X) \in I$ be a monic polynomial and suppose $\langle f_1(X), \ldots, f_n(X)\rangle + I^2 = I$. Replacing f_1 by $f_1 + f^p$ for sufficiently large $p > 0$ we may assume that f_1 is monic. Now, the theorem follows by applying 3.1.14 to the ring $A[X]/\langle f_1(X)\rangle$. □

The next theorem 3.1.18 generalises 3.1.11 and 3.1.14. Before proving the theorem we prove the following lemma.

Lemma 3.1.16 *Let A be a Noetherian ring, $J \subset A$ an ideal. Suppose $J = \langle b_1, \ldots, b_n, s\rangle$, where $s \in J^2$. Then there exists $c_1, \ldots, c_n$ in A such that if $d_i = b_i + sc_i$ then $\langle d_1, \ldots, d_n\rangle = J \cap J'$, where $J' + \langle s\rangle = A$ and $\mathrm{ht}(J') \geq n$. In particular, if $n \geq \dim(A) + 1$ then $J = \langle d_1, \ldots, d_n\rangle$.*

Proof. Using Lemma 3.1.12, we choose $c_i \in A$, $1 \leq i \leq n$, such that if $d_i = b_i + sc_i$, then the ideal $\langle d_1, \ldots, d_n\rangle$ satisfies the property: If $\mathfrak{p} \in \mathrm{Spec}(A)$ is such that $\mathfrak{p} \supset \langle d_1, \ldots, d_n\rangle$, $s \notin \mathfrak{p}$ then $\mathrm{ht}(\mathfrak{p}) \geq n$. Now, since $\langle d_1, \ldots, d_n, s\rangle = J$ and $s \in J^2$, by 3.1.9, $\langle d_1, \ldots, d_n\rangle = J \cap J'$, where $J' + \langle s\rangle = A$. We show that $\mathrm{ht}(J') \geq n$. Suppose $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{p} \supset J'$. Then $\mathfrak{p} \supset \langle d_1, \ldots, d_n\rangle$. Since $J + J' = A$, $\mathfrak{p} \not\supseteq J$ and hence $s \notin \mathfrak{p}$. It follows that $\mathrm{ht}(\mathfrak{p}) \geq n$. This implies that $\mathrm{ht}(J') \geq n$. Hence the lemma follows. □

Remark 3.1.17 Using 3.1.16 and 3.1.9, we can get another proof of 3.1.11.

Theorem 3.1.18 *Let A be a Noetherian ring, $I \subset A$ an ideal. Suppose I/I^2 is generated by n elements, where $n \geq \dim(A/\mathrm{Jac}(A)) + 1$. Then I is generated by n elements.*

Proof. Let $a_1, \ldots, a_n$ generate I modulo I^2. Then $\langle a_1, \ldots, a_n\rangle + I^2 = I$. Using 3.1.9, we choose $c \in I^2$ such that $\langle a_1, \ldots, a_n, c\rangle = I$. Let $B = A/\mathrm{Jac}(A)$ and bar denote reduction modulo $\mathrm{Jac}(A)$. Then

$$\langle \overline{a_1}, \ldots, \overline{a_n}, \overline{c}\rangle = \overline{I} = \frac{I + \mathrm{Jac}(A)}{\mathrm{Jac}(A)}.$$

Using Lemma 3.1.16 we choose $\overline{\mu_1}, \ldots, \overline{\mu_n} \in B$ such that $\langle \overline{a_1} + \overline{\mu_1 c}, \ldots, \overline{a_n} + \overline{\mu_n c}\rangle = \overline{I} \cap \overline{I}'$, where $\mathrm{ht}(\overline{I}') \geq n$ and $\overline{I} + \overline{I'} = B$. But, as $n > \dim(A/\mathrm{Jac}(A))$, $\overline{I}' = B$. This implies, $\langle \overline{a_1} + \overline{\mu_1 c}, \ldots, \overline{a_n} + \overline{\mu_n c}\rangle = \overline{I}$. Hence $\langle a_1 + \mu_1 c, \ldots, a_n + \mu_n c\rangle + \mathrm{Jac}(A) = I + \mathrm{Jac}(A)$. Let $J = \langle a_1 + \mu_1 c, \ldots, a_n + \mu_n c\rangle$. Since $c \in I^2$, the ideal J satisfies the property, $J + I^2 = I$. We claim that every maximal ideal of A containing J has to contain I. Let $\mathfrak{m}$ be a maximal ideal of A such that $\mathfrak{m} \supset J$. Since $\mathfrak{m} \supset \mathrm{Jac}(A)$, $\mathfrak{m} \supset J + \mathrm{Jac}(A)$ and hence $\mathfrak{m} \supset I$. Therefore, by Lemma 3.1.13, $J = I$. Hence I is generated by n elements. This proves the theorem. □

3.2 Some Patching Lemmas

Lemma 3.2.1 *Let A be a domain, I an ideal of A. Let $a, c \in A$ be such that $\langle a, c\rangle = A$. Then*

$$\begin{array}{ccc} I & \longrightarrow & I_a \\ \downarrow & & \downarrow \\ I_c & \longrightarrow & I_{ac} \end{array}$$

is a pullback diagram. This means that if two elements $x \in I_a, y \in I_c$ are equal in I_{ac}, then there exists a unique $z \in I$ such that $\frac{z}{1} = x$ in I_a and $\frac{z}{1} = y$ in I_c.

Proof. Let $x = \frac{b}{a^r} \in I_a$ and $y = \frac{d}{c^s} \in I_c$ be such that $\frac{b}{a^r} = \frac{d}{c^s}$ in I_{ac}, (where $b, d \in I$). Hence $bc^s = da^r$ in A. Since $\langle a, c\rangle = A$, $\langle a^r, c^s\rangle = A$. We choose $\lambda, \mu \in A$ such that $\lambda a^r + \mu c^s = 1$. Let $z = \lambda b + \mu d$. Then $a^r z = a^r \lambda b + a^r \mu d = a^r \lambda b + c^s \mu b = b(a^r\lambda + c^s\mu) = b$ and $c^s z = c^s \lambda b + c^s \mu d = a^r \lambda d + c^s \mu d = d(a^r\lambda + c^s\mu) = d$. Hence we have $\frac{z}{1} = \frac{b}{a^r}$ in I_a and $\frac{z}{1} = \frac{d}{c^s}$ in I_c. The uniqueness of z can be proved easily. □

Remark 3.2.2 The element $z \in I$ defined in 3.2.1 is called the pullback of (x, y).

Lemma 3.2.3 *Let A be a domain, I an ideal of A. Let $a, c \in A$ be elements such that $\langle a, c\rangle = A$. Suppose $I_a = \langle x_1, \ldots, x_n\rangle$, $I_c = \langle y_1, \ldots, y_n\rangle$ and $x_i = y_i$ in I_{ac}. Suppose $z_i \in I$ is the pullback of (x_i, y_i). Then $I = \langle z_1, \ldots, z_n\rangle$.*

Proof. Let $I_a = \left\langle \frac{b_1}{a^{r_1}}, \cdots, \frac{b_n}{a^{r_n}} \right\rangle$ and $I_c = \left\langle \frac{d_1}{c^{s_1}}, \cdots, \frac{d_n}{c^{s_n}} \right\rangle$, where $b_i, d_i \in I$, $1 \le i \le n$. Suppose $\frac{b_i}{a^{r_i}} = \frac{d_i}{c^{s_i}}$ in I_{ac} for all i. By 3.2.1, there exists unique $z_i \in I$ such that $z_i = \frac{b_i}{a^{r_i}}$ in I_a and $z_i = \frac{d_i}{c^{s_i}}$ in I_c. We claim $I = \langle z_1, \ldots, z_n\rangle$. Let $x \in I$. Then $x = \sum_{i=1}^n \frac{\lambda_i}{a^{r'_i}} \frac{b_i}{a^{r_i}} = \sum_{i=1}^n \frac{\lambda_i}{a^{r'_i}} z_i$ and $x = \sum_{i=1}^n \frac{\mu_i}{c^{s'_i}} \frac{d_i}{c^{s_i}} = \sum_{i=1}^n \frac{\mu_i}{c^{s'_i}} z_i$. Let $r'' = \max\{r'_i\}_{i=1}^n$ and $s'' = \max\{s'_i\}_{i=1}^n$. Let $r = \max(r'', s'')$. Then we have $a^r x = \sum_{i=1}^n \lambda'_i z_i$ and $c^r x = \sum_{i=1}^n \mu'_i z_i$, where $\lambda'_i, \mu'_i \in A$. Since $\langle a^r, c^r\rangle = A$, there exists $t_1, t_2 \in A$ such that $t_1 a^r + t_2 c^r = 1$. Therefore, $x = x(t_1 a^r + t_2 c^r) = t_1 a^r x + t_2 c^r x = \sum_{i=1}^n (t_1\lambda'_i + t_2\mu'_i) z_i$. This proves the claim. □

Lemma 3.2.4 *Let A be domain, I an ideal of A. Let $a, c \in A$ be such that $\langle a, c\rangle = A$. Suppose there exist two surjections $f : A_a^n \twoheadrightarrow I_a$ viz. $e_i \mapsto x_i$ and $g : A_c^n \twoheadrightarrow I_c$ viz. $e_i \mapsto y_i$ where $x_i \in I_a, y_i \in I_c$, $1 \le i \le n$. If there exists $\sigma \in GL_n(A_{ac})$ such that $\widehat{f}\sigma = \widehat{g}$ (where $\widehat{f} : A_{ac}^n \to I_{ac}$ and $\widehat{g} : A_{ac}^n \to I_{ac}$ are induced by f and g respectively) and further that $\sigma = \tau_1\tau_2$, where $\tau_1 \in GL_n(A_a)$ and $\tau_2 \in GL_n(A_c)$, then I is generated by n elements.*

Proof. Case 1. Suppose $\sigma = I_n$ *i.e.* $\widehat{f} = \widehat{g}$. Then in I_{ac}, $x_i = \widehat{f}(e_i) = \widehat{g}(e_i) = y_i$. Therefore, by Lemma 3.2.3, I is generated by n elements.

Case 2. (The general case) We are given that $\sigma = \tau_1\tau_2$, where $\tau_1 \in GL_n(A_a)$ and $\tau_2 \in GL_n(A_c)$. Consider the following diagram.

$$A_a^n \xrightarrow{\tau_1} A_a^n \xrightarrow{f} I_a$$

$$A_c^n \xrightarrow{\tau_2^{-1}} A_c^n \xrightarrow{g} I_c$$

By hypothesis, $\widehat{f}\sigma = \widehat{g}$, so that $\widehat{f}\tau_1 = \widehat{g}\tau_2^{-1}$ Therefore, we have the following commutative diagram:

$$\begin{array}{ccccc} A_{ac}^n & \xrightarrow{\tau_1} & A_{ac}^n & \xrightarrow{\widehat{f}} & I_{ac} \\ \| \text{Id} & & & & \| \text{Id} \\ A_{ac}^n & \xrightarrow{\tau_2^{-1}} & A_{ac}^n & \xrightarrow{\widehat{g}} & I_{ac} \end{array}$$

Therefore, Case 2, reduces to the Case 1. Hence the lemma follows. □

3.3 First Proof of Forster's Conjecture

The aim of this section is to give a proof of Forster's conjecture 3.3.3. We deduce it from a theorem of Mandal (See 3.3.2).

Lemma 3.3.1 *Let A be a ring and I an ideal of $A[X]$ containing a monic polynomial. Let J be an ideal of A such that $I + J[X] = A[X]$. Then $(I \cap A) + J = A$.*

Proof. Suppose that $(I \cap A) + J \neq A$. Then there exists a maximal ideal $\mathfrak{m}$ of A such that $(I \cap A) + J \subset \mathfrak{m}$. Thus, $\overline{\mathfrak{m}}$ is a maximal ideal of $A/I \cap A$. Since I contains a monic polynomial, the extension $R = A/I \cap A \hookrightarrow A[X]/I = S$ is integral. Therefore, there exists a maximal ideal $\mathfrak{M}$ of $A[X]$ containing I such that the maximal ideal $\overline{\mathfrak{M}}$ of $A[X]/I$ satisfies $\overline{\mathfrak{m}} = \overline{\mathfrak{M}} \cap A$. Since $J \subset \mathfrak{m}$, we have $I + J[X] \subset \mathfrak{M}$, a contradiction. Hence the lemma follows. □

The following theorem of Mandal (*cf.* [18]) generalises a result of N. Mohan Kumar (*cf.* [23], pg. 161). We follow [18] (Theorem 1.2), [5] (Prop. 3.3) and [23].

