GRADUATE SEMINAR REPORT
ON

REGULAR RINGS

By

Berhanu Bekele

Advisor:
Dr. Demissu Gemeda

School Of Graduate Studies
Addis Ababa University

June, 1998
Addis Ababa

PREFACE

The general interest to study regular rings stems from the fact that the theory is important in both algebraic geometry and the theory of commutative algebra.

In this paper we study regular local rings and regular rings. In the first section we give some of the preliminary results required in the development of the theory. In the second section we give the difinition of regular local rings, a necessary and sufficient conditions for a noethenan local ring to be regular and finally the definition of regular rings. The last section is centered around the theorem that a regular local ring is a unique factorization domain (UFD).

I would like to record my gratitude to my advisor Dr. Demissu Gemeda for his critical reading of the paper and the assistance which he has given in correcting the proofs.

I would like to thank also my friends Mihirete Alemneh and Yohannes Taye for their encouragement and constructive suggestion to me.

Finally, I thank W/t Bizuayehu Adafre for a superb job of typing my paper.

Berhanu Bekele

June, 1998

C O N T E N T S

Page

1. Preliminaries

Lemma 1: Let A be a noetherian ring.

Let I be an ideal of A, p any maximal ideal of A. Then, I/Ip form, in a natural way, a finite dimensional vector space over the field A/p.

Note:- If (A, m, k) is a local ring , where m is the unique maximal ideal of A and $k = A/m$ and I a proper ideal of A, then by Lemma 1 I/Im is a finite dimensional vector space over k. Let us denote its dimension by $\text{rank}_k(I/Im)$.

Definition 1:- A prime ideal p is called a minimal prime over ideal of an ideal I, if it contains I, and if there is no prime ideal containing I which is strictly contained in p.

Lemma 2:- Let A be a noetherian ring, $(a_1, a_2, \ldots, a_n)$ a proper ideal of A and p minimal prime over ideal of $(a_1, a_2, \ldots, a_n)$. Then height of p is atmost n.

Lemma 3:- If p is a prime ideal (in a noetherian ring A) of height $r (r \geq 1)$, then it is possible to find r elements $a_1, a_2, \ldots, a_r$ such that p is a minimal prime over ideal of $(a_1, a_2, \ldots, a_r)$.

Lemma 4:- Suppose A is a noetherian ring and that I is a proper ideal of height r $(r \geq 1)$, then it is possible to find r elements $a_1, a_2, \ldots, a_r$ belonging to I such that if $1 \leq i \leq r$, then $(a_1, a_2, \ldots, a_i)$ is of height i.

Note:- If (A, m) is a noetherian local ring, by dim (A) we mean the coheight of the zero ideal or $\dim(A) = \text{ht}(m)$. Thus the dimension of a noetherian local ring is finite by Lemma 2, and every generator set of m contains atleast dim A elements.

Lemma 5:- Let (A, m, k) be a noetherian local ring.

Then, dim A is equal to the smallest number of non zero elements required to generate an m-primary ideal.

Proof:- Let d = dim A. We consider two cases.

Case 1:- Let d = 0

Then, A has only one proper prime ideal , and hence (0) is an m-primory ideal. Then since (0) is generated by ϕ or {0} , the number of non-zero elements needed to generate (0) is zero.

Hence, the Lemma holds.

Case 2. Let $d \geq 1$

Let $(a_1, a_2, \ldots, a_s)$ be an η-primary ideal.

WTS :- d = s

By Lemma 2, we have dim A = ht(m) ≤ s (since m is minimal prime over ideal of $(a_1, \ldots, a_s)$.

Furthermore, by Lemma 4, since $1 \leq d \leq s$, we can find d elements $b_1, b_2, \ldots, b_d$ contained in m such that $(b_1, b_2, \ldots, b_d)$ has height d. But since m is the only prime ideal of rank d, and no prime ideal has a larger height, $(b_1, b_2, \ldots b_d)$ must be m-primary.

⇒ the number of elements required to generate an m-primary ideal is d.

Hence, the proof.

Definition 2:- Let (A, m, k) be a noetherian local ring, I a proper ideal. If $I = (a_1, a_2, \ldots, a_n)$ and if no proper subset of $\{a_1, a_2, \ldots, a_n\}$ generates I then we say $a_1, a_2, \ldots, a_n$ is a minimal generator of I.

Lemma 6:- Let (A, m, k) be a noetherian local ring, I = proper ideal of A. Let , for $a \in I$, $\bar{a}$ denote the image of a in I/Im.

Then , $I = (a_1, a_2, \ldots, a_2)$ if and only if $I/Im = k\bar{a}_1 + k\bar{a}_2 + \ldots + k\bar{a}_s$. Further , the a_i form a minimal generator of I if and only if the $\bar{a}_i$ form a basis of I/Im over k, and every minimal generator of I contains exactly $\text{rank}_k(I/Im)$ elements.

2. Regular Rings

Let (A, m, k) = a noetherian local ring of dimension d.

Now, by lemma 5, there are d elements of m which generates a primary ideal belonging to m (or m-primary ideal), but there is no an m-primary ideal which is generated by d-1 elements.

Definition 3:- If $d \geq 1$, then the set of d elements $\{x_1, x_2, \ldots, x_d\}$ which generates an m-primary ideal is called a system of parameters in A.

(ii) A system of parameters $x_1, x_2, \ldots, x_d$ is called a regular system of parameters if it generates the maximal ideal of A.

Definition 4:- A noetherian local ring which has a regular system of parameters is called a regular local ring.

Equivalently, A noetherian local ring (A, m, k) is regular if $\dim A = \text{rank}_k(m/m^2)$.

To see this , since number of elements of a minimal generator of m is equal to $\text{rank}_k(m/m^2)$, we have ingeneral $\dim A \leq \text{rank}_k(m/m^2)$, and the equality holds if and only if A is regular.

Example:- The formal power series $A = K[[X_1, X_2, \ldots, X_n]]$ over a field k is a regular local ring.

Proof: We know that if k is a field, then A is a noetherian local ring and $m = (x_1, x_2, \ldots, x_s)$ is its maximal ideal (*)
Again observe that:

1) In $A = k[[x_1, x_2, \ldots, x_n]]$ any chain of prime ideals different from A has atmost n + 1 terms.
To see the existence consider $(0) \subseteq (x)_1 \subseteq \ldots \subseteq (x_1, x_2, \ldots, x_n)$.

2) Any chain $p_1 \subset p_2 \subset \ldots \subset p_r$ of prime ideals can be refined into a chain of n + 1 prime ideals ($\neq$A).

Now since dim A = ht(m) we get dim A = n

But from (*) and Lemma 6, we have $\text{rank}_p(m/m^2) = n$, where $p = A/m$.

$$\therefore \dim A = \text{rank}_p(m/m^2)$$

Henu, A is a regular local ring

Now we are ready to prove a necessary and sufficient condition for a noetherian local ring to be regular. To do that we need the following well known results form dimension theory.

1. Let k be a field , and $k(x_o, x_1, \ldots, x_r)$ a homogeneous polynomial of degree s. Let $R = k[x_o, x_1, \ldots, x_r]/(k(x_o, x_1, \ldots, x_r))$.

   Then, for $n \geq s$, $l(a_n) = \begin{pmatrix} n+r \\ r \end{pmatrix} - \begin{pmatrix} n-s+r \\ r \end{pmatrix}$, which is a polynomial of degree r-1 in n.

2. Let (A, m, k) be a noetherian local ring, and set $G = Gr_m(A)$.

   Then dim A = dim G.

3. If $l(M_n)$ is a polynomial of degree n-1, then the samuel function $X_M(n) = l(M|I^{n+1}M)$ is a polynomial of degree d.

Theorem 1:- Let (A, m, k) be a noetherian local ring.

Then , A is regular iff the graded ring $Gr_m(A) = \oplus_{n\geq o} m^n/m^{n+1}$ associated to be m-adic filtration is isomorphic to a polynomial ring $k[X_1, X_2, \ldots X_n]$.

Proof:- (⇒) **Suppose A is regular.**

Let $\{x_1, x_2, \ldots x_d\}$ be a regular system of parameters.

$$\Rightarrow m = (x_1, x_2, \ldots x_d)$$

Let $\bar{x}_i$ be the image of x_i in m/m^2

Then , $Gr_m(A) = A/m \oplus m/m^2 \oplus \ldots = k\,[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_d]$.

Now, define $\Psi : k[X_1, X_2, \ldots, X_d] \longrightarrow Gr_m(A)$ by $\Psi(X_i) = \bar{x}_i$.

clearly , Ψ is a surjective homomorphism.

Then $0 \longrightarrow \ker \Psi \longrightarrow k[X_1, \ldots, X_d] \longrightarrow Gr_m(A) \longrightarrow 0$ is exact.

$$\Rightarrow Gr_m(A) = k[X_1, X_2, \ldots, X_d] \,/\, \ker \Psi$$

Claim:- $\ker \Psi = 0$

Suppose not , i.e. $\ker \Psi \neq 0$.

Then it contains a homogeneous polynomial $f(x_1, x_2, \ldots, x_d) \neq 0$ of degree r.

$$\Rightarrow (f(x)) \subseteq I$$

Now consider $k[X_1, X_2, \ldots, X_d]/\ker \Psi$ and $k[X_1, X_2, \ldots, X_d]/(f(x))$. clearly the length of any homogeneous piece of $k[X]/\ker \Psi$ is less than or equal to the length of the corresponding homogeneous piece of $k[X]/(f(x))$. But from (1) above, for $n > r$ the length of a homogeneous piece of $k[X]/(f(x))$ is equal to $\binom{n+d-1}{d-1} - \binom{n-r+d-1}{d-1}$, which is a polynomial of degree d-2 in n.

$\Rightarrow$ For $n > r$, the length of a homogeneous piece of $k[x]/\ker \Psi$ has degree atmost d-2.

$\therefore$ By (3) , the samuel function $l(A/m^{n+1})$ (= the samuel function of $k[X_1, \ldots, X_d]/\ker\Psi$) of A has degree atmost d-1.

This is a contradiction to the fundamental theorem of dimension theory (ie, the degree of the samuel function = dim A).

$$\therefore \ker \Psi = (0)$$

$$\text{Hence, } Gr_m(A) \cong k[X_1, X_2, \ldots, X_d]$$

($\Leftarrow$) <u>Suppose $Gr_m(A) \cong k[X_1, X_2, \ldots, X_d]$.</u>

<u>WTS</u>:- A is regular.

It suffices to show that $\dim A = \operatorname{rank}_k(m/m^2)$

Now, $\dim A = \dim (Gr_m(A))$ . . . by (2) above

$= \dim (k[X_1, X_2, \ldots, X_d])$

$= \dim k + d$

$= d$ . . . . since $\dim k = 0$

- since $Gr_{m}(A) \cong k[X_1, X_2, \ldots, X_d]$, by comparing the homogeneous component of degree 1, we get $m/m^2 \equiv kX_1 + KX_2 + \ldots + KX_d$

$$\Rightarrow \text{rank}_k(m/m^2) = \text{rank}_k\ (kX_1 + KX_2 + \ldots + KX_d)$$

$$= d$$

$$\therefore \dim A = \text{rank}_k(m/m^2).$$

Hence, A is regular.

Now let us see two properties of a regular local ring, the first one tells us that a regular local ring is an integral domain (which is ofcourse a corollary of theorem 1) and the second one says a regular local ring of dimension 0 is nothing but a field. To do this we need the following two lemmas.

Lemma 7:- Let A = a noetherian ring, and I = rad(A)

Then $\overset{\infty}{\bigcap} I^n = (0)$.

Lemma 8:- Let A = a ring, I an ideal of A such that $\overset{\infty}{\bigcap} I^n = (0)$. Suppose $Gr_I(A)$ is an integral domain, then A is an ID.

Proof:- Here we use the following fact: "$\alpha \in m^h, \alpha \notin m^{h+1}, \beta \in m^k, \beta \notin m^{k+1}$, where h and k are non-negative integers, then $\alpha\beta \notin m^{h+k+1}$".

Let x, y be non-zero elements of A.

WTS:- $xy \neq 0$.

- Since $\overset{\infty}{\bigcap} I^n = (0)$, there exist integers $r, s \geq 0$ such that $x \in I^r$, $x \notin I^{r+1}$, $y \in I^s, y \notin I^{s+1}$. Let $\bar{x}$ and $\bar{y}$ denote the images of x and y in I^r/I^{r+1} and I^s/I^{s+1} resp.
- Since $x \notin I^{r+1}$ and $y \notin I^{s+1}$, $\bar{x}$ and $\bar{y}$ are non-zero elements of I^r/I^{r+1} and I^s/I^{s+1} resp.

$\Rightarrow \quad \bar{x}.\bar{y} \neq 0$ ... since $Gr_m(A)$ is an ID.

$\Rightarrow \quad \overline{xy} \neq 0$

$\Rightarrow \quad xy \neq 0$

Hence, A is an integral domain.

Corollary 1:- A regular local ring A is an integral domain. If dim A = 1, then A is a principal ideal domain.

Proof:- Let (A, m, k) be a regular local ring of dimension d.

Then, by theorem 1, $Gr_m(A) \cong k[X_1, X_2, \ldots, X_d]$.