Theorem 3.3.2 *Let A be a Noetherian domain, I an ideal of $A[X]$ containing a monic polynomial. Suppose that I/I^2 is generated by n elements, where $n \geq \dim\left(\frac{A[X]}{I}\right) + 2$. Then I is generated by n elements.*

Proof. Let $b_1, \ldots, b_n \in I$ generate I modulo I^2. By assumption I contains a monic polynomial $f(X)$. The elements $b_1 + f^p, b_2, \ldots, b_n$ also generate I modulo I^2 if $p > 1$. Since $f(X)$ is a monic polynomial, for sufficiently large p the element $a_1 = b_1 + f^p$ is monic. Let $J = I \cap A$. Since I contains monic polynomial, the extension $A/J \hookrightarrow A[X]/I$ is integral. Since the ideal $\langle J^2[X], a_1 \rangle$ contains a monic polynomial *viz.* a_1, the extension $A/J^2 \hookrightarrow A[X]/\langle J^2[X], a_1 \rangle$ is integral (the inclusion following from Lemma 1.9.25). Therefore, by 1.9.18, we have

$$\dim\left(\frac{A[X]}{I}\right) = \dim\left(\frac{A}{J}\right) = \dim\left(\frac{A}{J^2}\right) = \dim\left(\frac{A[X]}{\langle J^2[X], a_1 \rangle}\right).$$

Let $B = \frac{A[X]}{\langle J^2[X], a_1 \rangle}$, and bar denote the reduction modulo $\langle J^2[X], a_1 \rangle$. Then $n-1$ elements $\overline{b}_2, \ldots, \overline{b}_n$ generate $\overline{I}$ modulo $\overline{I}^2$. Since $n \geq \dim\left(\frac{A[X]}{I}\right) + 2$, we have

$$n - 1 \geq \dim\left(\frac{A[X]}{I}\right) + 2 - 1 = \dim\left(\frac{A[X]}{I}\right) + 1 = \dim(B) + 1.$$

Therefore, using Theorem 3.1.11, it follows that $\overline{I}$ is generated by $n-1$ elements, say $\overline{a_2}, \ldots, \overline{a_n}$. Therefore, we have $\langle a_1, a_2, \ldots, a_n \rangle + J^2[X] = I$. Since $J^2[X] \subset I^2$, by Lemma 3.1.9, there exists an ideal I' of $A[X]$ such that $\langle a_1, a_2, \ldots, a_n \rangle = I \cap I'$, where $I' + J^2[X] = A[X]$. Since $a_1, a_2, \ldots, a_n$ generate $I \cap I'$, I' contains a monic polynomial *viz.* a_1. Hence it follows from Lemma 3.3.1 that $I' \cap A + J^2 = A$. Therefore, $I' \cap A$ contains an element of the form $1 + j$ for some $j \in J$. This implies that $I'_{1+j} = A_{1+j}[X]$. Since $I \cap I' = \langle a_1, a_2, \ldots, a_n \rangle$, we have $I_{1+j} = \langle a_1, a_2, \ldots, a_n \rangle A_{1+j}[X]$. Therefore, we have surjection $f : A_{1+j}[X]^n \twoheadrightarrow I_{1+j}$ *viz.* $e_i \mapsto a_i(X)$.

On the other hand $j \in J = I \cap A$ implying that $I_j = A_j[X]$ and hence we have a surjection $g : A_j[X]^n \twoheadrightarrow I_j$ *viz.* $e_1 \mapsto 1, e_i \mapsto 0$ for $i > 1$.

Since $a_1(X), \ldots, a_n(X)$ generate $I_{j(1+j)} = A_{j(1+j)}[X]$, the row $[a_1(X), \ldots, a_n(X)]$ is unimodular in $A_{j(1+j)}[X]$. Since $a_1(X)$ is monic in X, by Theorem 2.7.2, there exists a matrix $\alpha(X,T) \in GL_n(A_{j(1+j)}[X,T])$ such that $\alpha(X,0) = I_n$ and

$$\alpha(X,1)\begin{pmatrix} a_1(X) \\ a_2(X) \\ . \\ . \\ a_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}. \tag{12}$$

Let $C = A_{j(1+j)}[X]$ and $\beta(T) = \alpha(X,T)$. Then $\beta(T) \in GL_n(C[T])$ and $\beta(0) = I_n$. By Lemma 2.6.1, $\beta(T) = \alpha(X,T) = \tau_1(X,T)\tau_2(X,T)$ for some $\tau_1(X,T) \in GL_n(A_{1+j}[X,T])$ and $\tau_2(X,T) \in GL_n(A_j[X,T])$. Putting $T = 1$ we see that $\sigma(X) = \alpha(X,1)$ splits. Now, by (12), the following diagram is commutative:

$$\begin{array}{ccc} A_{j(1+j)}[X]^n & \xrightarrow{\widehat{f}} & I_{j(1+j)} \\ {\scriptstyle \sigma(X)}\uparrow & & \| {\scriptstyle \mathrm{Id}} \\ A_{j(1+j)}[X]^n & \xrightarrow{\widehat{g}} & I_{j(1+j)} \end{array}$$

where $\widehat{f}, \widehat{g}$ are surjections induced by f and g, *i.e.* $\widehat{g} = \widehat{f}\sigma(X)$, where $\sigma(X) = \tau_1(X,1)\tau_2(X,1)$, $\tau_1(X,1) \in GL_n(A_{1+j}[X])$, $\tau_2(X,1) \in GL_n(A_j[X])$ Therefore, by 3.2.4, I is generated by n elements. This completes the proof. □.

Corollary 3.3.3 (*cf.* [23], [34]) *Let k be a field and $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ be a prime ideal such that $k[X_1, \ldots, X_n]/\mathfrak{p}$ is regular. Then $\mathfrak{p}$ is generated by n elements.*

Proof. Let $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ be such that $k[X_1, \ldots, X_n]/\mathfrak{p}$ is regular. If $\mathrm{ht}(\mathfrak{p}) = 1$, then $\mathfrak{p}$ is principal and there is nothing to prove. So, we assume that $\mathrm{ht}(\mathfrak{p}) \geq 2$. Using automorphism of $k[X_1, \ldots, X_n]$, *cf.* 1.10.3, we may assume that $\mathfrak{p}$ contains a monic polynomial in X_n. Let $A = k[X_1, \ldots, X_{n-1}]$ and $X = X_n$. By the Forster-Swan theorem, (*cf.* [9], [41]) $\mathfrak{p}/\mathfrak{p}^2$ is generated by n elements. Since $\mathrm{ht}(\mathfrak{p}) \geq 2$, $\dim(A[X]/\mathfrak{p}) \leq n-2$. Therefore, $n \geq \dim(A[X]/\mathfrak{p}) + 2$. Now, by Mandal's theorem, $\mathfrak{p}$ is generated by n elements. □

3.4 On some Addition Principles

The aim of this section is to prove some addition principles (see 3.4.8, 3.4.9). We begin this section with the following theorem.

Theorem 3.4.1 *Let k be a field and $\mathfrak{m}$ be a maximal ideal of $k[X_1, \ldots, X_n]$. Then $\mathfrak{m}$ is generated by n elements.*

Proof. We prove the theorem by induction on number of variables n. Using 1.10.2, we get $\mathrm{ht}(\mathfrak{m}) = n$. Let $A = k[X_1, \ldots, X_{n-1}]$. Then $\dim(A[X_n]) = n = \mathrm{ht}(\mathfrak{m})$. Hence by Lemma 1.8.3, $\mathrm{ht}(\mathfrak{m} \cap A) \geq n-1$. But, as $\dim(A) = n-1$, it follows that $\mathrm{ht}(\mathfrak{m} \cap A) = n-1$. Therefore, $\mathfrak{m} \cap A$ is a maximal ideal of A. Let $\mathfrak{m} \cap A = \mathfrak{m}_1$. Then

$$k_1[X_n] \cong \frac{A[X_n]}{\mathfrak{m}_1[X_n]} \cong \frac{A}{\mathfrak{m} \cap A}[X_n],$$

where $k_1 = A/\mathfrak{m}_1$ is a field. Let bar denote reduction modulo $\mathfrak{m}_1[X_n]$. Since $k_1[X_n]$ is a PID, $\overline{\mathfrak{m}}$ is generated by a single element. By induction it follows that $\mathfrak{m}_1$ is generated by $(n-1)$ elements. Therefore, $\mathfrak{m}$ is generated by n elements. □

Similarly, one can prove the following corollary.

Corollary 3.4.2 *Let k be a field and $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be a maximal ideals of $k[X_1, \ldots, X_n]$. Let $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$. Then I is generated by n elements.*

Lemma 3.4.3 (Chinese Remainder Theorem) *Let A be a ring, I, J ideals of A such that $I + J = A$. Let $\eta : A \to A/I \oplus A/J$ be the homomorphism (of A-modules) defined by $\eta(a) = (\overline{a}, \overline{a})$. Then η is surjective and $\ker(\eta) = I \cap J$.*

Proof. It is clear that $\ker(\eta) = I \cap J$. Since $I + J = A$, $1 = x + y$, where $x \in I$, $y \in J$. Let $(\overline{r}, \overline{s}) \in A/I \oplus A/J$. Since $rx + ry = r$, $\eta(ry) = (\overline{r}, \overline{0})$. Similarly, $\eta(sx) = (\overline{0}, \overline{s})$. Hence $\eta(ry + sx) = (\overline{r}, \overline{s})$, showing that η is surjective. □

Lemma 3.4.4 *Let A be a ring, J_1, J_2 be ideals of A such that $J_1 + J_2 = A$. Let $J = J_1 \cap J_2$. Then $J/J^2 \cong J_1/J_1^2 \oplus J_2/J_2^2$ as A-modules.*

Proof. We define an A-linear map $f : J \to J_1/J_1^2 \oplus J_2/J_2^2$ by $x \mapsto (\bar{x}, \overline{x})$. Since $J_1 + J_2 = A$, we have $J_1^2 + J_2^2 = A$. We show that f is surjective. Let $(\overline{r}, \overline{s}) \in J_1/J_1^2 \oplus J_2/J_2^2$. We choose $x \in J_1^2$, $y \in J_2^2$ such that $x + y = 1$. Hence $rx + ry = r$. We have $f(ry) = (\bar{r}, \overline{0})$ and similarly, $f(sx) = (\bar{0}, \overline{s})$. Therefore, $f(ry + sx) = (\bar{r}, \overline{s})$.

Note that surjectivity of f can also be proved as follows. We consider as above an element $(\bar{r}, \overline{0}) \in J_1/J_1^2 \oplus J_2/J_2^2$. We want an element $x \in J_1 \cap J_2$ such that $(\bar{x}, \overline{x}) = (\bar{r}, \overline{0})$, *i.e.* $x - r \in J_1^2$ and $x \in J_2^2$. We will be done if we show that $(J_1 \cap J_2 \cap J_2^2) + J_1^2 = J_1$, *i.e.* it is enough to show that $J_1^2 + J_1 \cap J_2^2 = J_1$. Now, multiplying the equation $J_1 + J_2^2 = A$ by J_1 we get $J_1^2 + J_1 J_2^2 = J_1$. Hence the assertion follows. Similarly, we can show that $(\overline{0}, \overline{s})$ is in the image of f. Hence f is surjective.

Since $J_1^2 + J_2^2 = A$, $J_1^2 \cap J_2^2 = J_1^2 J_2^2$ and hence $\ker(f) = J_1^2 \cap J_2^2 = J_1^2 J_2^2 = (J_1 J_2)^2 = (J_1 \cap J_2)^2 = J^2$. Therefore, $J/J^2 \cong J_1/J_1^2 \oplus J_2/J_2^2$. Hence the lemma follows. □

Lemma 3.4.5 *Let A be a ring, I_1, I_2 ideals of A such that $I_1 + I_2 = A$. Let $I = I_1 \cap I_2$. Suppose that both I_1/I_1^2 and I_2/I_2^2 are generated by n elements. Then I/I^2 is generated by n elements.*

Proof. Let $g_1, \ldots, g_n \in I_1$ and $f_1, \ldots, f_n \in I_2$ be generators of I_1/I_1^2 and I_2/I_2^2 respectively. We claim that $(\overline{g_i}, \overline{f_i})$ generate $I_1/I_1^2 \oplus I_2/I_2^2$. Let $\overline{x} \in I_1/I_1^2$. Then $x = \sum_{i=1}^n \lambda_i g_i + c$ for some $c \in I_1^2$, where $\lambda_i \in A$, $1 \leq i \leq n$. Since $I_1 + I_2 = A$, $\lambda_i = \mu_i + \nu_i$, where $\mu_i \in I_1$ and $\nu_i \in I_2$. Therefore, $x = \sum_{i=1}^n (\mu_i + \nu_i) g_i + c = \sum_{i=1}^n \nu_i g_i + d$, where $d \in I_1^2$. Since $\nu_i f_i = 0$ in I_2/I_2^2 we have, $(\overline{x}, \overline{0}) = \sum_{i=1}^n \nu_i (\overline{g_i}, \overline{f_i})$.

A similar computation works for an element of the form $(\overline{0}, \overline{y})$ for $\overline{y} \in I_2/I_2^2$. Hence it follows that the elements $(\overline{g_i}, \overline{f_i})$ generate $I_1/I_1^2 \oplus I_2/I_2^2$. Now, from Lemma 3.4.4, it follows that I/I^2 is generated by n elements. □

Remark 3.4.6 The motivation for the above proof is the following : The surjections $(A/I_1)^n \twoheadrightarrow I_1/I_1^2$ and $(A/I_2)^n \twoheadrightarrow I_2/I_2^2$, given by $\overline{g_i}$ and $\overline{f_i}$ induce via the Chinese remainder theorem, a surjection $(A/I)^n \cong (A/I_1)^n \oplus (A/I_2)^n \twoheadrightarrow I_1/I_1^2 \oplus I_2/I_2^2$ *i.e.* we get n elements which generate $I_1/I_1^2 \oplus I_2/I_2^2$.