- Since K is an integral domain, $k[X_1, \ldots, X_d]$ is an integral domain.

$\Rightarrow \quad Gr_m(A)$ is an ID.

But, $m = rad(A) \quad \Rightarrow \bigcap_{}^{\infty} m^n = (0)$ by Lemma 7.

Hence, by Lemma 8, A is an integral domain.

To prove the second assertion:

- Since A is regular and of dimension 1, a minimal generator of m must contain only a single element, then m is principal.

Let $m = (a)$

Let I = an ideal of A , $I \neq (0)$.

WTS:- I is some power of m.

- Since $I \neq (0), \exists\, n \geq 0$ such that $I \subseteq m^n$ but $I \not\subseteq m^{n+1}$ (because $\bigcap^{\infty} m^n = (0)$).

Then, we can find $x \in I$ but $x \notin m^{n+1} = (a^{n+1})$.

$x \in I \Rightarrow x \in m^n = (a^n)$

$\Rightarrow x = a^n u$ for some $u \notin m$ (if $u \in m = (a)$, we get $x \in m^{n+1} \Rightarrow\Leftarrow$)

$\therefore$ U is a unit

$\Rightarrow$ x and a^n are associates.

$\therefore (a^n) = (x) \subseteq I \subseteq (a^n)$

$\therefore I = (a^n) = m^n$

Hence, I is principal

- Since I is arbitrary, **A is a PID.**

Theorem 2:- A regular local ring of dimension zero is a field.

Proof:- Let (A, m, k) be a regular local ring, $\dim A = 0$

$$\Rightarrow \quad \mathrm{rank}_k(m/m^2) = 0$$

$$\Rightarrow \quad m = m^2$$

$$\Rightarrow \quad m = m^s \quad \forall s \geq 2.$$

But, $\bigcap^{\infty} m^n = (0)$ and $m = \bigcap^{\infty} m^n$ (Lemma 7)

$$\Rightarrow \quad m = (0)$$

$\therefore K = A/m = A$ (or A has no proper ideal other than (0))

Hence, A is a field

So far we have seen the definition of a regular local ring, and that a regular local ring is an integral domain, and a necessary and sufficient condition for a noetherian local ring (A, m, k) to be regular is that $Gr_m(A)$ is a polynomial ring over k. Next we see another necessary and sufficient condition. To do that we need results from homological algebra.

3. Homological Concepts

Definition 5:- A complex (or a chain complex) $\mathbb{X}$ is a sequence of modules and maps $\mathbb{X}: \ldots \longrightarrow \mathbb{X}_{n+1} \xrightarrow{d_{n+1}} \mathbb{X}_n \xrightarrow{d_n} \mathbb{X}_{n-1} \longrightarrow \ldots,\ n \in \mathbb{Z}$ with $d_n d_{n+1} = 0 \ \forall n$.

- The maps d_n are called differentiation

Note:- (1) $d_n d_{n+1} = 0 \ \forall n$ implies $\mathrm{Im}\, d_{n+1} \subseteq \ker d_n \ \forall n$.

(2) If it is necessary to display the differentials , we will write $(\mathbb{X}, d)$ instead of $\mathbb{X}$.

Examples 1: 1. Every exact sequence is a complex. In particular every short exact sequence is a complex, since if $0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$ is a short exact sequence, then $\ldots\ 0 \longrightarrow 0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0 \longrightarrow 0 \longrightarrow \ldots$ is also a complex.

2. If $\mathbb{X}$ is a complex and F is a covariant functor, then $F(\mathbb{X})$: $\ldots \longrightarrow F(\mathbb{X}_{n+1}) \longrightarrow F(\mathbb{X}_n) \longrightarrow F(\mathbb{X}_{n-1}) \longrightarrow \ldots$ is also a complex.

In particular if $\mathbb{X}$ is an exact sequence, then $F(\mathbb{X})$ is a complex (which is usually not exact)

Definition 6: If $\mathbb{X}$ and $\mathbb{X}'$ are complexes, a <u>chain map</u> $f: \mathbb{X} \longrightarrow \mathbb{X}'$ is a sequence of maps $f_n: \mathbb{X}_n \longrightarrow \mathbb{X}'_n$ for all $n \in \mathbb{Z}$, such that the following diagram commutes:

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & \mathbb{X}_{n+1} & \xrightarrow{d_{n+1}} & \mathbb{X}_n & \xrightarrow{d_n} & \mathbb{X}_{n-1} & \longrightarrow & \ldots \\
 & & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} & & \\
\ldots & \longrightarrow & \mathbb{X}_{n+1} & \xrightarrow{d'_{n+1}} & \mathbb{X}'_n & \xrightarrow{d'_n} & \mathbb{X}'_{n-1} & \longrightarrow & \ldots
\end{array}$$

Proposition 1: Let comp = the class of all complexes and chain maps. Then, comp is a pre-additive category. (i.e. the Hom's are abelian groups and distributivity law holds).

Definition 7: If $(\mathbb{X}, d)$ is a complex, <u>it's n^{th} homology module</u>, is defined by:

$$H_n(\mathbb{X}) = \ker d_n / \mathrm{Im}\ d_{n+1}.$$

Note: Since $Im\ d_{n+1} \subseteq \ker d_n$, the quotient module does make sense.

The elements of $\ker d_n$ are called <u>n-cycles</u> and the elements of $Im\ d_{n+1}$ are called <u>n-boundaries</u>.

Notation:- $\ker d_n = z_n(\mathbb{X}) = z_n$, $Im\ d_{n+1} = B_n(\mathbb{X}) = B_n$

$$\therefore\ H_n(\mathbb{X}) = Z_n(\mathbb{X})/B_n(\mathbb{X}).$$

We claim H_n is a functor, so it remains to define the action of H_n on morphisms (= chain maps).

Definition 8:- If $f: \mathbb{X} \to \mathbb{X}'$ is a chain map, define

$$H_n(f) : H_n(\mathbb{X}) \longrightarrow H_n(\mathbb{X}') \text{ by: } z_n + B_n(\mathbb{X}) \longrightarrow f_n(z_n) + B_n(\mathbb{X}')$$

- $H_n(f)$ is called the induced map by f, and is denoted by f_*.

Proposition 2: For each n, H_n : comp $\longrightarrow$ M (category of A-modules) is an additive functor (i.e. $H_n(f+g) = H_n(f) + H_n(g)$ for every pair of morphisms lying in the same group).

Definition 9: A complex $(\mathbb{X},d)$ is a subcomplex of $(\mathbb{X}',d')$ if each $\mathbb{X}_n$ is a submodule of $\mathbb{X}'_n$ and $d_n = d'_n/_{\mathbb{X}_n}$ for all n.

Note:- 1. There is also a quotient module

$$\mathbb{X}'/\mathbb{X}: \ldots \longrightarrow \mathbb{X}'_{n+1}/\mathbb{X}_{n+1} \xrightarrow{\bar{d}_{n+1}} \mathbb{X}'_n/\mathbb{X}_n \longrightarrow \ldots$$

where $\bar{d}_{n+1} : a'_{n+1} + \mathbb{X}_{n+1} \longrightarrow d'_{n+1}(a'_{n+1}) + \mathbb{X}_n$.

2. $\mathbb{X}$ is a subcomplex of $\mathbb{X}'$ when the inclusion map $i_n : \mathbb{X}_n \to \mathbb{X}'_n$ constitute a chain map.

i.e.
$$\begin{array}{ccccccc} \ldots \longrightarrow & \mathbb{X}_{n+1} & \xrightarrow{d_{n+1}} & \mathbb{X}_n & \xrightarrow{d_n} & \mathbb{X}_{n-1} & \longrightarrow \ldots \\ & \downarrow i_{n+1} & & \downarrow i_n & & \downarrow i_{n-1} & \\ \ldots \longrightarrow & \mathbb{X}'_{n+1} & \xrightarrow{d'_{n+1}} & \mathbb{X}'_n & \xrightarrow{d'_n} & \mathbb{X}'_{n-1} & \longrightarrow \ldots \end{array}$$

Suppose the inclusion map constitute a chain map.

WTS:- $\mathbb{X}$ is a subcomplex of $\mathbb{X}'$.

- clearly $\mathbb{X}_n$ is a submodule of $\mathbb{X}_n$.

And, since for each $x_n \in \mathbb{X}_n$, we have $i_{n-1}d_n(x_n) = d'_n\, i_n\,(x_n)$

$$\Rightarrow \quad d_n(x_n) = d_n'(x_n)$$

$$\Rightarrow \quad d_n = d_n'|_{\mathbb{X}_n}.$$

Hence, $\mathbb{X}$ is a subcomplex of $\mathbb{X}_n'$.

<u>**Proposition 3**</u>: If $f:\mathbb{X}\to\mathbb{X}'$ is a chain map, define complexes kerf, Imf, and coker f as follows:

$$\ker f : \ldots \longrightarrow \ker f_n \xrightarrow{p_n} \ker f_{n-1} \longrightarrow \ldots \quad \text{where } p_n = d_n|_{\ker f_n}.$$

$$Im\, f: \ldots \longrightarrow Im\, f_n \xrightarrow{q_n} Im\, f_{n-1} \longrightarrow \ldots. \quad \text{where } q_n = d_n'|_{Im\, f_n}$$

Then $\mathbb{X}/\ker f \cong \mathrm{Im} f$.

<u>**Proof:-**</u> Consider the commutative diagram:

$$\begin{array}{ccccccc} \mathbb{X} : \ldots & \to & \mathbb{X}_n & \xrightarrow{d_n} & \mathbb{X}_{n-1} & \longrightarrow & \ldots \\ & & \downarrow f_n & & \downarrow f_{n-1} & & \\ \mathbb{X}' : \ldots & \to & \mathbb{X}_n' & \xrightarrow{d_n'} & \mathbb{X}_{n-1}' & \longrightarrow & \ldots \end{array}$$

- Clearly ker f is a subcomplex of $\mathbb{X}$, by the note above.

And, $\mathbb{X}|\ker f = \ldots \longrightarrow \mathbb{X}_n/\ker f_n \longrightarrow \mathbb{X}_{n-1}/\ker f_{n-1} \longrightarrow \ldots$

$\cong \ldots \longrightarrow \mathrm{Im} f_n \longrightarrow \mathrm{Im} f_{n-1} \longrightarrow \ldots$ (since $\mathbb{X}_n/\ker f_n \cong \mathrm{Im} f_n$)

$\cong \mathrm{Im} f$.

Hence, $\mathbb{X}/\ker f \cong \mathrm{Im} f$

<u>**Proposition 4**</u>: Define $\mathbb{X}' \xrightarrow{f} \mathbb{X} \xrightarrow{g} \mathbb{X}''$ to be exact if $\mathrm{Im} f = \ker g$ .. (*)
Then (*) is exact if and only if the sequence of modules are exact for all $n \in \mathbb{Z}$.

<u>**Proof:**</u> Consider the following diagram:

$$\begin{array}{ccccccccc} \mathbb{X}' : \ldots & \to & \mathbb{X}_{n+1}' & \longrightarrow & \mathbb{X}_n' & \longrightarrow & \mathbb{X}_{n-1}' & \longrightarrow & \ldots \\ f\downarrow & & \downarrow f_{n+1} & & \downarrow f_n & & & & \\ \mathbb{X} : \ldots & \longrightarrow & \mathbb{X}_{n+1} & \longrightarrow & \mathbb{X}_n & \longrightarrow & \mathbb{X}_{n-1} & \longrightarrow & \ldots \\ g\downarrow & & \downarrow g_{n+1} & & \downarrow g_n & & & & \\ \mathbb{X}'' : \ldots & \longrightarrow & \mathbb{X}_{n+1}'' & \longrightarrow & \mathbb{X}_n'' & \longrightarrow & \mathbb{X}_{n-1}'' & \longrightarrow & \ldots \end{array}$$

Thus, (*) is exact iff imf = ker g

iff $\ldots \to \text{imf}_n \to \text{imf}_{n-1} \to \ldots$ and $\ldots \to \text{kerg}_n \to \text{kerg}_{n-1} \to \ldots$ are equal.

iff im f_n = ker g_n for all n.

iff $\mathbb{X}'_n \xrightarrow{f_n} \mathbb{X}n \xrightarrow{g_n} \mathbb{X}''_n$ is exact $\forall n \in \mathbb{Z}$.

From proposition 4 we have if $\mathbb{X}' \longrightarrow \mathbb{X} \to \mathbb{X}''$ is an exact sequence of complexes. Then for each n, $\mathbb{X}'_n \to \mathbb{X}_n \to \mathbb{X}''_n$ is an exact sequence of modules. The next natural question is: what do homology functors do to short exact sequences of complexes ? They are, ingeneral, neither left nor right exact. (we shall see that if $0 \to \mathbb{X}' \to \mathbb{X} \to \mathbb{X}'' \to 0$ is exact, then $H_n(\mathbb{X}') \to H_n(\mathbb{X}') \to H_n(\mathbb{X}'')$ is exact) To do this we need the followng results:

Proposition 5: If A is a ring and $f: M \to N$ is an A-module homomorphism and k is a submodule of kerf, then there is a unique A-module homomorphism $\bar{f}: M/K \to N$ such that $\bar{f}(m+k) = f(m)$ for all $m \in M$, $\text{Im}\bar{f} = \text{Im}f$ and $\ker\bar{f} = \ker f/k$. $\bar{f}$ is an A-module isomorphism iff f is an A-module epimorphism and k = kerf. In particular $M/\ker f \cong \text{I}mf$.