The following theorem is in ([36], Theorem 4). We follow ([6], Prop. 3.1).

Theorem 3.4.7 *Let A be a Noetherian domain with $\dim(A) = d$. Let J_1 and J_2 be two ideals of A of height n such that $J_1 + J_2 = A$. Assume that J_1 and J_2 are both generated by n elements. Assume further that $n \geq \frac{d+3}{2}$. Then $J_1 \cap J_2$ is generated by n elements.*

Proof 1. Suppose $J_1 = \langle a_1, \ldots, a_n \rangle$ and $J_2 = \langle b_1 \ldots, b_n \rangle$. Since $J_1 + J_2 = A$, the row $[\overline{a_1}, \ldots, \overline{a_n}]$ is unimodular in A/J_2, where bar denotes reduction modulo J_2. Since $\mathrm{ht}(J_2) = n$, $\dim(A/J_2) \leq d-n$. By hypothesis, $n \geq \frac{d+3}{2} \Rightarrow 2n \geq d+3 \Rightarrow n \geq d-n+3 \Rightarrow n \geq \dim(A/J_2)+2$. Therefore, by 2.1.10, there exists a matrix $\alpha \in E_n(A/J_2)$ such that

$$\alpha \begin{pmatrix} \overline{a_1} \\ \overline{a_2} \\ . \\ . \\ \overline{a_n} \end{pmatrix} = \begin{pmatrix} \overline{1} \\ \overline{0} \\ . \\ . \\ 0 \end{pmatrix}.$$

By Lemma 2.1.13, there exists a lift, say σ of α in $E_n(A)$. Hence

$$\begin{pmatrix} a'_1 \\ a'_2 \\ . \\ . \\ a'_n \end{pmatrix} = \sigma \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix} \text{ modulo } J_2 \tag{13}$$

Hence $J_1 = \langle a'_1, \ldots, a'_n \rangle$, where $a'_1 = 1$ modulo J_2 and $a'_i = 0$ modulo J_2 for $i > 1$. Applying Lemma 3.1.12, we choose $\lambda_1, \ldots, \lambda_{n-1} \in A$ such that the ideal

$$\tilde{J_1} = \langle a'_1 + \lambda_1 a'_n, \ldots, a'_{n-1} + \lambda_{n-1} a'_n \rangle$$

satisfies the property that if $\mathfrak{p} \supset \tilde{J_1}$ and $a'_n \notin \mathfrak{p}$, then $\mathrm{ht}(\mathfrak{p}) \geq n-1$.

On the other hand, if $\mathfrak{p} \supset \tilde{J_1}$ and $a'_n \in \tilde{J_1}$, then $\mathfrak{p} \supset \langle a'_1, \ldots, a'_n \rangle$ and since $\mathrm{ht}\langle a'_1, \ldots, a'_n \rangle = \mathrm{ht}(J_1) = n$, we have $\mathrm{ht}(\mathfrak{p}) \geq n$.

Let $a''_i = a'_i + \lambda_i a'_n$, $1 \leq i \leq n-1$, $a''_n = a'_n$. By the above results, $\mathrm{ht}(\tilde{J_1}) = \mathrm{ht}\langle a''_1, \ldots, a''_{n-1} \rangle \geq n-1$. Since $a'_n = 0$ modulo J_2, from equation (13) we have

$$(a''_1, \ldots, a''_{n-1}) = (1, 0, \ldots, 0) \text{ modulo } J_2. \tag{14}$$

Thus, $\langle a''_1, \ldots, a''_{n-1} \rangle + J_2 = A$, *i.e.* $\tilde{J_1} + J_2 = A$. Let bar denote the reduction modulo $\tilde{J_1}$. Since $\tilde{J_1} + J_2 = A$, $[\overline{b_1}, \ldots, \overline{b_n}] \in \mathrm{Um}_n\left(A/\tilde{J_1}\right)$. As $\mathrm{ht}(\tilde{J_1}) \geq n-1$,

$$\dim\left(A/\tilde{J_1}\right) \leq d-(n-1). \tag{15}$$

Since $n \geq \frac{d+3}{2} \Rightarrow n \geq d-n+3 \Rightarrow n \geq d-(n-1)+2 \Rightarrow n \geq \dim\left(A/\tilde{J_1}\right)+2$. By Theorem 2.1.10, there exists $\beta \in E_n\left(A/\tilde{J_1}\right)$ such that

$$\beta \begin{pmatrix} \overline{b_1} \\ \overline{b_2} \\ . \\ . \\ \overline{b_n} \end{pmatrix} = \begin{pmatrix} \overline{1} \\ \overline{0} \\ . \\ . \\ \overline{0} \end{pmatrix}.$$

Let $\tau \in E_n(A)$ be the lift of β. Then

$$\begin{pmatrix} b'_1 \\ b'_2 \\ . \\ . \\ b'_n \end{pmatrix} = \tau \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix} \text{ modulo } \tilde{J}_1. \tag{16}$$

Hence $J_2 = \langle b'_1 \ldots, b'_n \rangle$, where $b'_1 = 1$ modulo $\tilde{J}_1$ and $b'_i = 0$ modulo $\tilde{J}_1$ for $i > 1$. Using Lemma 3.1.12, we choose $\mu_1, \ldots, \mu_{n-1} \in A$ such that $\tilde{J}_2 = \langle b'_1 + \mu_1 b'_n, \ldots, b'_{n-1} + \mu_{n-1} b'_n \rangle$ satisfies the property that if $\mathfrak{p} \supset \tilde{J}_2$ and $b'_n \notin \mathfrak{p}$, then $\mathrm{ht}(\mathfrak{p}) \geq n-1$. As before, if $\mathfrak{p} \supset \tilde{J}_2$ and $b'_n \in \tilde{J}_2$, then $\mathrm{ht}(\mathfrak{p}) \geq n$. Let $b''_i = b'_i + \mu_i b'_n$, $1 \leq i \leq n-1$, $b''_n = b'_n$. Then $\mathrm{ht}(\tilde{J}_2) = \mathrm{ht}\langle b''_1, \ldots, b''_{n-1} \rangle \geq n-1$. Since $b'_n = 0$ modulo $\tilde{J}_1$ from equation (16), we have

$$(b''_1, \ldots, b''_{n-1}) = (1, 0, \ldots, 0) \text{ modulo } \tilde{J}_1. \tag{17}$$

Therefore, we have $\langle b''_1, \ldots, b''_{n-1} \rangle + \tilde{J}_1 = A$. Hence $J_1 = \langle a''_1, \ldots, a''_n \rangle$ and $J_2 = \langle b''_1, \ldots, b''_n \rangle$ where $\langle a''_1, \ldots, a''_{n-1} \rangle + \langle b''_1, \ldots, b''_{n-1} \rangle = A$, $\mathrm{ht}\langle a''_1, \ldots, a''_{n-1} \rangle \geq n-1$, and $\mathrm{ht}\langle b''_1, \ldots, b''_{n-1} \rangle \geq n-1$. Consider the ideals $I_1 = \langle a''_1, \ldots, a''_{n-1}, X - a''_n \rangle$ and $I_2 = \langle b''_1, \ldots, b''_{n-1}, X - b''_n \rangle$ of $A[X]$ and assume $I = I_1 \cap I_2$. In view of (1), $I_1 + I_2 = A[X]$. Now we have a natural map $\phi : A \to A[X]/I_1$. Since $a''_n \mapsto \overline{X}$, ϕ is surjective. By 1.9.25, $\ker(\phi) = \langle a''_1, \ldots, a''_{n-1} \rangle$ and hence

$$\frac{A}{\tilde{J}_1} = \frac{A}{\langle a''_1, \ldots, a''_{n-1} \rangle} \simeq \frac{A[X]}{I_1} \tag{18}$$

By (15), $\dim(A[X]/I_1) \leq d - (n-1)$. Similarly,

$$\frac{A}{\tilde{J}_2} = \frac{A}{\langle b''_1, \ldots, b''_{n-1} \rangle} \simeq \frac{A[X]}{I_2} \tag{19}$$

and $\dim(A[X]/I_2) \leq d - (n-1)$. Lemma 3.4.4 gives an isomorphism of $A[X]$-modules $I/I^2 \simeq I_1/I_1^2 \oplus I_2/I_2^2$. Since I_1/I_1^2 and I_2/I_2^2 are generated by n elements, it follows from Lemma 3.4.5 that I/I^2 is generated by n elements. Since $I_1 + I_2 = A[X]$, no prime ideal of $A[X]$ contains both I_1 and I_2. Therefore,

$$\dim\left(\frac{A[X]}{I}\right) = \mathrm{Sup}\left(\dim\frac{A[X]}{I_1}, \dim\frac{A[X]}{I_2}\right)$$

Using equations (18) and (19), we have $\dim(A[X]/I) \leq d - (n-1)$. By hypothesis, $n \geq \frac{d+3}{2} \Rightarrow n \geq \dim\left(\frac{A[X]}{I}\right) + 2$. Since I/I^2 is generated by n elements, it follows from Theorem 3.3.2 that I is generated by n elements. Putting $X = 0$, we see that $J = J_1 \cap J_2$ is generated by n elements. This completes the proof. □

Proof 2. As in the first proof assume that we have chosen generators $a''_1, \ldots, a''_n$ of J_1 and $b''_1, \ldots, b''_n$ of J_2 such that $\langle a''_1, \ldots, a''_{n-1} \rangle + \langle b''_1, \ldots, b''_{n-1} \rangle = A$. Let $\tilde{J}_1 = \langle a''_1, \ldots, a''_{n-1} \rangle$ and $\tilde{J}_2 = \langle b''_1, \ldots, b''_{n-1} \rangle$. Then there exist elements $c \in \tilde{J}_1$ and $d \in \tilde{J}_2$ such that $c + d = 1$. Now, $(J_1 \cap J_2)_c = \langle b''_1, \ldots, b''_{n-1}, b''_n \rangle_c$ and $(J_1 \cap J_2)_d = \langle a''_1, \ldots, a''_{n-1}, a''_n \rangle_d$. This gives surjections, $f : A_d^n \twoheadrightarrow (J_1 \cap J_2)_d$ (sending $e_i \mapsto a''_i$) and $g : A_c^n \twoheadrightarrow (J_1 \cap J_2)_c$ (sending $e_i \mapsto b''_i$). By the choice of c, the row $[a''_1, \ldots, a''_{n-1}] \in \mathrm{Um}_{n-1}(A_c)$. Therefore, by 2.1.6,

there exists $\tau \in E_n(A_c)$ such that

$$\tau \begin{pmatrix} a_1'' \\ a_2'' \\ . \\ . \\ a_n'' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Similarly, there exist $\tau' \in E_n(A_d)$ such that

$$\tau' \begin{pmatrix} b_1'' \\ b_2'' \\ . \\ . \\ b_n'' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}$$

Therefore,

$$\tau'^{-1}\tau \begin{pmatrix} a_1'' \\ a_2'' \\ . \\ . \\ a_n'' \end{pmatrix} = \begin{pmatrix} b_1'' \\ b_2'' \\ . \\ . \\ b_n'' \end{pmatrix}.$$

By 2.6.6, $\tau'^{-1}\tau = \alpha_1\alpha_2$, where $\alpha_1 \in GL_n(A_c)$, $\alpha_2 \in GL_n(A_d)$ and

$$\alpha_1\alpha_2 \begin{pmatrix} a_1'' \\ a_2'' \\ . \\ . \\ a_n'' \end{pmatrix} = \begin{pmatrix} b_1'' \\ b_2'' \\ . \\ . \\ b_n'' \end{pmatrix}.$$

Hence the following diagram is commutative:

$$\begin{array}{ccc} A_{cd}^n & \xrightarrow{\widehat{f}} & A_{cd} \\ {\scriptstyle \alpha_1\alpha_2}\uparrow & & \| {\scriptstyle \mathrm{Id}} \\ A_{cd}^n & \xrightarrow{\widehat{g}} & A_{cd} \end{array}$$

Using 3.2.4, it follows that $J = J_1 \cap J_2$ is generated by n elements. □

The following Corollary generalises 3.4.2.

Corollary 3.4.8 *Let A be a Noetherian domain with $\dim(A) = d \geq 3$. Let J_1 and J_2 be ideals of A of height d such that $J_1 + J_2 = A$. Suppose that J_1 and J_2 are generated by d elements. Then so is $J_1 \cap J_2$.*

The following theorem ([37], Theorem 2.3) settles the Corollary in the case where $d = 2$. We give two proofs. The first proof follows [5], Theorem 3.2. The second proof follows [20], Theorem 2.3.