Lemma 9:- (Connecting homomorphism)

Let $0 \to \mathbb{X}' \xrightarrow{i} \mathbb{X} \xrightarrow{p} \mathbb{X}' \to 0$ be an exact sequence of complexes. Then, for each n, there is a homomorphism $\partial n: H_n(\mathbb{X}'') \to H_{n-1}(\mathbb{X}')$ defined by: $z''+B_n(\mathbb{X}'') \longrightarrow i^{-1}_{n-1} d_n p^{-1}_n(z'') + B_{n-1}(\mathbb{X}')$.

Proof:- We have:

$$
\begin{array}{ccccccccc}
0 & & & & 0 & & 0 & & \\
\downarrow & & & & \downarrow & & \downarrow & & \\
\mathbb{X}': \ldots \to & \mathbb{X}'_{n+1} & \to & & \mathbb{X}'_n & \xrightarrow{d'_n} & \mathbb{X}'_{n-1} & \to & \ldots \\
\downarrow & & & & \downarrow i_n & & \downarrow i_{n-1} & & \\
\mathbb{X}: \ldots \to & \mathbb{X}_{n+1} & \to & & \mathbb{X}_n & \xrightarrow{d_n} & \mathbb{X}_{n-1} & \to & \ldots \\
\downarrow & & & & \downarrow p_n & & \downarrow p_{n-1} & & \\
\mathbb{X}'': \ldots \to & \mathbb{X}''_{n+1} & \to & & \mathbb{X}''_n & \xrightarrow{d''_n} & \mathbb{X}''_{n-1} & \to & \ldots \\
\downarrow & & & & \downarrow & & \downarrow & & \\
0 & & & & 0 & & 0 & &
\end{array}
$$

Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{X}'_n & \xrightarrow{i_n} & \mathbb{X}_n & \xrightarrow{p_n} & \mathbb{X}''_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'_n} & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d''_n} & & \\ 0 & \longrightarrow & \mathbb{X}'_{n-1} & \xrightarrow{i_{n-1}} & \mathbb{X}_{n-1} & \xrightarrow{p_{n-1}} & \mathbb{X}''_{n-1} & \longrightarrow & 0 \end{array}$$

To show well-definedness

Suppose $z'' \in \mathbb{X}''$ and $d''_n(z'') = 0$ (ie, $z'' \in \ker d''_n$)
- since p_n is onto, $\exists a_n \in \mathbb{X}_n$ such that $p_n(a_n) = z''$

Now, consider $p_n(a_n)$.

By commutativity, we have $p_{n-1} d_n(a_n) = d''_n\, p_n(a_n) = d''_n(z'') = 0.$

$$\Rightarrow \quad d_n(a_n) \in \ker p_{n-1}$$

$$\Rightarrow \quad d_n(a_n) \in Im\, i_{n-1} \ \ldots \text{ since } \ker p_{n-1} = Im\, i_{n-1}.$$

$\therefore\ i_{n-1}^{-1}(d_n(a_n))$ makes sense.

Now, since i_{n-1} is 1-1, there is a unique $a'_{n-1} \in \mathbb{X}'_{n-1}$ such that $i_{n-1}(a'_{n-1}) = d_n(a_n)$.

Suppose we had lifted z'' to $\bar{a}_n \in \mathbb{X}_n$. Then by the same argument as above, $\exists!\ \bar{a}'_{n-1} \in \mathbb{X}'_{n-1}$ with $i_{n-1}(\bar{a}'_{n-1}) = d_n(\bar{a}_n)$.

clearly $a_n - \bar{a}_n \in \ker p_n$. (since $p_n(a_n - \bar{a}_n) = p_n(a_n) - p_n(\bar{a}_n) = z'' - z'' = 0$)

$$\Rightarrow \quad a_n - \bar{a}_n \in \mathrm{Im}\, i_n$$

$$\therefore\ \exists\ x'_n \in \mathbb{X}'_n \text{ -- } i_n(x'_n) = a_n - \bar{a}_n.$$

But $i_{n-1}(a'_{n-1}) = d_n a_n$ and $i_{n-1}(\bar{a}'_{n-1}) = d_n \bar{a}_n$.

$$\Rightarrow \quad i_{n-1}(a'_{n-1} - \bar{a}'_{n-1}) = d_n(a_n - \bar{a}_n) = d_n(i_n(x'_n)) = d_n i_n(x'_n)$$

$$\Rightarrow \quad i_{n-1}(a'_{n-1} - \bar{a}'_{n-1}) = d_n i_n(x'_n) = i_{n-1}(d'_n(x_n))$$

$$\Rightarrow \quad a'_{n-1} - \bar{a}'_{n-1} = d'_n(x_n) \ \ldots \text{ since } i_{n-1} \text{ is injective}$$

$$\therefore\ a'_{n-1} - \bar{a}'_{n-1} \in \mathrm{im}\, d'_n = B_{n-1}(\mathbb{X}') \subseteq \ker d'_{n-1}.$$

Hence, the map is well-defined and from $\ker d''_n \longrightarrow \mathbb{X}'_{n-1}/Im\, d'_n$. Clearly it is a homomorphism.

But, this map sends Imd''_{n+1} into 0 and $i^{-1}_{n-1}d_n p^{-1}_n(z'') = a'_{n-1}$ is a cycle, i.e. it is in ker d'_{n-1}.

$\therefore$ Im d''_{n+1} is contained in the kernel of the map.

Hence, by the above proposition, the given map induces a homomorphism from ker $d''_n/Im\ d''_{n+1}$ into ker $d'_{n-1}/Im\ d'_n$.

Therefore, $\exists\ \partial n : H_n(\mathbb{X}'') \longrightarrow H_{n-1}(\mathbb{X}')$

Definition 10: The maps $\partial n : H_n(\mathbb{X}'') \longrightarrow H_{n-1}(\mathbb{X}')$ are called connecting homomorphisms.

Now, we prove the long exact sequence theorem.

Theorem 3:- (Long exact sequence)

If $0 \longrightarrow \mathbb{X}' \xrightarrow{i} \mathbb{X} \xrightarrow{p} \mathbb{X}'' \longrightarrow 0$ is an exact sequence of complexes, then there is an exact sequence of modules

$$\cdots \longrightarrow H_n(\mathbb{X}') \xrightarrow{i_*} H_n(\mathbb{X}) \xrightarrow{p_*} H_n(\mathbb{X}'') \xrightarrow{\partial} H_{n-1}(\mathbb{X}') \xrightarrow{i_*} H_{n-1}(\mathbb{X}) \longrightarrow \cdots$$

Proof: consider the following diagram:

$$\begin{array}{ccccccc}
\cdots \longrightarrow & H_{n+1}(\mathbb{X}') & \longrightarrow & H_n(\mathbb{X}') & \longrightarrow & H_{n-1}(\mathbb{X}') & \longrightarrow \cdots \\
& H_{n+1}(i)\downarrow & & H_n(i)\downarrow = i_* & & H_{n-1}(i)\downarrow & \\
\cdots \longrightarrow & H_{n+1}(\mathbb{X}) & \longrightarrow & H_n(\mathbb{X}) & \longrightarrow & H_{n-1}(\mathbb{X}) & \longrightarrow \cdots \\
& H_{n+1}(p)\downarrow & & H_n(p)\downarrow = p_* & & H_{n-1}(p)\downarrow & \\
\cdots \longrightarrow & H_{n+1}(\mathbb{X}'') & \longrightarrow & H_n(\mathbb{X}'') & \longrightarrow & H_{n-1}(\mathbb{X}'') & \longrightarrow \cdots
\end{array}$$

Where $H_n(\mathbb{X})$ = ker d_n / Im d_{n+1} , $H_{n-1}(\mathbb{X})$ = ker $d_{n-1}/Im\ d_n$ and so on. Here we have six inclusions to verify.

1. im $i_* \subseteq$ ker p_*
2. ker $p_* \subseteq$ im i_*
3. im $p_* \subset$ ker ∂
4. ker $\partial \subset$ im p_*
5. im $\partial \subset$ ker i_*
6. ker $i_* \subseteq$ im ∂.

- Since the notation is self explanatory we omit the subscripts. We will prove her only (1) for the rest we can use a similar argument.

1. $Im\, i_* \subseteq \ker p_*$

Let $y \in Im\, i_* \Rightarrow \exists\, x \in H_n(\mathbb{X}')$ such that $i_*(x) = y$

But, $x \in H_n(\mathbb{X}')$ implies $x \in \ker d'_n / Im\, d'_{n+1}$

$\Rightarrow\ x = ar\ Imd_{n+1}$ for some $a \in \ker d'_n$.

Thus, $p_*(y) = p_*(i_*(x))$

$= p_*(i_*(a + Im\, d'_{n+1}))$

$= p_*(i(a) + Im\, d_{n+1}))$ ... since $i_*(a + Imd'_{n+1}) = i(a) + Im\, d'_{n+1}$

$= p(i(a)) + Im\, d''_{n+1}$

$= (poi)(a) + Im\, d''_{n+1}$

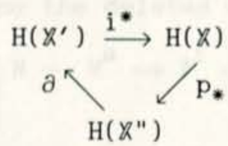
$= 0 + Im\, d''_{n+1}$

$= Im\, d''_{n+1}$

$\Rightarrow\ y \in \ker p_*$

Hence, $im\, i_* \subseteq \ker p_*$

Theorem 3 is often called the exact triangle because of the following diagram:



Definition 11:- Let A be a ring.

Let M be an A-module.

(a) **A free resolution** of a module M is an exact sequence

$$\cdots \longrightarrow F_n \xrightarrow{d_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_o \xrightarrow{\epsilon} M \longrightarrow o$$

in which each F_n is a free module.

(b) **An injective resolution** of M is an exact sequence

$$0 \longrightarrow M \longrightarrow E^o \longrightarrow E^1 \longrightarrow \cdots \longrightarrow E^n \longrightarrow E^{n+1} \longrightarrow \cdots$$

in which each E_n is injective.

(c) A <u>**projective resolution**</u> of M is an exact sequence

$$\ldots \rightarrow p_n \xrightarrow{d_n} p_{n-1} \longrightarrow \ldots \rightarrow p_2 \xrightarrow{d_2} p_1 \xrightarrow{d_1} p_o \xrightarrow{\epsilon} M \longrightarrow o$$

in which each p_n is projective.

Proposition 6:
1. Every module has an injective resolution.
2. Every module has a free resolution.

Note: Since free modules are projective, free resolutions are a special kind of projective resolutions. Hence, every module has a projective resolution.

Definition 12: A complex $(\mathbb{X},d)$ is called a left (right) complex if $x_n = 0\ \forall n < 0\ (\forall n > 0)$.

Let $\mathbb{X}$ be a complex of the form

$$\mathbb{X} : \ldots \longrightarrow \mathbb{X}_1 \rightarrow \mathbb{X}_o \rightarrow M \rightarrow o$$

The complex obtained by suppressing M is:

$\mathbb{X}_M$: $\ldots \rightarrow \mathbb{X}_1 \rightarrow \mathbb{X}_o \rightarrow o$ and is called the <u>deleted complex of $\mathbb{X}$</u>.

- Similary, we define the deleted complex $\mathbb{Y}_N$ of the complex

$\mathbb{Y}_N : 0 \rightarrow N \rightarrow \mathbb{Y}^0 \rightarrow \mathbb{Y}^1 \rightarrow \ldots$ by suppressing N.

Deleted complexes arise in practice from either a projective resolution or an injective resolutions of a module. If we suppress M from the projective resolution $\ldots \rightarrow p_1 \rightarrow p_0 \rightarrow M \rightarrow 0$, we really have not lost any information , for $M = \text{coker}\ (p_1 \rightarrow p_0)$.

Ext

Let A = a commutative ring with unity.

Let M, N = A-modules.

Consider the projective resolution of M and it's deleted complex,

$$\mathbb{P} : \ldots \rightarrow p_r \xrightarrow{d_r} P_{r-1} \rightarrow \ldots \rightarrow P_1 \xrightarrow{d_1} p_o \xrightarrow{\epsilon} M \rightarrow 0$$

$$\mathbb{P}_M : \ldots \rightarrow p_r \xrightarrow{d_r} P_{r-1} \rightarrow \ldots \rightarrow P_1 \xrightarrow{d_1} p_o \rightarrow 0 \qquad (*)$$

Then , apply the contravariant functor $Hom_A(-,N)$ to lP_M. we obtain the complex

$$Hom_A(lP_M,N): 0 \rightarrow Hom_A(p_o,N) \xrightarrow{d_1^*} Hom_A(p_1,N) \xrightarrow{d_2^*} \dots \rightarrow Hom_A(p_{r-1},N) \xrightarrow{d_r^*} Hom_A(p_r,N) \rightarrow \dots$$

Definition 12: $Ext_A^n(M,N) = H_n(Hom_A(lP_M,N))$

$$= H_n(lP_M,N)$$

$$= \ker d_n^* / Im d_{n-1}^*$$

Alternatively

Consider an injective resolution of N and it's deleted complex:

$$lE : 0 \rightarrow N \xrightarrow{\epsilon} E^0 \xrightarrow{d_o} E^1 \xrightarrow{d_1} \dots \rightarrow E_o^r \xrightarrow{d_r} E^{r+1} \rightarrow \dots \qquad (**)$$

$$lE_N: 0 \rightarrow E^0 \xrightarrow{d_o} E^1 \xrightarrow{d_1} \dots \rightarrow E^r \xrightarrow{d_r} E^{r+1} \rightarrow \dots$$

Now, apply the covariant functor $Hom_A(M,-)$ to lE_N , to get

$$Hom_N(M,lE_N): 0 \rightarrow Hom_A(M,E^0) \xrightarrow{d_{o*}} Hom_A(M,E^r) \xrightarrow{d_{1*}} \dots \rightarrow Hom_A(M,E^r) \xrightarrow{d_{r*}} Hom_A(M,E^{r+1}) \rightarrow \dots$$

Definition:- $Ext_A^n(M,N) = H_n(Hom_A(M,lE_N))$

$$= \ker d_{n*} / Im\, d_{n-1*}$$

Tor

Consider lP_M , which is in (*)

Apply the covariant functor — ⊗N to lP_M.