Theorem 3.4.9 *Let A be a Noetherian domain with $\dim(A) = 2$. Let J_1, $J_2 \subset A$ be ideals of height 2 such that $J_1 + J_2 = A$. Suppose that J_1, J_2 are generated by 2 elements. Then $J_1 \cap J_2$ is also generated by 2 elements.*

Proof 1. Suppose $J_1 = \langle f_1, f_2 \rangle$, $J_2 = \langle g_1, g_2 \rangle$. Since $\mathrm{ht}(J_2) = 2$ and $\dim(A) = 2$, it follows that $\sqrt{J_2} = \cap_{i=1}^{n} \mathfrak{m}_i$, where $\mathfrak{m}_i$'s are maximal ideals of A. Since $J_1 + J_2 = A$, $J_1 \not\subseteq \mathfrak{m}_i$ for all i. Therefore, by Theorem (1.2.1), $J_1 = \langle f_1, f_2 \rangle \not\subseteq \cup_{i=1}^{n} \mathfrak{m}_i$. Using Lemma (1.2.2), we choose $\lambda \in A$ such that $f_1 + \lambda f_2 \notin \cup_{i=1}^{n} \mathfrak{m}_i$. Then $J_1 = \langle f_1', f_2 \rangle$, where $f_1' = f_1 + \lambda f_2$ satisfies $\langle f_1' \rangle + \mathfrak{m}_i = A$ for $i = 1, 2, \ldots, n$ and hence

$$\langle f_1' \rangle + \sqrt{J_2} = \langle f_1' \rangle + \cap_{i=1}^{n} \mathfrak{m}_i = A.$$

We claim, $(1 + f_1' A) \cap J_2 \neq \phi$. Note that since $\langle f_1' \rangle + \sqrt{J_2} = A$, $\langle f_1' \rangle + J_2 = A$. So, there exists $c \in A$ such that $g - cf_1' = 1$, where $g \in J_2$. This implies, $1 + cf_1' \in J_2$, hence the claim.

Now, $J = J_1 \cap J_2$ implies that $J = \langle f_1', f_2 \rangle \cap \langle g_1, g_2 \rangle$. Therefore, we have surjective maps $\alpha : A^2_{1+f_1'c} \twoheadrightarrow J_{1+f_1'c} = (J_1 \cap J_2)_{1+f_1'c} = (J_1)_{1+f_1'c}$, sending $e_1 \mapsto f_1'$ and $e_2 \mapsto f_2$, and $\beta : A^2_{f_1'} \twoheadrightarrow J_{f_1'} = (J_1 \cap J_2)_{f_1'} = (J_2)_{f_1'}$ sending $e_i \mapsto g_i$. Since $f_1' \in J_1$ and $(1 + f_1'c) \in J_2$, these two maps give surjections

$$\widehat{\alpha}, \widehat{\beta} : A^2_{f_1'(1+f_1'c)} \twoheadrightarrow J_{f_1'(1+f_1'c)} = A_{f_1'(1+f_1'c)},$$

where $\widehat{\alpha}$ and $\widehat{\beta}$ be the surjections induced from α and β. We show that there exists $\sigma \in GL_2(A_{f_1'(1+f_1'c)})$ such that the diagram

$$\begin{array}{ccc} A^2_{f_1'(1+f_1'c)} & \xrightarrow{\widehat{\alpha}} & A_{f_1'(1+f_1'c)} \\ {\scriptstyle\sigma}\uparrow & & \| {\scriptstyle \mathrm{Id}} \\ A^2_{f_1'(1+f_1'c)} & \xrightarrow{\widehat{\beta}} & A_{f_1'(1+f_1'c)} \end{array}$$

commutes and $\sigma = \gamma_1\gamma_2$, where $\gamma_1 \in GL_n(A_{1+f_1'c})$ and $\gamma_2 \in GL_n(A_{f_1'})$.

Now, f_1' is a unit in $A_{f_1'}$. So by 2.1.6, there exists $\tau \in E_2(A_{f_1'})$ such that

$$\tau \begin{pmatrix} f_1' \\ f_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

As $1 + f_1'c \in \langle g_1, g_2 \rangle$, it follows that $[g_1, g_2] \in \mathrm{Um}_2\left(A_{1+f_1'c}\right)$. Since any unimodular row of length 2 is completable, we have $\tau' \in SL_2\left(A_{1+f_1'c}\right)$ such that

$$\tau' \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}.$$

Let $\sigma = \tau\tau'$. Then $\widehat{\alpha}\sigma = \widehat{\beta}$. Since $\tau \in E_2(A_{f_1'})$, by 2.6.8, there exist $\gamma_1 \in GL_2(A_{1+f_1'c})$ and $\gamma_2 \in GL_2(A_{f_1'})$ such that $\sigma = \tau\tau' = \gamma_1\gamma_2$. Now the result follows by applying Lemma 3.2.4 to the above diagram. □

Proof 2. Let the notation be as in Proof 1. Let $J_1 = \langle f_1', f_2 \rangle$, $J_2 = \langle g_1, g_2 \rangle$, where $\langle f_1' \rangle + J_2 = A$. Let $J = J_1 \cap J_2$. We claim that the ideal $I = \langle f_1', X - 1 \rangle \cap \langle g_1, g_2 \rangle A[X]$ of $A[X]$ is generated by two elements. If so, then

$$\langle f_1', X - 1 \rangle \cap \langle g_1, g_2 \rangle A[X] = \langle p_1(X), p_2(X) \rangle$$

where $p_1(X), p_2(X) \in I$. Putting $X = 1 + f_2$, it follows that $J_1 \cap J_2$ is generated by two elements.

Proof of the claim: Let $I_1 = \langle f_1', X-1\rangle$, $I_2 = \langle g_1, g_2\rangle A[X]$ and $I = I_1 \cap I_2$. Since $I(0) = \langle g_1, g_2\rangle$, we have a surjection $\gamma : A^2 \twoheadrightarrow I(0)$ *viz.* $e_i \mapsto g_i$, $i = 1, 2$. Since $\langle f_1'\rangle + J_2 = A$, we can choose an element $c \in A$ such that $1 + f_1'c \in \langle g_1, g_2\rangle = J_2$. We want to define surjections

$$\alpha : A_{1+f_1'c}[X]^2 \twoheadrightarrow I_{1+f_1'c} = \langle f_1', X-1\rangle A_{1+f_1'c}[X]$$

$$\beta : A_{f_1'}[X]^2 \twoheadrightarrow I_{f_1'} = \langle g_1, g_2\rangle A_{f_1'}[X]$$

such that $\alpha(0) = \gamma_{1+f_1'c}$ and $\beta(0) = \gamma_{f_1'}$, where $\gamma_{1+f_1'c}$ and $\gamma_{f_1'}$ are induced from γ. Let us define $\beta(e_1) = g_1$, $\beta(e_2) = g_2$.

To define α we first define $\alpha' : A_{1+f_1'c}[X]^2 \twoheadrightarrow I_{1+f_1'c}$, *viz.* $e_1 \mapsto f_1'$, $e_2 \mapsto X-1$. Then $\alpha'(0)(e_1) = f_1'$, $\alpha'(0)(e_2) = -1$. Note that $\langle g_1, g_2\rangle \in \mathrm{Um}_2(A_{1+f_1'c})$, as $1 + f_1'c \in \langle g_1, g_2\rangle$. Therefore, there exists $\tau \in GL_2(A_{1+f_1'c})$ such that

$$\tau \begin{pmatrix} f_1' \\ -1 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}.$$

Let

$$\tau \begin{pmatrix} f_1' \\ X-1 \end{pmatrix} = \begin{pmatrix} h_1(X) \\ h_2(X) \end{pmatrix}. \tag{20}$$

Since $I_{1+f_1'c} = \langle f_1', X-1\rangle$ and $\tau \in GL_2(A_{1+f_1'c}[X])$, it follows that $\langle h_1(X), h_2(X)\rangle = I_{1+f_1'c}$. Putting $X = 0$ in (20), we see that

$$\tau \begin{pmatrix} f_1' \\ -1 \end{pmatrix} = \begin{pmatrix} h_1(0) \\ h_2(0) \end{pmatrix}.$$

Now, we define $\alpha : A_{1+f_1'c}[X]^2 \twoheadrightarrow I_{1+f_1'c}$ as follows: $\alpha(e_1) = h_1(X)$, $\alpha(e_2) = h_2(X)$. Since $I_{f_1'(1+f_1'c)} = A_{(1+f_1'c)f_1'}[X]$, we get $\langle h_1(X), h_2(X)\rangle \in \mathrm{Um}_2(A_{f_1'(1+f_1'c)}[X])$. By 2.7.4, there exists a $\sigma(X) \in GL_2(A_{f_1'(1+f_1'c)}[X])$ such that $\sigma(0) = I_2$ and

$$\sigma(X) \begin{pmatrix} h_1(X) \\ h_2(X) \end{pmatrix} = \begin{pmatrix} h_1(0) \\ h_2(0) \end{pmatrix} = \tau \begin{pmatrix} f_1' \\ -1 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}.$$

Hence the following diagram is commutative:

$$\begin{array}{ccc} A_{f_1'(1+f_1'c)}[X]^2 & \xrightarrow{\widehat{\alpha}} & I_{f_1'(1+f_1'c)} \\ {\scriptstyle \sigma(X)}\uparrow & & \| {\scriptstyle Id} \\ A_{f_1'(1+f_1'c)}[X]^2 & \xrightarrow{\widehat{\beta}} & I_{f_1'(1+f_1'c)} \end{array}$$

Since $\sigma(0) = I_2$, by 2.6.1, $\sigma(X)$ splits and hence the claim follows from (3.2.4). Hence the result follows. □

4 Another Proof of Förster's Conjecture

4.1 Some useful Lemmas

Lemma 4.1.1 *Let A be a domain and $b(\neq 0) \in A$. Let $\langle b\rangle = \langle c_1, \ldots, c_n\rangle$, where $c_i \in A$. Suppose $c_i = bd_i$, $d_i \in A$. Then $[d_1, \ldots, d_n] \in Um_n(A)$.*

Proof. By hypothesis, $b = \sum_{i=1}^{n} g_i c_i = \sum_{i=1}^{n} g_i b d_i$ for some $g_i, d_i \in A$. Hence $b\,(1 - \sum_{i=1}^{n} g_i d_i) = 0$. Since A is a domain, $\sum_{i=1}^{n} g_i d_i = 1$, proving the assertion. □

Lemma 4.1.2 *Let A be a Noetherian domain of finite dimension and $s \in A$. Let $T = A_{s\langle 1+sA\rangle}$. Then $dim(T) < dim(A)$.*

Proof. We claim that for any maximal ideal $\mathfrak{m}$ of A either $\mathfrak{m} \cap \langle s \rangle \neq \phi$ or $\mathfrak{m} \cap \langle 1+sA \rangle \neq \phi$ If $s \in \mathfrak{m}$ we are through. Otherwise, $\langle \mathfrak{m}, s \rangle = A$. This implies that there exists $c \in \mathfrak{m}, d \in A$ such that $1 = c + ds$. Thus, $c = 1 - ds \in \mathfrak{m}$. Hence $\mathfrak{m} \cap \langle 1 + sA \rangle \neq \phi$, proving the claim. Thus, no maximal ideal of A survives in the localized ring $T = A_{s\langle 1+sA\rangle}$, *i.e.* $dim(T) < dim(A)$. □

Lemma 4.1.3 *Let A be a Noetherian domain and $S \subset A$ a multiplicative closed set. If $I \subset A$ is an ideal such that*

$$S^{-1}I = \left\langle \frac{c_1}{s_1}, \ldots, \frac{c_k}{s_k} \right\rangle, \quad s_i \in S \ (1 \leq i \leq k),$$

then there exists $s \in S$ such that $I_s = \left\langle \frac{c_1}{s_1}, \ldots, \frac{c_k}{s_k} \right\rangle$.

Proof. Since A is Noetherian, I is finitely generated. Suppose $g_1, \ldots, g_n$ generate I. Then $\frac{g_i}{1} \in S^{-1}I$. Hence $\frac{g_i}{1} = \sum_{j=1}^{k} \frac{\mu_i}{s'_{ij}} \frac{c_j}{s_j}$, where $s'_{ij} \in S$, $\mu_{ij} \in A$. Let $s''_i = \Pi_{j=1}^{k} s'_{ij} s_j$ and $s = \Pi_{i=1}^{n} s''_i$. Hence $I_s = \left\langle \frac{c_1}{s_1}, \ldots, \frac{c_k}{s_k} \right\rangle$. □

Theorem 4.1.4 *Let A be a domain with $\dim(A) = d$ and $I \subset A$ an ideal. Suppose I/I^2 is generated by n elements, where $n \geq d + 1$. Then I is generated by n elements.*

Remark 4.1.5 This theorem has already been proved (3.1.11). We give another proof.

Proof. Let $a_1, \ldots, a_n \in I$ generate I modulo I^2. Then $\langle a_1, \ldots, a_n \rangle + I^2 = I$. Therefore, by 3.1.7, there exists $e \in I$ such that $e(1-e) \in \langle a_1, \ldots, a_n \rangle$ and $I = \langle a_1, \ldots, a_n, e \rangle$. Since $e \in I$, $I_e = A_e$. Since $1 - e$ is unit in A_{1-e} and $e(1-e) \in \langle a_1, \ldots, a_n \rangle$, $e \in \langle a_1, \ldots, a_n \rangle A_{1-e}$. Since $I = \langle a_1, \ldots, a_n, e \rangle$ we have

$$I_{1-e} = \langle a_1, \ldots, a_n \rangle A_{1-e}. \tag{21}$$

Thus, we have surjections: $f_1 : A_{1-e}^n \twoheadrightarrow I_{1-e}$, sending $e_i \mapsto a_i$ and $f_2 : A_e^n \twoheadrightarrow I_e$, sending $e_1 \mapsto 1$ and $e_i \mapsto 0$ for $i > 1$. Since $e(1-e) = \sum_{i=1}^{n} \lambda_i a_i$, $\sum_{i=1}^{n} \left(\frac{\lambda_i}{e(1-e)} \right) a_i = 1$. Hence the row $[a_1, \ldots, a_n]$ is unimodular in $A_{e(1-e)}$. Since $\dim(A) = d$, by Lemma 4.1.2, we have $\dim \left(A_{e(1+eA)} \right) \leq d - 1$. Also, $n \geq d + 1 = d - 1 + 2$, $n \geq \dim \left(A_{e(1+eA)} \right) + 2$. Therefore, by 2.1.10, there exists a matrix $\sigma \in E_n \left(A_{e(1+eA)} \right)$ such that

$$\sigma \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Let $\sigma = \Pi_{i=1}^{r} e_{ij}(\lambda_{ij})$, $\lambda_{ij} \in A_{e(1+eA)}$. Since there are only finitely many λ_{ij}'s, we can choose $b \in A$ such that $\sigma \in E_n \left(A_{e(1+eb)} \right)$. Let $1 + ef = (1-e)(1+eb)$. Hence from

equation (21), we have a surjection $f_3 : A^n_{1+ef} \twoheadrightarrow I_{1+ef} = \langle a_1, \ldots, a_n \rangle_{1+ef}$ induced from f_1. Thus, we have the following commutative diagram:

$$\begin{array}{ccc} A^n_{e(1+ef)} & \xrightarrow{\widehat{f_3}} & I_{e(1+ef)} = \langle a_1, \ldots, a_n \rangle = A_{e(1+ef)} \\ {\scriptstyle\sigma}\uparrow & & \\ A^n_{e(1+ef)} & \xrightarrow{\widehat{f_2}} & I_{e(1+ef)} = \langle 1, 0, \ldots, 0 \rangle = A_{e(1+ef)} \end{array}$$

where $\widehat{f_2}$ and $\widehat{f_3}$ are induced surjections from f_2 and f_3. But, since σ is elementary by 2.6.5 and 2.6.4, σ splits. Using 3.2.4, it follows that I is generated by n elements. This completes the proof. □

4.2 On the Eisenbud-Evans conjecture

The aim of this section is to prove theorem 4.2.2 of N. Mohan Kumar (*cf.* [23], §3 Theorem 2) (see also [34], Theorem 1) which settles a conjecture of Eisenbud-Evans. We first prove a special case of 4.2.1. The proofs of 4.2.1 and 4.2.2 are the ones given in [5]. We deduce Forster's conjecture 4.2.3 from 4.2.2.

Theorem 4.2.1 *Let A be a Noetherian domain with $\dim(A) = d$ and I an ideal of $A[X]$ such that $\mathrm{ht}(I) \geq 2$. Suppose that I/I^2 generated by n elements, where $n \geq d+1$. Then I is generated by n elements.*

Proof. Since $\mathrm{ht}(I) \geq 2$, using 1.8.3, it follows that $\mathrm{ht}(I \cap A) \geq 1$. Let $J = I \cap A$. Then $J \neq 0$. We choose $s \in J^2 \subset I^2$ such that $s \neq 0$. Consider the map $A[X] \to A[X]/sA[X]$ sending $I \mapsto \overline{I}$, where bar denotes reduction modulo $sA[X]$. Since $s \in I^2$,

$$\frac{\overline{I}}{\overline{I}^2} = \frac{\frac{I + \langle s \rangle}{\langle s \rangle}}{\frac{I^2 + \langle s \rangle}{\langle s \rangle}} \simeq \frac{I + \langle s \rangle}{I^2 + \langle s \rangle} \simeq \frac{I}{I^2}.$$

Since I/I^2 is generated by n elements we can choose $a_1(X), \ldots, a_n(X) \in I$ such that $\langle a_1(X), \ldots, a_n(X) \rangle + I^2 = I$, so that $\overline{a_1(X)}, \ldots, \overline{a_n(X)}$ generate $\overline{I}/\overline{I}^2$. We have

$$n \geq \dim(A) + 1 \geq \dim(A[X]) - 1 + 1 \geq \dim\left(\frac{A[X]}{sA[X]}\right) + 1.$$

By Theorem 3.1.11, we can choose $b_1(X), \ldots, b_n(X) \in I$ such that $\overline{b_1(X)}, \ldots, \overline{b_n(X)}$ generate $\overline{I}$. Therefore, $\langle b_1(X), \ldots, b_n(X), s \rangle = I$. Since $s \in J^2 \subset I^2$, by Lemma 3.1.16, we can choose $c_i(X) \in A[X]$ such that if $d_i(X) = b_i(X) + sc_i(X)$, then $\langle d_1(X), \ldots, d_n(X) \rangle = I \cap I_1$, where $I_1 + sA[X] = A[X]$ and $\mathrm{ht}(I_1) \geq n \geq d+1$.

It follows from Lemma 2.8.3 that I_1 contains a monic polynomial and hence using Lemma 3.3.1, we get $\langle s \rangle + I_1 \cap A = A$. Thus, $I_1 \cap A$ contains an element of the form $1 + sa$ for some $a \in A$. Let $S = \langle 1 + sA \rangle$. Then $S^{-1}I_1 = S^{-1}A[X]$ and hence

$$S^{-1}\langle d_1(X), \ldots, d_n(X) \rangle = S^{-1}I \cap S^{-1}I_1 = I_S$$

By Lemma (4.1.3), there exists $g \in A$ such that $I_{1+sg} = \langle d_1(X), \ldots, d_n(X) \rangle_{1+sg}$. Also, since $s \in I$, $1 \in I_s$. Therefore, we have surjections: $f : A_{1+sg}[X]^n \twoheadrightarrow I_{1+sg}$, sending

$e_i \mapsto d_i(X)$ and $f' : A_s[X]^n \twoheadrightarrow I_s$, sending $e_1 \mapsto 1$, $e_i \mapsto 0$ for $i > 1$. By Lemma 4.1.2, $\dim(A_{sS}) < \dim(A) = d$. Hence, $n \geq d+1 = d-1+2 \geq \dim(A_{sS})+2$. Let $B = A_{sS}[X]$. Since $s \in I$, $I_{sS} = A_{sS}[X]$. Since $S^{-1}\langle d_1(X), \ldots, d_n(X)\rangle = I_S$, it follows that the row $[d_1(X), \ldots, d_n(X)]$ is unimodular in $A_{sS}[X]$. By Lemma 2.8.4, there exists a matrix $\sigma(X,T) \in GL_n(B[T])$ such that $\sigma(X,0) = I_n$ (which implies that $\sigma(X,T) \in SL_n(B[T])$) and

$$\sigma(X,1)\begin{pmatrix} d_1(X) \\ d_2(X) \\ . \\ . \\ d_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Since $\sigma \in SL_n(A_{sS}[X,T])$, we obtain $c \in A$ such that $\sigma(X,T) \in SL_n\left(A_{s(1+sc)}[X,T]\right)$. Let $1 + sh = (1 + sc)(1 + sg)$. Then we have the following commutative diagram.

$$\begin{array}{lll} A_{s(1+sh)}[X]^n & \xrightarrow{\quad\widehat{f}\quad} & I_{s(1+sh)} \qquad = \langle d_1(X), \ldots, d_n(X)\rangle \\ {\scriptstyle\sigma(X,1)}\uparrow & & \| \\ A_{s(1+sh)}[X]^n & \xrightarrow{\quad\widehat{f'}\quad} & I_{s(1+sh)} \qquad = \langle 1, 0, \ldots, 0\rangle \end{array}$$

where $\widehat{f}$, $\widehat{f'}$ are induced by f and f'. Since $\sigma(X,0) = I_n$, by 2.6.5, $\sigma(X,1)$ splits. Using 3.2.4, it follows that I is generated by n elements. □

Now we give another proof of the Theorem 4.2.1, in which we need not assume that $\mathrm{ht}(I) \geq 2$.

Theorem 4.2.2 *Let A be a Noetherian domain with $\dim(A) = d$. Let I be an ideal of $A[X]$. Suppose I/I^2 is generated by n elements, where $n \geq d+1$. Then I is generated by n elements.*

Proof. Let S' be the multiplicative closed subset $A - \{0\}$. Then ${S'}^{-1}A$ is a field and hence ${S'}^{-1}A[X]$ is a PID. So, there exists an element $g(X) \in I$ such that the ideal ${S'}^{-1}I$ of ${S'}^{-1}A[X]$ is generated by $g(X)$. Using Lemma 4.1.3, we choose $s \in S'$ such that $I_s = \langle g(X)\rangle_s$. Let $f(X) \in I^2$, $f(X) \neq 0$ and $sf(X) = h(X)$. Then $h(X) \neq 0$, as A is a domain. Since $h(X) \neq 0$, $\dim\left(A[X]/\langle h(X)\rangle\right) \leq d$. Now, consider the natural surjection $A[X] \twoheadrightarrow A[X]/\langle h(X)\rangle$. Since I/I^2 is generated by n elements, $\overline{I}/\overline{I}^2$ is also generated by n elements, where bar denote the reduction modulo $h(X)$. As $n \geq \dim\left(A[X]/\langle h(X)\rangle\right) + 1$, using Theorem 3.1.11, $\overline{I}$ is generated by n elements, say $\overline{a_1(X)}, \ldots, \overline{a_n(X)}$. Hence $I = \langle a_1(X), \ldots, a_n(X), h(X)\rangle$, where $h(X) \in I^2$. Applying Lemma 3.1.16, we can find $c_1(X), \ldots, c_n(X)$ in $A[X]$ such that

$$\langle a_1(X) + c_1(X)h(X), \ldots, a_n(X) + c_n(X)h(X)\rangle = I \cap I_1,$$

where $\mathrm{ht}(I_1) \geq d+1$ and $\langle h(X)\rangle + I_1 = A[X]$. Since $h(X) = sf(X)$, $sA[X] + I_1 = A[X]$. Let $b_i(X) = a_i(X) + c_i(X)h(X)$, $1 \leq i \leq n$.

Since $\mathrm{ht}(I_1) \geq d+1$, by Lemma 2.8.3, I_1 contains a monic polynomial and hence using Lemma 3.3.1, we get $\langle s\rangle + I_1 \cap A = A$. Thus, $I_1 \cap A$ contains an element of the form $1 + sa$, where $a \in A$. Let $S = 1 + sA$. Then $S^{-1}I_1 = S^{-1}A[X]$. Since $\langle b_1(X), \ldots, b_n(X)\rangle = I \cap I_1$, $S^{-1}I = I_S = S^{-1}\langle b_1(X), \ldots, b_n(X)\rangle$. Therefore, there are surjections: $A_S[X]^n \twoheadrightarrow I_S$, sending $e_i \mapsto b_i(X)$ and $A_s[X]^n \twoheadrightarrow I_s$, sending $e_1 \mapsto g(X)$, $e_i \mapsto 0$ for $i > 1$.

These two surjections induce surjections $A_{sS}[X]^n \twoheadrightarrow I_{sS}$, sending $e_i \mapsto b_i(X)$ and $A_{sS}[X]^n \twoheadrightarrow I_{sS}$, sending $e_1 \mapsto g(X)$, $e_i \mapsto 0$ for $i > 1$. Since $\langle b_1(X), \ldots, b_n(X)\rangle_{sS} = I_{sS} = \langle g(X)\rangle_{sS}$, we have $b_i(X) = g(X)f_i(X)$, where $f_i(X) \in A_{sS}[X]$ $(1 \leq i \leq n)$. By Lemma 4.1.1, $[f_1(X), \ldots, f_n(X)]$ is unimodular row in the ring $A_{sS}([X])$. As in (4.2.2), we see that there exists a matrix $\sigma(X,T) \in SL_n(A_{sS}[X,T])$ such that $\sigma(X,0) = I_n$ and

$$\sigma(X,1)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

$$\text{Hence } \sigma(X,1)\begin{pmatrix} b_1(X) \\ b_2(X) \\ . \\ . \\ b_n(X) \end{pmatrix} = \begin{pmatrix} g(X) \\ 0 \\ . \\ . \\ 0 \end{pmatrix}.$$

Now, proceeding as in Theorem 4.2.1, we see that I is generated by n elements. □

Corollary 4.2.3 (Forster's Conjecture) *Let k be a field and $\mathfrak{p} \subset A = k[X_1, \ldots, X_n]$ be a prime ideal such that $A/\mathfrak{p}$ is regular. Then $\mathfrak{p}$ is generated by n elements.*

Proof. By the Forster-Swan theorem, $\mathfrak{p}/\mathfrak{p}^2$ is generated by n elements. The corollary now follows from 4.2.2. □

4.3 On a variant of Mandal's Theorem

Let A be a Noetherian ring. Let $I \subset A[X]$ be an ideal. Then we have the following diagram :

$$\begin{array}{ccc} I & \longrightarrow & I/I^2 \\ \downarrow{\scriptstyle X=0} & & \downarrow{\scriptstyle X=0} \\ I(0) & \longrightarrow & I(0)/I(0)^2 \end{array}$$

Suppose I contains a monic polynomial and I/I^2 is generated by n elements, where $n \geq \dim(A[X]/I)+2$. Then by Theorem (3.3.2), I is generated by n elements. Therefore, $I(0)$ is also generated by n elements. Let $a_1, \ldots, a_n$ generate $I(0)$. It is a quite natural to ask whether $a_1, \ldots, a_n$ can be lifted to a set of generators of I. We have the following theorem due to Mandal. This says that the answer to the above question is affirmative if the corresponding set of generators $\overline{a_1}, \ldots, \overline{a_n}$ of $I(0)/I(0)^2$ can be lifted to generators $\overline{g_1(X)}, \ldots, \overline{g_n(X)}$ of I/I^2.