Then, $lP_M \otimes N: \dots \rightarrow p_r \otimes N \xrightarrow{d_r \otimes 1} p_{r-1} \otimes N \rightarrow \dots \rightarrow p_1 \otimes B \xrightarrow{d_1 \otimes 1} p_o \otimes B \rightarrow 0$

Definition 13:- $Tor_n^A(M,N) = H_n(lP_M \otimes N)$

$$= \ker (d_n \otimes 1) \, | I_m(d_{n+1} \otimes 1).$$

Alternativey

consider lP_N

Apply the covariant functor M⊗ — to lP_N to get:

$$M \otimes lP_N: \dots \rightarrow M \otimes p_r \xrightarrow{1 \otimes d_r} M \otimes p_{r-1} \rightarrow \dots \rightarrow M \otimes p_1 \xrightarrow{1 \otimes d_1} M \otimes p_o \rightarrow 0$$

Definition : $Tor_n^A(M,N) = H_n(M \otimes 1P_N) = \ker(1 \otimes d_n)/Im(1 \otimes d_{n+1})$

Now, let us see some of the elementary properties of Ext and Tor.

Lemma 12:- Let $\ldots \rightarrow p_2 \xrightarrow{d_2} p_1 \xrightarrow{d_1} p_o \xrightarrow{\epsilon} M \rightarrow 0$ be a projective resolution of M and $k_o = \ker \epsilon$, and $k_n = \ker d_n \quad \forall n \geq 1$

Then , $Tor_{n+1}(M,N) \cong Tor_n(k_o,N) \cong Tor_{n-1}(k_1,N) \cong \ldots \cong Tor_1(k_{n-1},N)$.

Proof:- Clearly $\ldots \rightarrow p_2 \xrightarrow{d_2} p_r \xrightarrow{d_1} k_o \rightarrow 0$ is a projective resolution of k_o. (since $k_o = Im\, d_1 = \ker \epsilon$). Since the indices are no longer correct define

$$Q_{n-1} = p_n \text{ and } \Delta_{n-1} = d_n \quad \forall n \geq 1.$$

so, we get $\ldots \rightarrow Q_2 \xrightarrow{\Delta_2} Q_1 \xrightarrow{\Delta_1} Q_o \longrightarrow K_o \longrightarrow 0$

$$\begin{aligned} \text{Thus, } Tor_n(k_o,N) &= H_n(k_o \otimes N) \\ &= \ker(\Delta_n \otimes 1)/Im(\Delta_{n+1} \otimes 1) \\ &= \ker(d_{n+1} \otimes 1)/Im(d_{n+2} \otimes 1) \\ &= H_{n+1}(M \otimes N) \\ &= Tor_{n+1}(M,N) \end{aligned}$$

Hence, $\mathbf{Tor_{n+1}(M,N) \cong Tor_n(k_o,N)}$

Again, we have the projective resolution $\ldots \rightarrow p_3 \xrightarrow{d_3} p_2 \xrightarrow{d_2} k_1 \rightarrow 0$ of k_1.

To correct the indices, define $Q_{n-2} = p_n$ and $\Delta_{n-2} = d_n \quad \forall n \geq 2$.

$$\begin{aligned} \text{Thus , } Tor_{n-1}^A(k_1,N) &= H_{n-1}(k_1 \otimes N) \\ &= \ker(\Delta_{n-1} \otimes 1)/Im(\Delta_n \otimes 1) \\ &= \ker(d_{n+1} \otimes 1)/Im(d_{n+2} \otimes 1) \\ &= H_{n+1}(M \otimes N) \\ &= Tor_{n+1}(M,N) \end{aligned}$$

Hence, $\mathbf{Tor_{n+1}(M,N) \cong Tor_n(k_o,N) \cong Tor_{n-1}(k_1,N)}$.

And, the remaining isomorphisms are obtained by iteration.

Therefore, $Tor_{n+1}(M,N) \cong Tor_n(k_o,N) \cong \ldots \cong Tor_1(k_{n-1},N)$

Lemma 13: Let $0 \to M \xrightarrow{\epsilon} E_o \xrightarrow{d_o} E_1 \xrightarrow{d_1} E_2 \xrightarrow{d_2} \ldots$ be an injective resolution of M, and define $L^o = Im\,\epsilon$, $L^n = Im\, d_{n-1}$ $\forall n \geq 1$. Then:

$$Ext_A^{n+1}(N,M) \cong Ext^n(N,L^o) \cong \ldots \cong Ext^1(N,L^{n-1}).$$

Proof: clearly $0 \to L^o \to E_1 \to E_2 \to \ldots$ is an injective resolution of L^o

put $Q_{n-1} = E_n$ and $\Delta_{n-1} = d_n$ $\forall n \geq 1$.

Then, $0 \to L^o \to Q_o \xrightarrow{\Delta_o} Q_1 \xrightarrow{\Delta_1} \ldots$

Thus, $Ext_A^n(N,L^o) = H_n\ (Hom_A(N,L^o))$

$= ker\ \Delta_{n*} \,|\, Im\ \Delta_{n-1*}$

$= ker\ d_{n+1*} \,|\, Im\ d_{n*}$

$= H_{n+1}(Hom_A(N,M))$

$= Ext_A^{n+1}(N,M)$

Hence, $Ext_A^{n+1}(N,M) \cong Ext_A^n(N,L^o)$.

The rest can be shown by iteration, so we have:

$$Ext_A^{n+1}(N,M) \cong Ext_A^n(N,L^o) \cong \ldots \cong Ext_A^1(N,,L^{n-1})$$

Lemma 14: Let $\ldots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_o \xrightarrow{\epsilon} N \to 0$ be a projective resoution and $k_o = ker\epsilon$, $k_n = kerd_n$ $\forall n \geq 1$. Then, if we apply the covaraiant functor, then we have $Ext_A^{n+1}(M,N) \cong Ext_A^n(k_o,N) \cong \ldots \cong Ext_A^1(k_{n-1},N)$.

Proof: Similar to the proofs of the above lemmas.

Lemma 15: $Ext^o(M,-)$ is equivalent to Hom(M,-), similary $Ext^o(-,N)$ and Hom(-,N) are equivalent.

Proof: If $1E_N: 0 \to E_0 \to E_1 \to \ldots$, then $Ext^0(M,N) = \ker d_{0_*} / Im d_{-1_*}$

$= \ker d_0^* \ldots$ since $Im d_{-1_*} = 0$

If the non-deleted injective resolution is: $0 \to N \to E_0 \to E_1 \to \ldots$, then the left exactness of Hom(M,-) gives an exact sequence

$$0 \to Hom(M,N) \xrightarrow{\epsilon_*} Hom(M,E_0) \xrightarrow{d_0^*} Hom(M,E_1) \to \ldots$$

So, we have $\ker d_{0_*} = Im\ \epsilon_*$

$\therefore\ \epsilon_*: Hom(M,N) \to Ext^0(M,N) = \ker d_{0*} = Im\ \epsilon_*$ is an isomorphism

Hence, $Ext^0(M,-)$ is equivalent to Hom(M,-).

Lemma 16: $Tor_0^A(M,-)$ is naturally equivalent to $M\otimes -$, and $Tor_0^A(-,N)$ is equivalent to $-\otimes N$.

Proof: If $1P_N : \ldots \to p_1 \xrightarrow{d_1} p_o \xrightarrow{d_o}$, then

$Tor_o(M,N) = \ker(1\otimes d_o)/im(1\otimes d_1) = M\otimes p_o/im(1\otimes d_1) = Coker(1\otimes d_1)$.

If the non-deleted resolution is $\ldots \to p_1 \xrightarrow{d_1} p_o \xrightarrow{\epsilon} N \to o$, then the right-exactness of $M\otimes -$ gives us an exact sequence:

$$M\otimes p_1 \xrightarrow{1\otimes d} M\otimes p_o \xrightarrow{1\otimes\epsilon} M\otimes N \to 0$$

$\Rightarrow\ im(1\otimes d_1) = \ker(1\otimes\epsilon)$

Thus, by proposition 1, the map $1\otimes\epsilon$ induces an isomorphism from $M\otimes p_o/\ker(1\otimes\epsilon)$ into $M\otimes N$

But, $M\otimes p_o/\ker(1\otimes\epsilon) = M\otimes p_o/Im(1\otimes d_1) = Tor_o(M,N)$

$\therefore\ Tor_o(M,N) \cong M\otimes N$

Hence, $Tor_o(M,-)$ is equivalent to $M\otimes -$.

- similarly we can prove the other assertion.

For convenience, we list without proof some of the other properties.

Lemma 17: If $0 \to N' \to N \to N'' \to 0$ is an exact sequence of modules and if we apply the covariant functor Hom(M,-), then there is a long exaact sequence:

$0 \longrightarrow Hom(M,N') \longrightarrow Hom(M,N) \longrightarrow Hom(M,N") \xrightarrow{\partial} Ext^1(M,N') \longrightarrow \ldots$

with natural connecting homomorphisms.

Lemma 18: If $o \longrightarrow M' \longrightarrow M \longrightarrow M" \longrightarrow 0$ is an exact sequence of modules, and if we apply the contravariant functor Hom(-,N), then there is a long exact sequence:

$0 \longrightarrow Hom(M",N) \longrightarrow Hom(M,N) \longrightarrow Hom(M',N) \xrightarrow{\partial} Ext^1(M",N) \longrightarrow \ldots$

with natural connecting homomorphisms.

Lemma 19: If $0 \longrightarrow N' \longrightarrow N \longrightarrow N" \longrightarrow 0$ is an exact sequence, then there is a long exact sequence

$\ldots \longrightarrow Tor_1(M,N") \xrightarrow{\partial} M\otimes N' \longrightarrow M\otimes N \longrightarrow M\otimes N" \longrightarrow 0$

with natural connecting homomorphisms, similarly in the other variable.

Next, by using the above concepts we will prove:

If A is a regular local ring of dimension n, then gl.dim A = n. For the proof of this we shall need the following definitions and Lemmas.

Definition 14: Let A = a ring.

The projective (respectively injective) dimension of an A-module M is the length a shortest projective (resp. injective) resolution of M, and denoted by proj.dim M (resp. inj.dim M).

Remark: 1) For an A-module M, we say proj.dim M $\le$ n if there is a projective resolution $0 \longrightarrow p_n \longrightarrow \ldots \longrightarrow p_1 \longrightarrow p_0 \longrightarrow M \longrightarrow 0$. If no such finite resolution exists, define proj.dim M = ∞. Otherewise if n is the least such integer define proj.dim M = n.

2) For an A-module M, we say inj.dim M $\le$ n, if there is an injective resolution $0 \longrightarrow M \longrightarrow E_0 \longrightarrow E_1 \longrightarrow \ldots \longrightarrow E_n \longrightarrow 0$. If no such finite resolution exists, define inj.dim M = ∞. Otherwise if n is the least such integer, define inj.dim M = n.

Examples: (i) If M is projective, then proj.dim M = 0

(because, $0 \to M \xrightarrow{\epsilon} M \to 0$ is a projective resolution of M)

(ii) If M is injective, then inj.dim M = 0

Theorem 4: Given any A-module M, it is always possible to construct an exact sefuence $0 \to k \to F \to M \to 0$ in which F is free.

Proof: Let $\{x_i\}_{i\in I}$ be any system of generators for M. (such a system certainly exists, for example, the family might consist of all the elements of M)

Next, let $\{a_i\}_{i\in I}$ be a family of new symbols but with the same index set, and let F be the free A-module on these symbols. Then, there is a unique homomorphism $f: F \longrightarrow M$ given by $f(a_i) = s_i$. If $\sum_I r_i a_i$ denote a typical element of F, then $f\left(\sum_I r_i a_i\right) = \sum_I r_i x_i$.

$\therefore$ all the x_i belong to Imf

$\therefore$ Imf = M

$\Rightarrow F \xrightarrow{f} M \longrightarrow 0$

put k = kerf.

Thus, $0 \to k \to F \to M \to 0$ is exact, with F free.

Corollary 2: Every module is isomorphic to a factor module of a free module.