Theorem 4.3.1 (*cf.* [19]) *Let A be a Noetherian ring. Let $I \subset A[X]$ be an ideal containing a monic polynomial. Suppose I/I^2 is generated by n elements, where $n \geq \dim(A[X]/I)+2$. Suppose $I(0) = \langle a_1, \ldots, a_n\rangle$ and the generators $\overline{a_1}, \ldots, \overline{a_n}$ of $I(0)/I(0)^2$ can be lifted to the generators $\overline{g_1(X)}, \ldots, \overline{g_n(X)}$ of I/I^2. Then there exist a set of generators $\eta_1(X), \ldots, \eta_n(X)$ of I such that $\eta_i(0) = a_i$.*

Proof. By hypothesis, $\langle g_1(X), \ldots, g_n(X)\rangle + I^2 = I$ and $g_i(0) - a_i \in I(0)^2$. Now, we split the proof of the theorem in four steps.

Step 1. In this step we change $g_i(X)$ to $h_i(X)$ for $1 \leq i \leq n$, so that

$$\big\langle h_1(X), \ldots, h_n(X) \big\rangle + I^2 = I \tag{22}$$

and $h_i(0) = a_i$ for $1 \leq i \leq n$. We consider the elements $a_i - g_i(0)$. Note that $a_i - g_i(0) \in I(0)^2$. Since there is a natural surjection $I^2 \to I(0)^2$, there exists $\lambda_i(X) \in I^2$ such that $\lambda_i(0) = a_i - g_i(0)$, $1 \leq i \leq n$. We set $h_i(X) = \lambda_i(X) + g_i(X)$. Then $h_i(0) = a_i$ and since $\lambda_i(X) \in I^2$, $h_i(X) \equiv g_i(X)$ modulo I^2. Further, by choosing a monic polynomial $f \in I$ and replacing h_1 by $h_1 + Xf^p$ for large $p > 1$, we may assume that h_1 is monic.

Step 2. In this step we shall prove that $\big\langle h_1(X), \ldots, h_n(X) \big\rangle + I^2X = I$. Suppose the left hand side is equal to K. Using Lemma 3.1.5, it is enough to show that (i) $K + I^2 = I$ (ii) $V(K) = V(I)$. Since $h_i(X) \in K$, (i) follows from (22). Also, $K \subset I$ implies $V(I) \subset V(K)$. So, to prove (ii) we have to show that $V(K) \subset V(I)$.

Let $\mathfrak{p} \in V(K)$. Then $I^2X \subset \mathfrak{p}$. Hence $\mathfrak{p} \supset I^2$ or $X \in \mathfrak{p}$. If $\mathfrak{p} \supset I^2$ then as $\mathfrak{p}$ is a prime ideal, $\mathfrak{p} \supset I$. On the other hand if $X \in \mathfrak{p}$, then $\mathfrak{p} \supset \big\langle h_1(0), \ldots, h_n(0) \big\rangle$. Hence $\mathfrak{p} \supset \big\langle I(0), X \big\rangle \supset I$. Thus, $V(K) \subset V(I)$.

Step 3. By Lemma 3.1.9, it follows that there exists some $d(X) \in I^2X$ such that $\big\langle h_1(X), \ldots, h_n(X), d(X) \big\rangle = I$. Let $J = I \cap A$. Now, we consider the ring $S = \frac{A[X]}{\big\langle J^2[X], h_1(X) \big\rangle}$.

Let bar denote reduction modulo $\big\langle J^2[X], h_1(X) \big\rangle$. Since $n \geq \dim\big(A[X]/I\big) + 2$, as in 3.3.2, $n - 1 \geq \dim(S) + 1$. Since $\overline{I} = \big\langle \overline{h_2(X)}, \ldots, \overline{h_n(X)}, \overline{d(X)} \big\rangle$, where $\overline{d(X)} \in \overline{I^2}$, using 3.1.16, we can find $\lambda_i(X) \in A[X]$, $2 \leq i \leq n$, such that $\overline{I} = \big\langle \overline{h_2'(X)}, \ldots, \overline{h_n'(X)} \big\rangle$, where $h_i'(X) = h_i(X) + \lambda_i(X)d(X)$. Note that since $d(X) \in I^2X$, $h_i'(0) = h_i(0) = a_i$. Therefore, $\big\langle h_1(X), h_2'(X), \ldots, h_n'(X) \big\rangle + J^2[X] = I$. By Lemma 3.1.9,

$$\big\langle h_1(X), h_2'(X), \ldots, h_n'(X) \big\rangle = I \cap I',$$

where $I' + J^2[X] = A[X]$. Since $h_1(X) \in I'$ is monic, by Lemma 3.3.1, $I' \cap A + J^2 = A$.

Step 4. It is clear from Step 3, that I' contains an element of the form $1+j$, where $j \in J$. Therefore, $(I \cap I')_{1+j} = I_{1+j} = \big\langle h_1(X), h_2'(X), \ldots, h_n'(X) \big\rangle$. Also, $j \in J = I \cap A$ implies that $I_j = A_j[X]$. Since $j \in J$, $j \in I(0) = \big\langle a_1, \ldots, a_n \big\rangle$, $j = \sum_{i=1}^n \lambda_i a_i$, for some $\lambda_i \in A$. That means $1 = \sum_{i=1}^n \frac{\lambda_i}{j} a_i \in I(0)_j$. Therefore, we have surjections: $A_{1+j}[X]^n \twoheadrightarrow I_{1+j}$ sending $e_1 \mapsto h_1(X)$ and $e_i \mapsto h_i'(X)$ for $2 \leq i \leq n$, and $A_j[X]^n \twoheadrightarrow I_j = A_j[X]$ sending $e_i \mapsto a_i$. These two maps induce surjections; $A_{j(1+j)}[X]^n \twoheadrightarrow I_{j(1+j)} = A_{j(1+j)}[X]$ *viz.* $e_1 \mapsto h_1(X)$, $e_i \mapsto h_i'(X)$ for $2 \leq i \leq n$. $A_{j(1+j)}[X]^n \twoheadrightarrow I_{j(1+j)} = A_{j(1+j)}[X]$ *viz.* $e_i \mapsto a_i$. Let $f_1(X) = h_1(X)$ and $f_i(X) = h_i'(X)$ for $2 \leq i \leq n$. We have two unimodular rows $[f_1(X), f_2(X), \ldots, f_n(X)]$ and $[a_1, \ldots, a_n]$ in $A_{j(1+j)}[X]$ such that $f_i(0) = a_i$. Since $f_1(X)$ is monic, by Lemma 2.7.4, there exists $\tau(X) \in GL_n(A_{j(1+j)}[X])$ such that $\tau(0) = I_n$ and

$$\tau(X) \begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix}.$$

This implies that $\tau(X) = \tau_1(X)\tau_2(X)$, where $\tau_2(X) \in GL_n(A_{1+j}[X])$ with $\tau_2(0) = I_n$ and $\tau_1(X) \in GL_n(A_j[X])$ with $\tau_1(0) = I_n$. Let

$$\tau_2(X)\begin{pmatrix} f_1(X) \\ f_2(X) \\ . \\ . \\ f_n(X) \end{pmatrix} = \begin{pmatrix} \mu_1(X) \\ \mu_2(X) \\ . \\ . \\ \mu_n(X) \end{pmatrix} \text{ and } \tau_1(X)^{-1}\begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_n \end{pmatrix} = \begin{pmatrix} \nu_1(X) \\ \nu_2(X) \\ . \\ . \\ \nu_n(X) \end{pmatrix}.$$

Then $\langle \mu_1(X), \ldots, \mu_n(X) \rangle = I_{1+j}$, and $\langle \nu_1(X), \ldots, \nu_n(X) \rangle = I_j$ and $\mu_i(X) = \nu_i(X)$ in $I_{j(1+j)}$. Let $\eta_i(X) \in I$, be the pull back of $(\mu_i(X), \nu_i(X))$. By 3.2.3, it follows that $I = \langle \eta_1(X), \ldots, \eta_n(X) \rangle$. Since $\tau_1(0) = \tau_2(0) = I_n$, $\mu_i(0) = f_i(0) = a_i$ and $\nu_i(0) = a_i$. Since $\eta_i(X) \in I$ is the pullback of $(\mu_i(X), \nu_i(X))$, $\eta_i(0) \in I(0)$ is the pullback of (a_i, a_i). Therefore, $\eta_i(0) = a_i$. This completes the proof. □

Appendix

Some topological examples: There are many useful analogies between topology and algebra. This appendix contains some topological examples. Some of these examples show that the various assumptions made in proving some of the theorems in this paper cannot be dropped. The facts in Topology used in this section are contained in [25].

Let A be a ring and $I \subset A$ is an ideal. The following example shows that the canonical map $SL_2(A) \to SL_2(A/I)$ is not surjective. Before proving this we prove the following useful lemmas.

Lemma 4.3.2 *Let A be a field or a local ring. Then $SL_n(A) = E_n(A)$.*

Proof. We prove the lemma by induction on n. Let $\alpha \in SL_n(A)$. We show that there exist $\beta, \gamma \in E_n(A)$ such that $\beta\alpha\gamma = I_n$. It follows that $\alpha = \beta^{-1}\gamma^{-1} \in E_n(A)$. It is enough to show that one can transform α to I_n by performing elementary row and column operations. Using 2.1.7, we can transform the first column of α to $(1, 0, \ldots, 0)^t$. Thus, there exists $\beta_1 \in E_n(A)$ such that

$$\beta_1\alpha = \begin{pmatrix} 1 & * \\ 0 & \tau \end{pmatrix}$$

(where $\tau \in SL_{n-1}(A)$). Using 2.1.6, we can transform the first row of $\beta_1\alpha$ to $(1, 0, \ldots, 0)$. Thus,

$$\beta_1\alpha\gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & \tau \end{pmatrix}$$

where $\gamma_1 \in E_n(A)$. Now, by induction there exist $\beta_2, \gamma_2 \in E_{n-1}(A)$ such that $\beta_2\tau\gamma_2 = I_{n-1}$. Let $\beta_2' = \begin{pmatrix} 1 & 0 \\ 0 & \beta_2 \end{pmatrix}$ and $\gamma_2' = \begin{pmatrix} 1 & 0 \\ 0 & \gamma_2 \end{pmatrix}$. Then $\beta_2'\beta_1\alpha\gamma_1\gamma_2' = I_n$. Setting $\beta = \beta_2'\beta_1$ and $\gamma = \gamma_1\gamma_2'$ the lemma follows. □

Lemma 4.3.3 *The group $SL_n(\mathbb{R})$ is path connected.*

Proof. By Lemma 4.3.2, $SL_n(\mathbb{R}) = E_n(\mathbb{R})$. Therefore, any $\sigma \in SL_n(\mathbb{R})$ can be written as $\sigma = \Pi_{i=1}^k E_{ij}(\lambda)$, $\lambda \in \mathbb{R}$. The map $[0, 1] \to SL_n(\mathbb{R})$ given by $t \mapsto \Pi_{i=1}^k E_{ij}(\lambda t)$ gives a path from I_n to σ, showing that $SL_n(\mathbb{R})$ is path connected. □

Definition 4.3.4 The group $O_n(\mathbb{R})$ is the subgroup of $SL_n(\mathbb{R})$ consisting of matrices $\alpha \in SL_n(\mathbb{R})$ such that $\alpha\alpha^t = I_n$. We define $SO_n(\mathbb{R}) = SL_n(\mathbb{R}) \cap O_n(\mathbb{R})$.

Example 4.3.5 (See 2.1.13)

We consider the ring $\mathbb{R}[X, Y, Z, T]$ and its ideal $\langle XY - ZT - 1\rangle$. Then the natural map

$$SL_2(\mathbb{R}[X, Y, Z, T]) \to SL_2\left(\frac{\mathbb{R}[X, Y, Z, T]}{\langle XY - ZT - 1\rangle}\right)$$

is not surjective. In fact, there is no lift of the matrix

$$\begin{pmatrix} \overline{X} & \overline{Z} \\ \overline{T} & \overline{Y} \end{pmatrix} \in \frac{SL_2(\mathbb{R}[X, Y, Z, T])}{\langle XY - ZT - 1\rangle}$$

to a matrix belonging to $SL_2(\mathbb{R}[X, Y, Z, T])$. We give a proof due to C.P. Ramanujam, *cf.* ([30], pg. 11).

Suppose to the contrary there exists $\tau \in SL_2(\mathbb{R}[X, Y, Z, T])$ such that

$$\tau = \begin{pmatrix} f_{11}(X, Y, Z, T) & f_{12}(X, Y, Z, T) \\ f_{21}(X, Y, Z, T) & f_{22}(X, Y, Z, T) \end{pmatrix} \text{ lifts } \begin{pmatrix} \overline{X} & \overline{Z} \\ \overline{T} & \overline{Y} \end{pmatrix}.$$

This implies that

$$1)\ f_{11}(X, Y, Z, T) - X = (XY - ZT - 1)h_{11}(X, Y, Z, T)$$
$$2)\ f_{12}(X, Y, Z, T) - Z = (XY - ZT - 1)h_{12}(X, Y, Z, T)$$
$$3)\ f_{21}(X, Y, Z, T) - T = (XY - ZT - 1)h_{21}(X, Y, Z, T)$$
$$4)\ f_{22}(X, Y, Z, T) - Y = (XY - ZT - 1)h_{22}(X, Y, Z, T)$$

where $h_{ij}(X, Y, Z, T) \in \mathbb{R}[X, Y, Z, T]$. We now define a map $r : M_2(\mathbb{R}) \to SL_2(\mathbb{R})$ as follows:

$$r\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} f_{11}(a, b, c, d) & f_{12}(a, b, c, d) \\ f_{21}(a, b, c, d) & f_{22}(a, b, c, d) \end{pmatrix}.$$

In view of equations 1, 2, 3, 4, if $ad - bc = 1$, $r\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Hence the map $r : M_2(\mathbb{R}) \to SL_2(\mathbb{R})$ is a retraction.

Therefore, the map $r_* : \pi_1(M_2(\mathbb{R}), I_2) \to \pi_1(SL_2(\mathbb{R}), I_2)$ is surjective. Now, since $M_2(\mathbb{R}) \approx \mathbb{R}^4$, $\pi_1(M_2(\mathbb{R}), I_2)$ is a trivial group. We prove that $\pi_1(SL_2(\mathbb{R}), I_2)$ is not a trivial group and that will yield the required contradiction.

There is an inclusion map $i : SO_2(\mathbb{R}) \hookrightarrow SL_2(\mathbb{R})$. Using the Gram-Schmidt orthogonalization process we get a map $r' : SL_2(\mathbb{R}) \to O_2(\mathbb{R})$. Note that $r'(\tau) = \tau$ if $\tau \in SO_2(\mathbb{R})$. We also have the determinant map $\det : O_2(\mathbb{R}) \to \{1, -1\}$. As $SL_2(\mathbb{R})$ is path connected and $\det(r'(I_2)) = 1$, the image of $\det(r') = \{1\}$. This shows that $r'(SL_2(\mathbb{R})) = SO_2(\mathbb{R})$ and $r' : SL_2(\mathbb{R}) \to SO_2(\mathbb{R})$ is a retraction. So, we have surjection

$$(r')_* : \pi_1(SL_2(\mathbb{R}), I_2) \to \pi_1(SO_2(\mathbb{R}), I_2).$$

The homeomorphism, $j : S^1 \to SO_2(\mathbb{R})$ given by

$$(\cos\theta, \sin\theta) \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

shows that $\pi_1(SO_2(\mathbb{R}), I_2) \cong \pi_1(S^1, e) \cong \mathbb{Z}$. Therefore, it follows that $\pi_1(SL_2(\mathbb{R}), I_2)$ is not trivial. Hence the result follows. □

Example 4.3.6 We consider the ring $\mathbb{R}[X,Y]$ and its ideal $\langle X^2+Y^2-1\rangle$. There exists a natural map

$$SL_2(\mathbb{R}[X,Y]) \to SL_2\left(\frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle}\right).$$

We claim that there is no lift of the matrix

$$\begin{pmatrix} \overline{X} & \overline{Y} \\ -\overline{Y} & \overline{X} \end{pmatrix} \in SL_2\left(\frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle}\right)$$

to a matrix belonging to $SL_2(\mathbb{R}[X,Y])$. Assume to the contrary we get a lift

$$\tau = \begin{pmatrix} f_{11}(X,Y) & f_{12}(X,Y) \\ f_{21}(X,Y) & f_{22}(X,Y) \end{pmatrix} \text{ of } \begin{pmatrix} \overline{X} & \overline{Y} \\ -\overline{Y} & \overline{X} \end{pmatrix}$$

where $\tau \in SL_2(\mathbb{R}[X,Y])$. This implies that

$$1)\ f_{11}(X,Y) - X = (X^2+Y^2-1)h_{11}(X,Y)$$

$$2)\ f_{12}(X,Y) - Y = (X^2+Y^2-1)h_{12}(X,Y)$$

$$3)\ f_{21}(X,Y) + Y = (X^2+Y^2-1)h_{21}(X,Y)$$

$$4)\ f_{22}(X,Y) - X = (X^2+Y^2-1)h_{22}(X,Y)$$

where $h_{ij}(X,Y) \in \mathbb{R}[X,Y]$. We define a map $r : \mathbb{R}^2 \to SL_2(\mathbb{R})$ given by

$$(a,b) \mapsto \begin{pmatrix} f_{11}(a,b) & f_{12}(a,b) \\ f_{21}(a,b) & f_{22}(a,b) \end{pmatrix}.$$

Note that, in view of 1,2,3,4, if $a^2+b^2=1$, then $r(a,b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. As in 4.3.5, we get a retraction $r' : SL_2(\mathbb{R}) \to SO_2(\mathbb{R})$ and homeomorphism $j : S^1 \to SO_2(\mathbb{R})$. One can verify that the composite map $\alpha = j^{-1}.r'.r : \mathbb{R}^2 \to S^1$ is a retraction. This implies that $\alpha_* : \pi_1(\mathbb{R}^2) \to \pi_1(S^1)$ is surjective. But, $\pi_1(S^1) \cong \mathbb{Z}$ and $\pi_1(\mathbb{R}^2)$ is trivial. This is a contradiction, hence the claim. □

Example 4.3.7 Let us consider the ring $A = \frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle}$ and the maximal ideal $\mathfrak{m} = \langle x-1, y\rangle$ of A. Since $(x-1)(x+1) = -y^2 \in \mathfrak{m}^2$, it follows that $(x-1) \in \mathfrak{m}^2$ and hence $\mathfrak{m}/\mathfrak{m}^2$ is generated by one element. We show that $\mathfrak{m}$ is not principal. This shows that Question 2 raised in the introduction is not valid in general.

Algebraic Proof. We have an inclusion

$$A = \frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle} \hookrightarrow \frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle} = B$$

The change of variables $X+iY = U$ and $X-iY = V$ gives an isomorphism

$$\frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle} \cong \frac{\mathbb{C}[U,V]}{\langle UV-1\rangle}.$$

We claim that

$$\frac{\mathbb{C}[U,V]}{\langle UV-1\rangle} \cong \mathbb{C}[U,U^{-1}].$$

For, we have surjective map

$$\phi : \frac{\mathbb{C}[U,V]}{<UV-1>} \to \mathbb{C}[U,U^{-1}]$$

viz. $U \mapsto U$, $V \mapsto U^{-1}$. We want to define a map in opposite direction. Let S be the multiplicative closed subset $\{1, U, U^2, \dots\}$ of $\mathbb{C}[U]$. Clearly, U is unit in $\frac{\mathbb{C}[U,V]}{\langle UV-1\rangle}$. So, $U \to \overline{U}$ gives a homomorphism

$$\mathbb{C}[U] \to \frac{\mathbb{C}[U,V]}{\langle UV-1\rangle}.$$

Therefore, there exists a homomorphism

$$S^{-1}\mathbb{C}[U] = \mathbb{C}[U,U^{-1}] \to \frac{\mathbb{C}[U,V]}{\langle UV-1\rangle}.$$

It can be easily shown that the composites are identity, proving the claim.

Since $\mathbb{C}[U,U^{-1}]$ is a PID, the image of $\mathfrak{m}$ in $\frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle} \simeq \mathbb{C}[U,U^{-1}] = B$ is a principal ideal. We compute the generator. Since $X+iY = U$, $X-iY = U^{-1}$, we see that $X = \frac{U+U^{-1}}{2}$, $Y = \frac{U-U^{-1}}{2i}$. Hence $\mathfrak{m}B = S^{-1}I$, where $I = \langle U^2-2U+1, U^2-1\rangle = \langle U-1\rangle$.

One can easily check that the units of $\mathbb{C}[U,U^{-1}]$ are precisely the set $\{\lambda U^n | \lambda \in \mathbb{C}^*, n \in \mathbb{Z}\}$. Now, we make a general remark. Suppose $A \hookrightarrow B$ is an extension of domains and $J \subset A$ is an ideal such that $JB = \langle c\rangle$, where $c \in B$. Suppose $J = dA$, $d \in A$, then there exists a unit $\mu \in B$ such that $d = \mu c$.

Applying the above remark to the rings $A = \frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle}$ and $B = \frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle}$, we see that in order to prove that $\mathfrak{m}$ is not principal it is enough to show that for $\lambda \in \mathbb{C}^*$, and $n \in \mathbb{Z}$ the element $\lambda U^n(U-1)$ does not belong to the image of $\frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle}$ in $\frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle}$. Now, complex conjugation σ of $\mathbb{C}$ induces a ring isomorphism

$$\sigma : \frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle} \to \frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle}.$$

We have $\sigma(g) = g$, if and only if $g = \frac{g+\sigma(g)}{2}$ belongs to the image of $\frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle}$ in the ring $\frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle}$. Since $\sigma(X+iY) = X-iY$, $\sigma(U) = U^{-1}$.

Thus, if $\lambda U^n(U-1)$ belongs to the image of $\frac{\mathbb{R}[X,Y]}{\langle X^2+Y^2-1\rangle}$ in $\frac{\mathbb{C}[X,Y]}{\langle X^2+Y^2-1\rangle}$, then we get $\lambda U^n(U-1) = \overline{\lambda}U^{-n}(U^{-1}-1)$. This implies that $\lambda U^{2n+1} = -\overline{\lambda}$. This is a contradiction. This proves that $\mathfrak{m}$ is not principal. □

Topological Proof. Since $x-1 \in \mathfrak{m}$, $\mathfrak{m}_{(x-1)} = A_{(x-1)}$. Therefore, we have a surjection $f_1 : A_{(x-1)} \twoheadrightarrow \mathfrak{m}_{(x-1)}$, sending e_1 to 1. Since $(x+1)(x-1) \in \langle y\rangle$, $\mathfrak{m}_{(x+1)} = \langle y\rangle$ and hence we have a surjection $f_2 : A_{(x+1)} \twoheadrightarrow \mathfrak{m}_{(x+1)}$, sending e_1 to y. These two maps induce surjections $\widehat{f_1}, \widehat{f_2} : A_{(x+1)(x-1)} \twoheadrightarrow \mathfrak{m}_{(x+1)(x-1)} = A_{(x+1)(x-1)}$.

Suppose to the contrary that $\mathfrak{m} \subset A$ is principal, generated by $g \in A$. Then $y = gh_1$ and $1 = gh_2$, where h_1 is a unit of $A_{(x+1)}$ and h_2 is a unit of $A_{(x-1)}$. Therefore, $y = h_1 h_2^{-1} = h_1 h_3$, where h_3 is a unit of $A_{(x-1)}$. We write $h_1 = \frac{\lambda(x,y)}{(x+1)^n}$, $\lambda(x,y) \in A$. Since h_1 is a unit of $A_{(x+1)}$, there exists $\mu(x,y) \in A$ such that

$$\frac{\lambda(x,y)}{(x+1)^n}\frac{\mu(x,y)}{(x+1)^m} = 1.$$

Note that $\lambda(x,y), \mu(x,y)$ define functions from S^1 to $\mathbb{R}$ and $\frac{\lambda(x,y)}{(x+1)^n}$, $\frac{\mu(x,y)}{(x+1)^n}$ define functions from $S^1 - \{(1,0)\}$ to $\mathbb{R}$. Therefore, $\frac{\lambda(a,b)}{(a+1)^n} \neq 0$ for all $(a,b) \in S^1 - \{(-1,0)\}$, *i.e.* $h_1(a,b) \neq 0$ for all $(a,b) \in S^1 - \{(-1,0)\}$.

Since h_1 is continuous and $S^1 - \{(1,0)\}$ is connected, by the Intermediate Value theorem, it follows that either $h_1(a,b) > 0$ for all $(a,b) \in S^1 - \{(-1,0)\}$ or $h_1(a,b) < 0$ for all $(a,b) \in S^1 - \{(-1,0)\}$. Similarly, we see that h_3 is either positive for all $(a,b) \in S^1 - \{(-1,0)\}$ or negative for all $(a,b) \in S^1 - \{(1,0)\}$. Therefore, $h_1 h_3$ is either positive on $S^1 - \{(-1,0)\} - \{(1,0)\}$ or negative on $S^1 - \{(-1,0)\} - \{(1,0)\}$. But $y > 0$ on the part of $S^1 - \{-1,0\} - \{1,0\}$ which is above the X-axis and $y < 0$ on the part of $S^1 - \{(-1,0)\} - \{(1,0)\}$ which is below the X-axis. This contradicts the fact that $h_1 h_3 = y$, proving that $\mathfrak{m}$ is not a principal ideal. □

We end this section with the following theorem. The proof we give is based on [38].