Corollary 3: If the A-module M can be generated by $n (n \geq 0)$ elements, then it is possible to construct an exact sequence $0 \to k \to F \to M \to 0$, where F is a f.g free module.

Lemma 20: (i) An A.module M is projective iff $Ext_A^1(M,N) = 0$ for all A-module N.

(ii) M is injective iff $Ext_A^1(A/I,M) = 0$ for all ideal I of A.

Proof: (i) ($\Rightarrow$) **Suppose M is projective**

Then, $\ldots \longrightarrow p_1 \xrightarrow{d_1} p_o \xrightarrow{d_o} M \longrightarrow 0$ is a projective resolution of M, where $p_o = M$, $d_o = 1_M$, $p_i = 0$ $\forall i \geq 1$.

$\therefore$ $Hom_A(1P_M, N) : 0 \xrightarrow{d_o^*} Hom(p_o, N) \xrightarrow{d_1^*} \underbrace{Hom(p_1, N)}_{= (0)} \longrightarrow \ldots$

Thus, $Ext_A^1(M,N) = \ker d_1^* / \operatorname{im} d_o^* = 0$ since $\ker d_1^* = \operatorname{im} d_o^* = Hom(p_o, N)$

Hence, $Ext_A^1(M,N) = 0$

($\Leftarrow$) **Suppose $Ext_A^1(M,N) = 0$ for A-module N**

WTS: M is projective.

Consider the exact sequence $0 \longrightarrow N \xrightarrow{i} k \longrightarrow M \longrightarrow 0$. (The existence is by theorem 4). We need to show this exact sequence splits.

- since $0 \longrightarrow N \xrightarrow{i} k \longrightarrow M \longrightarrow 0$ is a short exact sequence, by lemma 18, there exist a long exact sequence

$$0 \longrightarrow Hom_A(M,N) \longrightarrow Hom_A(K,N) \xrightarrow{i^*} Hom_A(N,N) \xrightarrow{\partial} Ext_A^1(M,N) \longrightarrow \ldots$$

But from $Ext_A^1(M,N) = 0$, we get the exact sequence

$$Hom_A(K,N) \xrightarrow{i^*} Hom_A(N,N) \longrightarrow 0$$

Thus, for $1_N \in Hom_A(N,N)$, $\exists\, g \in Hom_A(K,N)$ such that $i^*(g) = 1_N$

$$\Rightarrow g \circ i = 1_N$$

$\therefore$ The above exact sequence splits.

Hence, M is projective.

(ii) ($\Rightarrow$) Since A/I is free as A-module, it is projective, hence by (i) we get $Ext_A^1(A/I, M) = 0$

($\Leftarrow$) **Suppose $Ext_A^1(A/I, M) = 0$ for all ideal I of A**

WTS: M is injective.

To prove this direction we use the criterion of Baer.

Subclaim: g_1 is well-defined and extends g_o.

- If $m_o + ax = m'_o + a'x$, then $(a-a')x = m'_o - mo \in Mo$

$\Rightarrow a-a' \in I$

$\therefore$ $g_o(a-a')x)$ and $h(a-a')$ are defined.

Also, $g_o(m'_o - m_o) = g_o(a-a')x) = h(a-a') = (a-a')h'(1)$

Thus, $g_o(m'_o) - g_o(m_o) = ah'(1) - a'h'(1)$

$\Rightarrow$ $g_o(m'_o) + a'h'(1) = g_o(m_o) + a\, h'(1)$.

$\therefore$ g_1 is well-defined.

- Since $g_1(m_o) = g_o(m_o)$ for all $mo \in M_o$, g_1 extends g_o.

$\therefore$ $(M_1, g_1) \in S$ and Larger than the maximal pair (M_o, g_o).

which is a contradiction.

Hence, $M_o = N$.

Therefore, $g_o : N \rightarrow E$ and $g_o oi = g_o|_A = f$.

Hence, E is injective

Proof of Lemma 20 (ii) (only if part)

Consider the exact sequence $0 \longrightarrow I \xrightarrow{i} A \longrightarrow A|I \longrightarrow 0$. By Lemma 18, there is a long exact sequence (by applying $Hom_A(-,M)$:

$$0 \longrightarrow Hom_A(A|I,M) \longrightarrow Hom_A(A,M) \xrightarrow{i^*} Hom_A(I,M) \xrightarrow{\partial} Ext^1\ (A|I,M) = 0.$$

$\therefore$ $Hom_A(A,M) \xrightarrow{i^*} Hom_A(I,M) \longrightarrow 0$ is exact.

Let $f \in Hom_A(I,M)$, then $\exists g \in Hom_A(A,M)$ such that $i^*(g) = f$

$\Rightarrow goi = f$

$\therefore$ g extends f.

$\therefore$ For any ideal I of A, the map $f : I \rightarrow A$ can be extended to A.

Hence, by Baer criterion, M is injective.

Lemma 21: Let A be a ring and n be a non-negative integer. Then the following conditions are equivalent:

(1) proj. dim $M \le n$ for all A-module M,

(2) proj. dim $M \le n$ for all f.g A-module M,

(3) inj. dim $M \le n$ for all A-module M,

(4) $Ext_A^{n+1}(M,N) = 0$ for all A-modules M, N.

Proof: (1) $\Rightarrow$ (2) : obvious

(2) $\Rightarrow$ (3) : Suppose proj. dim $M \le n$ for all f.g A-module M.

Let $0 \to M \to u_o \to u_1 \to \dots \to u_{n-1} \to c \to 0$ be an exact sequence with u_j injective $\forall j$. [The existence is from the fact that, if $0 \to M \xrightarrow{\epsilon} u_o \xrightarrow{d_o} u_1 \xrightarrow{d_1} \dots$ is an injective resoluiton of M & $L_o = im\epsilon$, $L_n = imd_{n-1}$ $\forall n \ge 1$, then we have $o \to M \to u_o \to u_1 \to \dots \to u_{n-1} \to L_{n-1} \to o$ is exact with u_j injective $\forall j$]

Let I = an ideal of A. (I arbitrary)

- Since $Ext^{n+1}(A/I,M) \cong Ext^1(A/I,L_{n-1})$, by Lemma 13, we get

$$Ext^{n+1}(A/I,M) \cong Ext^1(A/I,c)$$

- Since A/I is f.g A-module, by (2), $Ext^{n+1}(A/I,M) = 0$, (because proj.dim $A/I \le n$)

$$\Rightarrow Ext^1(A/I,c) = 0$$

By Lemma 20 (ii), we get c is injective.

$\therefore$ we have an injective resolution of M of length n, so inj. dim $M \le n$.

Hence, (3) holds

(3)$\Rightarrow$(4): **Suppose inj.dim $M \le n$ for all A-module M**

Then, by definition, there exist injective resolution

$o \to M \to E_o \to \dots \to E_n \to o \to \dots$ of M with $E_k = o$ $\forall k \ge n+1$

$\therefore$ $Hom_A(E_k,N) = (0)$ $\forall k \ge n+1$.

(i.e. $o \to Hom_A(E_n,N) \to Hom_A(E_{n-1},N) \to \dots \to Hom_A(E_1,N) \to Hom_A(E_o,N) \to Hom_A(M,N)$)

$\therefore$ $Ext^k(M,N) = 0$ $\forall k \ge n+1$

In particular Ext^{n+1} (M,N) = 0 for all A-modules M and N.

Hence, (4) is true.

(4)⇒(1): **Suppose Ext_A^{n+1}(M,N) = 0 for all A-modules M and N.**

WTS: proj. dim M ≤ n for all A-module M.

Take an exact sequence $0 \to C \to P_{n-1} \to P_{n-2} \to \dots \to P_1 \to P_o \to M \to 0$. (*)

Then, by Lemma 14, we have:

$$Ext_A^{n+1}(M,N) \cong Ext_A^1(c,N)$$

⇒ $Ext^1(c,N) = 0$ for all A-module N

∴ c is injective by Lemma 20 (i)

∴ (*) is a projective resolution of M of length n.

Hence, proj.dim M ≤ n for all A-module M

∴ **(1) holds.**

Now let p = sup {proj.dim M | M is an A-module}
i = sup {inj. dim M | M is an A-module}

We assert that p = i. To prove this

- since proj. dim M ≤ p for all A-module M (by definition)
  By lemma 21, inj. dim M ≤ p for all A-module M.
  ⇒ sup {inj. dim | M is an A-module} ≤ p
  ∴ i ≤ p
- similarly we can show that p ≤ i.

Hence, p = i

Definition 15: We call this common value, the **global dimension of A**, and denoted by gl.dim A. ie, gl.dim A = $\sup_M$ (proj. dim M).

Lemma 22: Let A = a noetherian ring

Let M = a f.g A-module.

Then, M is projective iff Ext_A^1 (M,N) = 0 for all f.g A-module N.

Proof: ($\Rightarrow$) **Suppose M is projective**

By Lemma 20 (i), $\mathrm{Ext}_A^1(M,N) = 0$ for all A-module N.

$\therefore$ $\mathrm{Ext}_A^1(M,N) = 0$ for all f.g A-module N.

($\Leftarrow$) **Suppose $\mathrm{Ext}_A^1(M,N) = 0$ for all f.g A-module N.**

WTS: M is projective.

Take a resolution $0 \to R \xrightarrow{i} F \to M \to 0$ with F f.g free A-module we need to show this exact sequence splits.

- clearly R is also f.g (since A is noetherian)

Thus, by Lemma 14, we have:

$$0 \to \mathrm{Hom}(M,R) \to \mathrm{Hom}(F,R) \xrightarrow{i^*} \mathrm{Hom}(R,R) \to \mathrm{Ext}^1(M,R) \to \dots \text{ is exact.}$$

But, $\mathrm{Ext}^1(M,R) = 0$ (by wepothesis since R is f.g).

$\therefore$ $\mathrm{Hom}(F,R) \xrightarrow{i^*} \mathrm{Hom}(R,R) \to 0$ is exact.

$\therefore$ For $1_R \in \mathrm{Hom}(R,R)$, $\exists$ $s: F \to R$ such that $i^*(s) = 1_R$

$\Rightarrow so i = 1_R$

$\therefore$ The exact sequence $0 \to R \to F \to M \to 0$ splits.

$\therefore$ M is isomorphic to a direct summand of a free R-module

Hence, M is projective.

Theorem 6: Let (A, m) = a local ring.

Let M = an A-module with minimal generating set $\{a_1, a_2, \dots, a_n\}$. If F is free on $\{x_1, x_2, \dots, x_n\}$, $\Psi: F \to M$ given by $\Psi(x_i) = a_i$ & $k = \ker \Psi$ then $k \subseteq mF$.

Proof: Suppose $k \subseteq mF$

Then , $\exists$ $\sum r_i x_i \in k$ not in mF.

- since $r \in A$ is a unit if and only if $r \notin m$, one of the coefficients, say r_1 must be a unit .

But, $\sum r_i a_i = 0 \quad \Rightarrow \quad a_1 = r_1^{-1}\left[\sum_{i=2}^{n} r_i a_i\right]$

which is a contradiction to the minimality of $\{a_1, a_2, \dots, a_n\}$.

$\therefore$ $\mathbf{k \subseteq mF}$

Lemma 23: Let (A, m, k) be a noetherian local ring.

Let M = a f.g A-module.

Then, proj. dim $M \leq n$ iff $Tor_{n+1}^{A}(M,k) = 0$.

Proof: (⇒) **Suppose proj. dim $M \leq n$**

Then, there is a projective resolution $0 \to p_n \to p_{n-1} \to \cdots \to p_1 \to p_o \to M \to o$.

By lemma 12, we have: $Tor_{n+1}^{A}(M,k) \cong Tor_{1}^{A}(p_n,k)$.

But, as one can easily see, $Tor_{1}^{A}(p_n,k) = 0$, since p_n is projective.

$$\therefore \mathbf{Tor_{n+1}^{A}(M,k) = 0}$$

(⇐) **Suppose $Tor_{n+1}^{A}(M,k) = 0$**

WTS: proj. dim $M \leq n$.

We proceed by induction on n.

Assume $n = 0$, ie $Tor_{1}^{A}(M,k) = 0$

we need to show proj.dim $M \leq 0$.

consider the exact sequence $o \to L \xrightarrow{i} F \xrightarrow{\Psi} M \to o$ (*) with f.g free, by the long exact theorem, we have the exact sequence:

$$\cdots \to Tor_{1}^{A}(M,k) \to L\otimes K \to F\otimes K \to M\otimes K \to 0$$

$$\therefore 0 \to L\otimes K \xrightarrow{i\otimes 1} M\otimes K \to 0 \text{ is exact}$$

Claim: $i\otimes 1 = 0$

- since $i(L) = \ker \Psi \subseteq mF$ (by thm 6), we have for $y \in L$, $i(y) \in mF$.

$$\Rightarrow i(y) = \sum r_j x_j,\ r_j \in m$$

If $\lambda \in k$, then $i\otimes 1(y\otimes\lambda) = i(y)\otimes\lambda = (\sum r_j x_j)\otimes\lambda = \sum x_j \otimes r_j \lambda$

But, $r_j\lambda = 0 \ \forall j$, since $k = A/m$ and $r_j \in m$, $r_j\lambda \in m$.

$\therefore i\otimes 1(y\otimes\lambda) = 0$

$\therefore i\otimes 1 = 0$ .... since $y\otimes\lambda$ is an arbitrary element of $L\otimes k$.

Thus $0 = \text{im}(i\otimes 1) = \ker(\Psi\otimes 1)$, this implies $\Psi\otimes 1$ is injective.

Therefore, $L\otimes k$ must be zero.

$\therefore \quad 0 = L\otimes k = L\otimes A/m \cong L/mL$

$\therefore L = mL$

- since A is noetherian, L is f.g and hence by Nakayama's Lemma, $L = 0$.

Hence, from (*) , we get Ψ is an isomorphism.

$\therefore F \cong M$

$\therefore$ M is free and hence projective

$\therefore$ proj. dim $M = 0$

Hence, proj. dim $M \le 0$

<u>**Assume $n > 0$**</u> , ie, $\text{Tor}^A_{n+1}(M,k) = 0$

Now, take a projective resolution of M , ie, $\ldots \to p_n \to p_{n-1} \to \ldots \to p_o \to M \to 0$.

Let $k_{n-1} = \ker d_{n-1}$.

Then, $0 \to k_{n-1} \to p_{n-1} \to \ldots \to p_1 \to p_o \to M \to o$ is exact.

By Lemma 12, $\text{Tor}^A_{n+1}(M,k) \cong \text{Tor}^A_1(k_{n-1},k)$

$\therefore \text{Tor}^A_1(k_{n-1},k) = 0$

The case $n = 0$ shows, k_{n-1} is free and hence projective.

$\therefore$ M has a projective resolution of length n.

Hence, proj. dim $M \le n$.

<u>**Recall:**</u>

1. If M is an A-module with $M_p = 0$ for all maximal ideal p of A, then $M = 0$. That is a module which is locally null at every maximal ideal is necessairly a null-module.
2. Let A = a ring, M an A-module.

   Then, $\text{Tor}^A_i(M,N)_p = \text{Tor}^{A_p}_i(M_p,N_p)$.

3. If A is noetherian, and M is f.g, then

$$\text{Ext}^i_A(M,N)_p = \text{Ext}^i_{A_p}(M_p,N_p)$$

Lemma 24: Let A = a noetherian ring

Let M = a f.g A-module. Then:

(i) proj.dim M is equal to the supremum of proj.dim M_p (as A_p-module), for the maximal ideal p of A

(ii) proj.dim $M \le n$ iff $\mathrm{Tor}^A_{n+1}(M, A/p) = 0$ for all maximal ideal p of A.

Proof: (i) Let $s = \sup_{\max.p} \{\text{proj.dim } M_p \mid M_p \text{ as } A_p\text{-module}\}$.

Let $\Omega(A)$ = the set of all maximal ideal of A.

First we show that proj.dim M ≥ s

If proj.dim $M = \infty$, there is nothing to prove.

Assume proj.dim $M = n < \infty$.

Then, by Lemma 21, $\mathrm{Ext}^{n+1}_A(M,N) = 0$ for all A-modules M and N.

Thus, for $p \in \Omega(A)$, we have $\mathrm{Ext}^{n+1}_A(M,N)p = 0$.

Now, let M_p and N_p be an A_p-modules, then M and N are A-modules

$$\therefore \mathrm{Ext}^{n+1}_A(M,N) = 0$$

$$\Rightarrow \mathrm{Ext}^{n+1}_A(M,N)p = 0$$

$$\Rightarrow \mathrm{Ext}^{n+1}_{A_p}(M_p,N_p) = 0 \text{ for all } A_p\text{-modules } M_p \text{ and } N_p.$$

$\therefore$ proj.dim $M_p \le n$ ... by Lemma 21.

$$\therefore \sup_{\max.p} (\text{proj.dim } M_p) \le n$$

Hence, proj.dim M ≥ s

To see the other inequality, ie, $s \ge$ proj.dim M

If $s = \infty$, we are done.

Assume $s = n < \infty$. Then for all $p \in \Omega(A)$, proj.dim $M_p \le n$

$$\Rightarrow \mathrm{Ext}^{n+1}_{A_p}(M_p,N_p) = 0 \text{ for all } A_p\text{-modules } M_p \text{ and } N_p$$

$$\Rightarrow \mathrm{Ext}^{n+1}_A(M,N)\,p = 0 \quad \text{for all } A\text{-modules } M \text{ and } N$$

$\Rightarrow \operatorname{Ext}_A^{n+1}(M,N) = 0$ from the above remark.

$\Rightarrow$ Proj.dim $\leq n = s$

Hence, proj.dim M = $\sup_{\max.p}$ (proj.dim M_p)

(ii) ($\Rightarrow$) **Suppose proj.dim M $\leq$ n.**

WTS: $\operatorname{Tor}_{n+1}^A(M, A/p) = 0$ for all maximal ideal p of A.

From (i) above we get proj.dim $M_p \leq n$ for all $p \in \Omega(A)$. But, we know that $(A_p, p_p, A_p/p_p) = (A_p, pA_p, k)$ is a noetherian local ring, and M_p is f.g.

Hence, by Lemma 23, we get $\operatorname{Tor}_{n+1}^{Ap}(M_p, A_p/p_p) = 0$

$$\Rightarrow \operatorname{Tor}_{n+1}^{Ap}(M_p, (A)_p) = 0$$

$$\Rightarrow \operatorname{Tor}_{n+1}^{A}(M_p, A/p)_p = 0$$

- since this is true for all $p \in \Omega(A)$, we get $\operatorname{Tor}_{n+1}^A(M, A/p) = 0$

Hence, $\operatorname{Tor}_{n+1}^A(M, A/p) = 0 \quad \forall p \in \Omega(A)$

($\Leftarrow$) **Suppose $\operatorname{Tor}_{n+1}^A(M, A/p) = 0$ for all $p \in \Omega(A)$**

WTS proj.dim M $\leq$ n.

For all $p \in \Omega(A)$, $\operatorname{Tor}_{n+1}^A(M, A/p)_p = 0$, which implies $\operatorname{Tor}_{n+1}^{A_p}(M_p, (A/p)_p) = 0$

$$\Rightarrow \operatorname{Tor}_{n+1}^{A_p}(M_p, (A_p/p_p)) = 0$$

Again by Lemma 23, proj.dim $M_p \leq n$ for all $p \in \Omega(A)$.

$$\therefore \sup_{\max.p} (\text{proj.dim } M_p) \leq n$$

Hence, proj.dim M $\leq$ n.

Lemma 25: The following conditions about a noetherian ring A are equivalent:

(1) gl.dim A $\leq$ n

(2) proj.dim M $\leq$ n for all f.g A-module M.

(3) inj.dim $M \le n$ for all f.g A-module M.

(4) $Ext_A^{n+1}(M,N) = 0$ for all f.g A-modules M and N.

(5) $Tor_{n+1}^A(M,N) = 0$ for all f.g A-modules M and N.

Proof: we proceed in the following manner: (5)⇔(2)⇔ (1)

$$\begin{array}{ccc} & \Uparrow & \Downarrow \\ & (4) & \Leftarrow (3) \end{array}$$

(1) ⇔ (2): If gl.dim $A \le n$, then $\sup_M$ proj.dim $M \le n$.

⇒ proj.dim $M \le n$ for all A-module M

⇒ proj.dim $M \le n$ for all f.g A-module M.

∴ **(1) ⇒ (2) holds**

If proj.dim $M \le n$ for all f.g A-module, then proj.dim $M \le n$ for all A-module M by lemma 21.

⇒ $\sup_M$ (proj.dim M) $\le n$

⇒ gl.dim $A \le n$

∴ (2) ⇒ (1) holds.

Hence , **(1) ⇔ (2)**

(1) ⇒ (3): If gl.dim $A \le n$, then proj.dim $M \le n$ for all A-module M

⇒ inj.dim $M \le n$ for all A-module M (by lemma 21.)

⇒ inj.dim $M \le n$ for all f.g A-module M.

Hence, (1) ⇒ (3)

(3) ⇒ (4): **Suppose inj.dim M ≤ n for all f.g A-module M**

WTS: $Ext_A^{n+1}(M,N) = 0$ for all f.g A-modules **M** and N.

Let M and N be f.g A-modules.

- since inj.dim $M \le n$, then there exist an injective **resolution**

$0 \to M \to Eo \to \dots \to E_n \to 0$ of M. Here $E_k = 0 \quad \forall k \ge n + 1$.

The left exactness of $Hom_A(-,N)$ gives us the exact **sequence**:

$0 \to Hom_A(E_n,N) \to Hom_A(E_{n-1},N) \to \dots \to Hom_A(Eo,N) \to Hom_A(M,N)$.

∴ $Hom_A(E_k,N) = 0 \quad \forall k \ge n + 1$

- since N is arbitrary f.g A-module, $Hom_A(E_k,N) = 0$ **for** all f.g A-module N.

∴ **$Ext_A^{n+1}(M,N) = 0$ for all f.g A-modules M and N.**

(4) ⇒ (2): Suppose $Ext_A^{n+1}(M,N) = 0$ for all f.g A-modules M and N.

WTS: proj.dim $M \le n$ for all f.g module M.

Let M and N be f.g A-modules.

Consider the projective resolution $\dots \to p_n \xrightarrow{d_n} p_{n-1} \xrightarrow{d_{n-1}} \dots \to p_2 \xrightarrow{d_2} p_1 \xrightarrow{d_1} p_o \xrightarrow{\epsilon} M \to o$ of M.

Let $k_n = \ker d_n \quad \forall n \ge 1$,. Then $0 \to k_{n-1} \to p_{n-1} \to p_{n-2} \to \dots \to p_1 \to p_o \to M \to 0$ is exact.

By lemma 14, $Ext_A^{n+1}(M,N) \cong Ext_A^1(k_{n-1}, N)$.

$\Rightarrow Ext_A^1(k_{n-1}, N) = 0$ since $Ext_A^{n+1}(M,N) = 0$ by hypothesis

∴ By lemma 22, k_{n-1} is projective.

Thus, M has a projective resolution of length n.

Hence, proj.dim $M \le n$ for all f.g A-module M.

(2) ⇔ (5): If proj.dim $M \le n$ for all f.g A-module M, then any f.g A-module M has a projective resolution $0 \to p_n \to p_{n-1} \to \dots \to p_o \to M \to o$.

But, $Tor_{n+1}(M,N) \cong Tor_1(p_n, N)$ for all f.g A-module N.

- since p_n is projective , $Tor_1(p_n, N) = 0$

∴ $Tor_{n+1}(M,N) = 0$ for all f.g A-modules M and N

Hence, (2) ⇒ (5)

If $Tor_{n+1}^A(M,N) = 0$ for all f.g A-modules , we get $Tor_{n+1}(M, A|p) = 0$ for all maximal ideal p of A.

Thus, by lemma 24(ii) , proj.dim $M \le n$ for all f.g A-module M.

∴ (5) ⇒ (2)

Hence, (2) ⇔ (5)

Lemma 26: For any noetherian ring A,

$$gl.dim\, A = \sup_{max.\, p} gl.dim(A_p).$$

Proof: Let $k = \sup_{max.\, p} gl.dim(A_p)$.

(≥): If gl.dim $A = \infty$, there is nothing to prove.

Assume gl.dim $A = n < \infty$.

Then, gl.dim A ≤ n. By Lemma 25, proj.dim M ≤ n for all f.g A-module M, and by lemma 24, we have $\sup_{\max.p}(\text{proj.dim } M_p) \le n$ for all f.g A_p-module M_p.

∴ proj.dim $M_p \le n$ for all f.g A_p-module M_p and for all $p \in \Omega(A)$.

∴ gl.dim $A_p \le n$, for all $p \in \Omega(A)$ ... by lemma 25.

∴ $\sup_{\max.p} \text{gl.dim}(A_p) \le n$

$$\textbf{Hence, gl.dim A} \ge \sup_{\max.p} \textbf{gl.dim} (A_p)$$

(≤): If k = ∞ , there is nothing to prove.

Assume k < ∞

Then, $\sup_{\max.p} \text{gl.dim}(A_p) \le k$, which implies gl.dim $A_p \le k$ for all $p \in \Omega(A)$..

Let M,N be f.g A-modules

Then, M_p and N_p are f.g A_p-modules.

∴ $\text{Tor}_{k+1}^{A_p}(M_p,N_p) = 0$ for all $p \in \Omega(A)$ by lemma 25.

∴ $\text{Tor}_{k+1}^{A}(M,N)_p = 0$ for all $p \in \Omega(A)$

∴ $\text{Tor}_{k+1}^{A}(M,N) = 0$

- since M and N are arbitrary , we get gl.dim A ≤ k by **lemma 25**

$$\textbf{Hence, gl.dim A} = \sup_{\max.p} \textbf{gl.dim}(A_p)$$

Theorem 7: Let (A,m,k) be a noetherian local ring.

Then, gl.dim A ≤ n iff $\text{Tor}_{n+1}^{A}(k,k) = 0$

Consequently, we have gl.dim A = proj.dim **k** (as A-module).

Proof: (⇒) **Suppose gl.dim A ≤ n**

- Since $k = A/m$ is a f.g A-module, by **Lemma 25** (5) we have $\text{Tor}_{n+1}^{A}(k,k) = 0$.