Theorem 4.3.8 *Let* $A = \frac{\mathbb{R}[X,Y,Z]}{\langle X^2+Y^2+Z^2-1\rangle}$. *Then, since* $x^2+y^2+z^2 = 1$, $(x,y,z) \in \mathrm{Um}_3(A)$. *There does not exist a matrix in* $SL_3(A)$ *having first row* (x,y,z).

To prove the theorem need a few definitions and lemmas.

Definition 4.3.9 A topological space Y is said to be contractible if the identity map $Y \to Y$ is homotopic to a constant map $Y \to Y$, (*i.e.* the map which sends every element of Y to a fixed element of Y).

Example 4.3.10 Let $S^2 = \{(a,b,c) \in \mathbb{R}^3 | a^2+b^2+c^2 = 1\}$ be the real two sphere. Let $P \in S^2$. Then, $S^2 - \{P\}$ is contractible.

We state some lemmas in generality we need them.

Lemma 4.3.11 *The map* $\alpha : S^1 \to SL_2(\mathbb{R})$ *given by*

$$\alpha(\cos\,\theta, \sin\,\theta) = \begin{pmatrix} \cos\,n\theta & -\sin\,n\theta \\ \sin\,n\theta & \cos\,n\theta \end{pmatrix}$$

is not homotopic to a constant map.

Proof. Let the notation be as in 4.3.5. Suppose to the contrary that α is homotopic to a constant map. Then so is the composite map $S^1 \xrightarrow{\alpha} SL_2(\mathbb{R}) \xrightarrow{r'} SO_2(\mathbb{R}) \xrightarrow{j^{-1}} S^1$. But, the composite map sends $z \in S^1$ to z^n. This map is not homotopic to a constant map. This yields a contradiction, proving the lemma. □

Lemma 4.3.12 *Let* $\alpha : S^1 \to SL_2(\mathbb{R})$ *and* $\beta : S^1 \to SL_2(\mathbb{R})$ *be continuous maps which are both homotopic to constant maps. Then* $\alpha\beta : S^1 \to SL_2(\mathbb{R})$ *is also homotopic to a constant map.* (Note that $\alpha\beta$ make sense as $SL_2(\mathbb{R})$ is a group).

Lemma 4.3.13 *Let $S^1 \subset X$, where X is a contractible topological space. Suppose $\alpha : S^1 \to SL_2(\mathbb{R})$ extends to a map $\lambda : X \to SL_2(\mathbb{R})$. Then α is homotopic to a constant map.*

Proof of Theorem (4.3.8)**.** Since $x^2+y^2+z^2 = 1$, $[z, x, y] \in \mathrm{Um}_3(A)$. Since $(z-1)$ is a unit of A_{z-1}, $[z(z-1), x, y] \in \mathrm{Um}_3(A_{z-1})$. Further, since $x^2+y^2+z^2 = 1$, we get $(z(z-1), x, y) \overset{E_3(A_{z-1})}{\sim} (1-z, x, y)$. Therefore,

$$(z, x, y) \overset{GL_3(A_{z-1})}{\sim} (z(z-1), x, y) \overset{E_3(A_{z-1})}{\sim} (1-z, x, y) \overset{E_3(A_{z-1})}{\sim} (1, 0, 0),$$

as $1-z$ is a unit of A_{z-1}. Thus, it follows that the row $[z, x, y]$ is completable in the ring A_{z-1}. We have a completion given by

$$\sigma = \begin{pmatrix} z & \frac{x}{z-1} & -\frac{y}{z-1} \\ x & -1 & 0 \\ y & 0 & 1 \end{pmatrix} \in SL_3(A_{z-1}).$$

Similarly, the row (z, x, y) is completable in the ring A_{z+1}. The matrix

$$\tau = \begin{pmatrix} z & -\frac{x}{z+1} & -\frac{y}{z+1} \\ x & 1 & 0 \\ y & 0 & 1 \end{pmatrix} \in SL_3(A_{z+1})$$

gives the completion. Since the first column of σ and τ are equal to (z, x, y), the matrix $\sigma^{-1}\tau$ has first column $(1, 0, 0)$ and

$$\sigma^{-1}\tau = \begin{pmatrix} 1 & * & * \\ 0 & \eta & \\ 0 & & \end{pmatrix}$$

where $\eta \in SL_2(A_{(z-1)(z+1)})$.

Now, we digress a little bit and introduce some notations which will be used in the rest of the proof. Since $\sigma \in SL_3(A_{z-1})$, we have a map $S^2 - (1, 0, 0) \to SL_3(\mathbb{R})$, sending (a, b, c) to $\sigma(a, b, c)$. (We denote the matrix $\sigma_{ij}(a, b, c)$ by $(\sigma(a, b, c))$).

Now, suppose $\beta \in SL_3(A)$ has first column (z, x, y). Then $\sigma^{-1}\tau = \sigma^{-1}\beta\beta^{-1}\tau$, where

$$\sigma^{-1}\beta = \begin{pmatrix} 1 & * & * \\ 0 & \eta_1 & \\ 0 & & \end{pmatrix} \text{ and } \beta^{-1}\tau = \begin{pmatrix} 1 & * & * \\ 0 & \eta_2 & \\ 0 & & \end{pmatrix}.$$

Note that $\eta_1 \in SL_3(A_{z-1})$ and $\eta_2 \in SL_3(A_{z+1})$. Since

$$\sigma^{-1}\tau = \begin{pmatrix} 1 & * & * \\ 0 & \eta & \\ 0 & & \end{pmatrix}$$

it follows that $\eta = \eta_1\eta_2$.

Let $U = S^2 - P$, where $P = (0, 0, 1)$ and $V = S^2 - Q$, where $Q = (0, 0, -1)$. Then, we have functions $\lambda_1 : U \to SL_2(\mathbb{R})$, sending (a, b, c) to $\eta_1(a, b, c)$, $\lambda_2 : V \to SL_2(\mathbb{R})$, sending (a, b, c) to $\eta_2(a, b, c)$ and $\lambda_3 : U \cap V \to SL_2(\mathbb{R})$, sending (a, b, c) to $\eta(a, b, c)$. A computation shows that

$$\eta|_{z=0} = \begin{pmatrix} x^2-y^2 & -2xy \\ 2xy & x^2-y^2 \end{pmatrix}.$$

If we restrict λ_3 to the equator S^1 we get a map $S^1 \to SL_2(\mathbb{R})$, given by

$$\lambda_3(\cos\,\theta, \sin\,\theta, 0) = \begin{pmatrix} \cos\,2\theta & -\sin\,2\theta \\ \sin\,2\theta & \cos\,2\theta \end{pmatrix}.$$

By Lemma 4.3.11, it follows that $\lambda_3|_{S^1}$ is not homotopic to constant map. But, since $\eta = \eta_1\eta_2$, it follows that $\lambda_3|_{S^1} = \lambda_1|_{S^1}.\lambda_2|_{S^1}$. Since λ_1 is defined on U, λ_2 is defined on V and U and V are contractible, by Lemma 4.3.13, $\lambda_1|_{S^1}$ and $\lambda_2|_{S^1}$ are homotopic to constant maps. Therefore, by Lemma 4.3.12, $\lambda_3|_{S^1}$ is homotopic to a constant map. This is a contradiction. Hence the theorem follows. □

References

[1] S. S. Abhyankar; Algebraic Space Curves. Sém. Math. Sup. 43, Les presses de l'université de Montréal (1971).

[2] S. S. Abhyankar; On Macaulay's Examples (Notes by A.Sathaye). In: Conf. Comm. Algebra; Lawrence (1972). Springer Lecture Notes in Math. 311 (1973), 1 - 16.

[3] M. F. Atiyah, I. G. Macdonald; Introduction to Commutative Algebra. Wesley, Reading, Mass. (1969).

[4] S. M. Bhatwadekar, R. A. Rao; Efficient Generation of Ideals in Polynomial Extensions of an Affine Domain. Unpublished manuscript.

[5] S. M. Bhatwadekar, Raja Sridharan; The Euler Class Group of a Noetherian Ring. Compositio Mathematica 122 (2000), 183 - 222.

[6] S. M. Bhatwadekar, Raja Sridharan; On Euler Classes and Stably Free Projective Modules. Proceedings of the International Colloquium on Algebra Geometry and Arithmetic, Mumbai 2000, Narosa Publishing House, pgs 139 - 158.

[7] D. Eisenbud; Commutative Algebra with a view Toward Algebraic Geometry. Springer, GTM 150 (1995).

[8] D. Eisenbud, E. G. Evans; Jr., Generating Modules Efficiently: Theorems from Algebraic K-Theory. J. Alg. 27 (1973), 278 - 315.

[9] O. Forster; Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring, Math.Z. 84 (1964), 80 - 87.

[10] N. S. Gopalakrishnan; Commutative Algebra. Oxonian Press, (1984).

[11] S. K. Gupta, M. P. Murthy; Suslin's work on linear groups over polynomial rings and Serre's problem. ISI Lecture Notes, no. 8 (1980).

[12] G. Horrocks; Projective modules over an extension of a local ring, Proc. London Math.Soc. 14 (1964), 714 - 718.

[13] I. Kaplansky; Commutative Rings. Allyn and Bacon, Boston (1970).

[14] L. Kronecker; Grundzuge einer arithmetischen Theorie der algebraischen Groben, J.reine angew. Math. 92 (1882), 1 - 123.

[15] E. Kunz; Introduction to Commutative Algebra and Algebraic Geometry; Birkhäuser, Boston (1985).

[16] T. Y. Lam; Serre's Conjecture. Lecture Notes in Mathematics (635), Springer - Verlag (1978).

[17] S. Lang; Algebra - Third Edition. Addison - Wesley (1993).

[18] S. Mandal; On efficient generation of ideals, Invent. Math. 46 (1978), 59 - 67.

[19] S. Mandal; Projective Modules and Complete Intersections. Lecture Notes in Mathematics (1672), Springer (1997).

[20] S. Mandal, Raja Sridharan; Euler Classes and complete intersections. Jornal of Mathematics of Kyoto University, Vol. 36, No. 3, (1996).

[21] H. Matsumura; Commutative Algebra, Second edition. Benjamin, New York (1980).

[22] Manoj Kumar Keshari; Euler Class Group of a Noetherian Ring. M.Phil Thesis, T.I.F.R, 2001.

[23] N. Mohan Kumar; On two conjectures about Polynomial Rings, Inv. Math. 46 (1978), 225 - 236.

[24] M. P. Murthy; Generators for Certain Ideals in Regular Rings of Dimension Three. Comm. Math. Helv. 47 (1972), 179 - 184.

[25] James R. Munkres; Topology, A first course. Prentice-Hall of India Private Limited (1996).

[26] Budh S. Nashier; Monic polynomials and generating ideals efficiently, Proc. Amer. Math. Soc. 95 (1985), 338 - 340.

[27] D. G. Northcott. Lessons on Rings, Modules and Multiplicities. Cambridge University Press (1968).

[28] C. Peskine; An introduction to Complex Projective Geometry, 1. Commutative Algebra. Cambridge University Press, Cambridge Studies in Advanced Mathematics vol. 47 (1996).

[29] D. Quillen; Projective Modules over Polynomial Rings. Inv. Math. 36 (1976), 167 - 171.

[30] C.P.Ramanujam; A TRIBUTE. Tata Institute of Fundamental Research Studies in Mathematics. Springer - Verlag, (1978).

[31] R. A. Rao; An elementary transformation of a special unimodular vector to its top coefficient vector. Proc. Amer. Math. Soc. 93 (1985), 21 - 24.

[32] D. Rees; Two Classical Theorems of Ideal Theory. Proc. Cambridge Philos. Soc. 52 (1956), 155 - 157.

[33] H. Sarges; Ein Beweis des Hilbertschen Basissatzes, J. reine angew. Math. 283/284 (1976), 436 - 437.

[34] A. Sathaye; On the Forster-Eisenbud-Evans Conjecture. Invent. Math. 46 (1978), 211-224.

[35] R. Y. Sharp; Steps in Commutative Algebra. London Mathematical Society Student Texts 19 (1990).

[36] Raja Sridharan; Non-vanishing sections of Algebraic Vector Bundles. J.Algebra.

[37] Raja Sridharan; Homotopy, the Codimension 2 Correspondence and Section of Rank 2 Vector Bundles. Journal of Algebra 176 (1995), 1001-1012.

[38] R. R. Simha; Spheres and Orthogonal Groups. Bombay Mathematical Colloquium, Bulletin vol. 14, Number 1, January 1998.

[39] A. A. Suslin; On Stably free modules, Math. USSR Sb. 31 (1977), 479 - 491.

[40] A. A. Suslin; Projective Modules over Polynomial Rings (Russian). Dokl. Akad. Nauk S. S. S. R. 26 (1976).

[41] R. Swan; The Number of Generators of a Module. Math. Z. 102 (1967), 318 - 322.

Rabeya Basu; School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India. email: rbasu@math.tifr.res.in, (Partially supported by the TIFR Endowment Fund).

Raja Sridharan; School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India. email: sraja@math.tifr.res.in