($\Leftarrow$) **Suppose $\mathrm{Tor}^A_{n+1}(k,k) = 0$**

WTS: $\mathrm{gl.dim}\, A \le n$

By lemma 24, $\mathrm{proj.dim}\, k \le n$. Thus by definition there is a projective resolution $0 \to p_n \to \ldots \to p_1 \to p_0 \to k \to 0$ of k. (*)

If we apply $M \otimes_A$ — for (*) , we get $\mathrm{Tor}_{n+1}(M,k) = 0$ for all A-module M.

In particular , $\mathrm{Tor}_{n+1}(M,k) = 0$ for f.g A-module M.

so, by Lemma 24, $\mathrm{proj.dim}\, M \le n$.

- Since gl.dim A can be computed from projective dimensions of f.g A-modules, we get $\mathrm{gl.dim}\, A \le n$ by Lemma 25.

To prove gl.dim A = proj.dim k (as A-module).

If we consider k as A-module, $\mathrm{proj.dim}\, k \le \mathrm{gl.dim}\, A$.

Let $s = \mathrm{proj.dim}\, k$. Then, $\mathrm{proj.dim}\, k \le s$

$\Rightarrow \mathrm{Tor}^A_{s+1}(k, A/m) = 0$ ... Lemma 24 (i)

$\Rightarrow \mathrm{Tor}^A_{s+1}(k,k) = 0$ ... since $k = A/m$

$\Rightarrow \mathrm{gl.dim}\, A \le s$ ... by theorem 7

$\Rightarrow \mathrm{gl.dim}\, A \le \mathrm{proj.dim}\, k$.

Hence, gl.dim A = proj.dim k (as A-module).

Lemma 27: Let (A, m, k) be a noetherian local ring,

Let M = a f.g A-module.

If $\mathrm{proj.dim}\, M = r < \infty$ and if x is an M-regular element in m, then $\mathrm{proj.dim}\,(M/xM) = r+1$

Proof: By hypothesis there is an exact sequence

$$0 \to M \xrightarrow{x} M/xM \to 0$$

where the first map is multiplication by x.

This short exact sequence gives the long exact sequence:

$$\mathrm{Tor}_i(M,k) \to \mathrm{Tor}_i(M/xM,k) \to \mathrm{Tor}_{i-1}(M,k)$$

Case 1: If $i > r+1$, then $Tor_i(M,k)$ and $Tor_{i-1}(M,k)$ are 0, since proj.dim M = r and M is f.g (by lemma 25)

$\therefore\ 0 \longrightarrow Tor_i(M/xM,k) \longrightarrow 0$ is exact.

$\therefore\ Tor_i(M/xM,k) = 0$

$\Rightarrow\ Tor_i(M/xM,A/m) = 0$

Thus, $Tor_{r+2}(M/xM,A/m) = 0$ and hence by lemma 24, proj.dim$(M/xM) \le r+1$.

$\therefore$ **proj.dim (M/xM) $\le$ r + 1.** **(*)**

Case 2: When $i = r+1$

Then, $Tor_{r+1}(M,k) \longrightarrow Tor_{r+1}(M/xM,k) \xrightarrow{\partial} Tor_r(M,k) \xrightarrow{x} Tor_r(M,k)$ is exact. But $Tor_{r+1}(M,k) = 0$ ... by Lemma 25

$\therefore\ 0 \longrightarrow Tor_{r+1}(M/xM,k) \longrightarrow Tor_r(M.k) \longrightarrow Tor_r(M,k)$ is exact.

- since $k = A/m$ is annihilated by x (because $x \in m$ by hypothesis), the module $Tor_r(M,k)$ is annihilated by x. [ie. let $\dots \to p_n \xrightarrow{d_n} p_{n-1} \xrightarrow{d_{n-1}} \dots \to p_1 \xrightarrow{d_1} p_o \longrightarrow M \longrightarrow o$ be a projective resolution of M, apply $- \otimes_A k$ to get $\dots \to p_n \otimes k \xrightarrow{d_n \otimes 1} p_{n-1} \otimes k \longrightarrow \dots \to M \otimes k \longrightarrow 0$. Then, $Tor_r(M,k) = \ker(d_r \otimes 1)/Im(d_{r+1} \otimes 1)$. But x annilates $p_r \otimes k = p_r \otimes A/m$, so it annihilates $\ker(d_r \otimes 1) \subseteq p_r \otimes K$. Thus, $Tor_r(M,k)$ is annihilated by x].

$\therefore$ Multiplication by x is a zero map on $Tor_r(M,k)$.

$\therefore\ 0 \longrightarrow Tor_{r+1}(M/xM,k) \longrightarrow Tor_r(M,k) \longrightarrow 0$ is exact.

But, since proj.dim M = r, $Tor_r(M,k) \ne 0$, hence $Tor_{r+1}(M/xM,k) \ne 0$.

$\therefore$ **proj.dim (M/xM) $\ge$ r + 1** **(**)**

[If proj.dim $(M/xM) < r+1$, then proj.dim $(M/xM) \le r$ and hence $Tor^A_{n+1}(M/xM,k) = 0$]

Hence, **(*) and (**) gives us proj.dim (M/xM) = r + 1**

Lemma 28: If (A,m,k) is a regular local ring, then m can be generated by an A-sequence $\{x_1,x_2,\dots,x_d\}$ with $d = \dim(A) = \mathrm{rank}_k(m/m^2)$

Proof: (kaplansky, 1970, p.119)

we now prove the main theorem.

Theorem 8: Let (A, m, k) be a regular local ring of dimension n. Then , gl.dim A = n.

Proof: since A is regular , $m = (x_1, x_2, \ldots, x_n)$, where $\{x_1, x_2, \ldots, x_n\}$ is an A-sequence.

Now let us apply lemma 27 repeatedly.

- since A as A-module is free and hence projective, we have proj.dim A = 0

(i) $x_1 \in m$ is not a zero divisor of A, implies proj.dim (A/xA) = proj.dim A + 1 = 0 + 1 = 1.

(ii) $x_2 \in m$ is not a zero divisor of $A/(x_1)$ implies

$$\text{proj.dim}\,([A/(x_1)]/(x_2)) = \text{proj.dim}\,(A/(x_1)) + 1 = 1 + 1 = 2$$

$$\therefore \text{proj.dim}\,(A/(x_1, x_2)) = 2$$

Finally, $x_n \in m$ is not a zero divisor of $A/(x_1, \ldots, x_{n-1})$ implies

$$\text{proj.dim}\,(A/(x_1, x_2, \ldots, x_n)) = \text{proj.dim}\,(A/(x_1, x_2, \ldots, x_{n-1})) + 1 = n - 1 + 1 = n$$

$\therefore$ proj.dim(A/m) = n ... since $m = (x_1, x_2, \ldots, x_n)$

$\therefore$ proj.dim (k) = n ... since $k = A/m$

But, by theorem 7, we have gl.dim A = proj.dim k.

Hence, gl.dim A = n

Next we prove the converse of theorem 8, namely a noetherian local ring of finite global dimension is regular. To prove this we need some results from koszul complex and we use the concept of minimal resolution.

Let A = a ring

Let M = an A-module

Let Ml = denote the complex $\ldots \to o \to o \to M \to o \to o \to \ldots$

Here, it is to be understood that $M_n = 0 \; \forall n \neq o$ and $M_o = M$, so that Ml is both a right complex and a left complex. Ml is called the complex associated to M.

Definition 16: By a left complex over M we mean a left complex $\mathbb{X}$ together with a chain map $\epsilon : \mathbb{X} \to Ml$ called the augmentation map.

ie,
$$\begin{array}{ccccccccccccc} \mathbb{X}: \ldots \to & \mathbb{X}_2 & \to & \mathbb{X}_1 & \to & \mathbb{X}_o & \to & o & \to & o & \to & o & \to \ldots \\ \epsilon \downarrow & & & & & \downarrow \epsilon_o & & & & & & & \\ Ml: \ldots \to & o & \to & o & \to & M & \to & o & \to & o & \to & o & \to \ldots \end{array}$$

Remark: (1) As we have seen from the above diagram only one component of ϵ is non-trivial, that is the so-called augmentation homomorphism. $\epsilon_o : \mathbb{X}_o \to M$.

(2) From the commutative diagram
$$\begin{array}{ccc} \mathbb{X}_o & \to & 0 \\ \downarrow & & \downarrow \\ M & \longrightarrow & o \end{array}$$
, we get a left complex $\ldots \to \mathbb{X}_2 \to \mathbb{X}_1 \to \mathbb{X}_o \to M \to o$ **(Δ)**

Definition 17: By a right complex over M we mean a right complex $\mathbb{Y}$ together with a chain map ϵ: $Ml \to \mathbb{Y}$

This time the non-tnvial part of ϵ is the augmentation homomorphism $\epsilon: M \to \mathbb{Y}_o$, and we get the right complex $o \to M \to \mathbb{Y}_o \to \mathbb{Y}_1 \to \ldots$ **(ΔΔ)**.

Let $\mathbb{Y}$ be a right complex over M and $\mathbb{X}$ a left complex over M.

Definition 18: If the sequence (Δ) and (ΔΔ) are exact, then we say that $\mathbb{Y}$ is an acyclic right complex over M and $\mathbb{X}$ is called an acyclic left complex over M.

Let (A, m, k) be a noetherian local ring.

Let M = a f.g A-module

Let $\Psi: M \to N$ be a homomorphism of f.g A-modules.

Definition 19: we say Ψ is <u>minimal</u> iff $\Psi\otimes 1_k : M\otimes k \to N\otimes k$ is an isomorphism. Equivalently, we say Ψ is minimal iff Ψ is surjective and $\ker \Psi \subseteq mM$.

Definition 20: A free resolution of M, $\ldots \to L_i \xrightarrow{d_i} L_{i-1} \to \ldots \to L_o \xrightarrow{d_o} M \to o$

(*) is called a minimal resolution if $d_i : L_i \to \ker d_{i-1}$ is minimal for all i.

Remark: If (*) is minimal , then

(i) since $d_o : L_o \to M$ is minimal , by definition we have

$$\bar{d}_o : L_o\otimes k \to M\otimes k \text{ is an isomorphism.}$$

(ii) The complex $L.\otimes k$: $\ldots \to \bar{L}_i \xrightarrow{\bar{d}_i} \bar{L}_{i-1} \to \ldots \to \bar{L}_o$, where $\bar{L}_i = L_i\otimes k \cong L_i/mL_i$, has trivial differentiation.

Proof: To see this $\bar{d}_i = L_i/mL_i \longrightarrow L_{i-1}/mL_{i-1}$.

- since $d_i : L_i \to \ker d_{i-1}$ is minimal , then d_i is surjective

$$\therefore d_i L_i = \ker d_{i-1}$$

- since $d_{i-1} = L_{i-1} \to \ker d_{i-2}$ is minimal, then $\ker d_{i-1} \subseteq mL_{i-1}$ (by definition)

$$\therefore d_i L_i \subseteq mL_{i-1}$$

Now let $x + mL_i \in L_i/mL_i$, then

$$\bar{d}_i(x + mL_i) = d_i(x) + mL_{i-1}$$

$$= mL_{i-1} \quad \ldots \text{ since } d_i(x) \subseteq mL_{i-1}$$

Hence, $\bar{d}_i = 0$ for all i

(iii) For each i, we have:

$$\mathrm{Tor}_i^A(M,k) = \ker \bar{d}_i / \mathrm{Im}\, \bar{d}_{i+1}$$

$$= \ker \bar{d}_i \quad \ldots\ldots\ldots \text{ since } \mathrm{Im}\, \bar{d}_{i+1} = (0)$$

$$= L_i/mL_i \quad \ldots\ldots\ldots\ldots \text{ since } \bar{d}_i \text{ is a zero map from } L_i/mL_i \to L_{i-1}/mL_{i-1}.$$

But, we know that the A-module L_i/mL_i can be regarded as a finite dimensional vector space over k, and that

$$\text{rank } L_i = \text{rank } L_i/mL_i.$$

$$\therefore \; L_i \text{ is f.g over A}$$

$$\textbf{Hence, rank } L_i = \text{rank}_k \; Tor_i^A(M,k).$$

Lemma 29: A minimal resolution of M exists and unique upto isomorphism

Proof: Let $\{u_1, u_2, \ldots, u_p\}$ be a minimal generating set of M.

Let $L_o = Ae_1 + Ae_2 + \ldots + Ae_p$ be a free module.

Define $\epsilon: L_o \to M$ by $\epsilon(e_i) = u_i$, which is clearly an epimorphism.

Let $k_1 = \ker \epsilon$.

Then, we have the exact sequence $0 \to k_1 \xrightarrow{d_1} L_o \xrightarrow{\epsilon} M \to 0$.

claim: $\ker \epsilon = d_1(k_1) \subseteq mL_o$.

Suppose not, ie, $\ker \epsilon \not\subseteq mLo$.

Then, $\exists\, \Sigma r_i e_i \in k$, but not in mL_o. So atleast one of the r_i's is not in m, say r_1.

$$\therefore \; r_1 \text{ is a unit.}$$

- since $\epsilon(\Sigma r_i e_i) = 0$ then $\Sigma r_i u_i = 0$, so we get $u_1 = r_1^{-1}(\sum_{i=2}^{n} r_i u_i)$ which is a contradiction to the minimality of $\{u_1, u_2, \ldots, u_p\}$.

$$\therefore \; \ker \epsilon \subseteq mL_o$$

$$\textbf{Hence, } \epsilon : L_o \to M \textbf{ is minimal}$$

Now consider $d_1 : k_1 \to \ker \epsilon$, clearly it is surjective and $\ker d_1 = (0) \subseteq mk_1$.

$$\therefore \; d_1 \textbf{ is also minimal}$$

- since A is noetherian, k_1 is f.g A-module, so we can proced as above, and finally we get a minimal resolution of M. This proves the existence part.

Uniqueness (see Matsumura, 1980, p.136)

The next Lemma is stated without proof.

Lemma 30: Let $\ldots \to L_i \xrightarrow{d_i} L_{i-1} \to \ldots \xrightarrow{d_1} L_o \xrightarrow{\epsilon} M \to 0$ be a minimal resolution of M. $\ldots \to F_i \xrightarrow{d'_i} F_{i-1} \to \ldots \xrightarrow{d'_1} F_o$ be a complex with an augementation homomorphism $\epsilon' : F_o \to M$ such that:

(i) each F_i is f.g free over A,

(ii) $\bar{\epsilon}' : \bar{F}_o \to \bar{M}$ is injective, and

(iii) $d'_i(F_i) \subseteq mF_{i-1}$ for each $i > 0$ and d'_i induces an injection

$$\bar{F}_i \longrightarrow (m|m^2) \otimes F_{i-1}.$$

Then, there exist a homomorphism of complexes over M $f : F \to L$. Such that each f_i maps F_i isomorphically onto a direct summand of L_i consequently, we have:

$$\text{rank } F_i \le \text{rank} L_i = \text{rank}_k \, Tor_i^A(M,k).$$

Theorem 9: Let (A, m, k) be a noetherian local ring,

Let $s = \text{rank}_k(m/m^2)$.

Then, $\text{rank}_k \, Tor_i^A(k,k) \ge \binom{s}{i}$ for $0 \le i \le s$.

Proof: Consider k as A-module. Then , k is f.g , and hence by lemma 29, it has a minimal resolution.

Let $\ldots \to L_i \to L_{i-1} \to \ldots \to L_1 \to L_o \to k \to o$ be the minimal resolution of k.

Let $m = (x_1, x_2, \ldots, x_s)$.

Consider the koszul complex $F. = k.(x_1, x_2, \ldots, x_s, A)$.

- clearly $F_o = A$, so there is an obvious augmentation homomorphism $\epsilon : F_o \to k$

WTS: The condition of Lemma 30 are all satisfied.

From $F_p = k_p(\underline{x}, A) \cong A \otimes_A \wedge^p G$, where $G = A_{x_1} + A_{x_2} + \ldots + A_{x_s}$ free A-module of rank s .

$\cong \wedge^p G$ ..... since A is free of dimension 1.

But, $\wedge^p G$ is a free A-module of dimension $\binom{s}{p}$.

$\therefore F_p$ is f.g free over A.

Hence, condition (i) is fuifilled.

- Consider $\bar{\epsilon}: A\otimes k \longrightarrow k\otimes k$
  - since $\epsilon: A \longrightarrow A/m$ is surjective and $\ker\epsilon = m \subseteq mA$, we get ϵ is minimal.

    $\therefore$ $\bar{\epsilon}$ is an isomorphism

    $\therefore$ $\bar{\epsilon}$ is injective.

Hence, condition (ii) is satisfied

- Let $d_p: F_p \to F_{p-1}$, where $F_p = k_p(\underline{x}, A)$ and $F_{p-1} = k_{p-1}(\underline{x}, A)$.

  Let $\sum_{i_1<\ldots<i_p} m_{i_1 i_L \ldots i_p} e_{i_1 i_2 \ldots i_p}$ be an orbitrary element of F_p.

Then,
$$d_p\left[\sum_{i_1<\ldots<i_p} m_{i_1 i_2 \ldots i_p} e_{i_1 i_2 \ldots i_p}\right] = \sum_{j=1}^{s} \underbrace{x_i}_{\in m} \underbrace{\underbrace{\left[\sum_{i_1<\ldots<i_{p-1}} m_{j\, i_1 \ldots i_{p-1}} e_{i_1 \ldots i_{p-1}}\right]}_{\in F_{p-1}}}_{\in mF_{p-1}}$$

So by construction we have $d_p(F_p) \subseteq m\, F_{p-1}$ (•).

To show d_p induces an injection from $\bar{F}_p \to m/m^2 \otimes_A F_{p-1}$, we have:

$$\bar{F}_p \cong F_p/m\, F_p \quad \text{and} \quad m/m^2 \otimes F_{p-1} \cong mF_{p-1}/m^2 F_{p-1}.$$

Let $\bar{d}_p: F_p/mF_p \to mF_{p-1}/m^2 F_{p-1}$.

Now, let $x = \sum_{i_1<\ldots<i_p} q_{i_1 \ldots i_p} e_{i_1 \ldots i_p}$, where $q_{i_1 \ldots i_p} \in A$ be an element of F_p such that $d_p(x) \in m^2 F_{p-1}$.

WTS: $x \in mF_p$.

To show this we shall examine the coefficients of $e_{i'_1 \ldots i'_{p-1}}$ in $d_p(x)$, where $i'_1, \ldots, i'_{p-1}$ are arbitrary integers satisfying $1 \le i'_1 < \ldots < i'_{p-1} \le s$.

Let i^* $(1 \le i^* \le n)$ be different from all $i'_1, \ldots, i'_{p-1}$ and choose $l^* = l^*(i^*)$, so that $i'_1 < \ldots < i'_{l^*} < i^* < i'_{l^*+1} < \ldots < i'_{p-1}$.

Then the term

$e_{i'_1 \ldots i'_{1*} i\, i'_{1*+1} \ldots i'_{p-1}}$ in the representation of x contributes to $d_p(x)$ a term $x^{*} q_{i'_1 \ldots i^{*} \ldots i'_{p-1}} e_{i'_1 i'_2 \ldots i'_{p-1}} \in m^2 F_{p-1}$. (since $d_p(x) \le m^2 d_{p-1}$).

$\therefore \sum_{i_*} x_i{}^{*}\, q_{i'_1 \ldots i^{*} \ldots i'_{p-1}} \in m^2$ ... since it is the coefficient of the element $d_p(x)$ of mF_{p-1}.

$\Rightarrow q_{i'_1 \ldots i^{*} \ldots i'_{p-1}} \in m.$

- since $i'_1, \ldots, i^{*}, \ldots, i'_{p-1}$ are arbitrary, we get $q_{i_1 \ldots i_p} \in m$ for all sets $i_1, i_2, \ldots, i_s$.

$\therefore x \in mF_p$.

Hence, the induced map is injective

so, all the condition of lemma 30 are satisfied.

$\therefore$ each F_i is isomorphic to a direct summand of L_i

$\therefore \operatorname{rank} F_i \le \operatorname{rank} L_i = \operatorname{rank}_k \operatorname{Tor}_i^A(k,k)$

But, $\operatorname{rank} F_i = \binom{s}{i}$ .... by the above discussion.

Hence, $\operatorname{rank}_k \operatorname{Tor}_i^A(k,k) \ge \binom{s}{i}$, $0 \le i \le s$

Now , we are ready to prove the converse of theorem 8.

Recall: Let (A, m, k) be a noetherian local ring.

Let M = f.g A-module.

Then: (1) The depth of M = 0 iff $m \in \operatorname{Ass}(M)$

(2) depth $M \le \dim M$ if $M \ne 0$

(3) If proj.dim $M < \infty$, then proj.dim M + depth M = depth A (This formula is due to Auslander - Buchsbaum)

Theorem 10: (serre) Let (A, m, k) be a noetherian local ring.

Then, A is regular iff gl.dim $A < \infty$.

Proof: ($\Rightarrow$) This is theorem 8.

($\Leftarrow$) Suppose gl.dim $A = n < \infty$.

WTS: A is regular.

we show $\dim A = \mathrm{rank}_k(m/m^2)$.

Let $S = \mathrm{rank}_k(m/m^2)$.

By theorem 9, since $\mathrm{rank}_k \mathrm{Tor}_s^A(k,k) \geq \begin{bmatrix} s \\ s \end{bmatrix} = 1$, we get $\mathrm{Tor}_s^A(k,k) \neq 0$.

$\therefore$ gl.dim $A \geq s$ .... (Δ)

[For if gl.dim $A < s$, then gl.dim $A \leq s-1 \Rightarrow \mathrm{Tor}_s^A(k,k) = 0$ which is a contradiction].

On the other hand, since $\mathrm{Ass}(A/m) = \{m\}$, ie, $m \in \mathrm{Ass}(k)$, depth $k = 0$ by (1) above. So if we consider k as A-module, we get proj.dim $k \leq$ gl.dim $A < \infty$, hence from (3) above we have:

proj.dim k + depth k = depth A.

$\therefore$ proj.dim k = depth A ($\Delta\Delta$)

Hence, $\dim A \leq \mathrm{rank}_k(m/m^2) = s$

= gl.dim A .... from (Δ)

= proj.dim k .... by theorem 7

= depth A ..... from ($\Delta\Delta$)

$\leq$ dim A .... from # 2 above

$\therefore \dim A = \mathrm{rank}_k(m/m^2)$.

Hence, A is regular.

Recall: Let s be a multiplicative subset of a ring A. Then:

(1) A_s is flat over A

(2) If A is commutative, and M is an A-module, then M is A-projective implies M_s is A_s-projective.

(3) If A is noetherian, then A_s is noetherian.

Corollary 4: If A is a regular local ring, then A_p is regular for any $p \in \mathrm{spec}\ (A)$.

Proof: Let (A, m, k) be a regular local ring.

Let $p \in \mathrm{spec}\ (A)$.

WTS: A_p is regular.

- clearly A_p is a noetherian local ring, by (3) above, so it suffices to show gl.dim $A_p < \infty$.

Let M = an A_p-module.

Consider M as A-module.

- since A is regular, gl.dim $A < \infty$, which implies proj.dim $M < \infty$.

Hence, M has a projective resolution of finite length, say n.

$$0 \to P_n \to P_{n-1} \to \dots \to P_o \to M \to 0.$$

$$\therefore n \le \text{gl.dim } A$$

By (1) above, A_p is flat over A, so by definition of flatness, we get:

$$0 \to P_n \otimes A_p \to P_{n-1} \otimes A_p \to \dots \to P_o \otimes A_p \to M \otimes A_p \to 0 \text{ is exact}$$

$$\Rightarrow \quad 0 \to (P_n)_p \to (P_{n-1})_p \to \dots \to (P_o)_p \to M_p = M \to 0 \text{ is exact.} \qquad (*)$$

But, by (2) above, each $(P_i)_p$ is A_p-projective $\forall i = 1,2,\dots,n$.

Hence, (*) is a projective resolution of M as A_p-module.

$\therefore$ proj.dim $M \le n$

$\therefore$ proj.dim $M \le n \le$ gl.dim A $\qquad$ (**)

- since M is arbitrary, (**) is true for all A_p-module M, so we have

$$\sup_M (\text{proj.dim } M) \le \text{gl.dim } A$$

$\Rightarrow$ gl.dim $A_p \le$ gl.dim $A < \infty$ since A is regular.

$\Rightarrow$ gl.dim $A_p < \infty$.

Hence, **by theorem 10, A_p is regular for all $p \in$ spec (A)**

Now we are in a position to give the definition of a regular ring.

Definition 21: A noetherian ring A is called <u>regular</u> if A_p is a regular local ring for every maximal ideal p of A.

In view of the above corollary, this definition is equivalent to saying that A_p is a regular local ring for every $p \in$ spec (A).

4. General properties of polynomial rings

Let A = a commutative ring with unity, and I ideal of A.

Let $A[x_1,\dots,x_n]$ = the ring of polynomials in $x_1,x_2,\dots,x_n$ with coefficients in A. Then, we have the followng properties:

Proposition7: $IA[x_1,x_2,\dots,x_n] \cap A = I$

Proposition 8: Let $\varnothing : A \to A/I$ be the natural mapping.

Then one can obtain a ring epimorphism $A[x_1,\dots,x_n] \to (A/I)[x_1,\dots,x_n]$ by operating with $\varnothing$ on the coefficients of each polynomial in $A[x_1,\dots,x_n]$. The kernel of this epimorphism is clearly $IA[x_1,\dots,x_n]$.

Hence, $\mathbf{A[x_1,x_2,\dots,x_n]/\ IA[x_1,\dots,x_n] \cong (A/I)[x_1,\dots,x_n]}$

(This isomorphism is frequently used to identify the two rings.)

Proposition 9: Let s be a non-empty multiplicative subset of A. Then, it is also a multiplicative subset of $A[x_1,x_2,\dots,x_n]$. So we may form the ring $A[x_1,x_2,\dots,x_n]_s$ of factions.

Let $f = \sum r_{v_1 v_2 \dots v_n} x_1^{v_1} x_2^{v_2} \dots x_n^{v_n} \in A[x_1,\dots,x_n]$ be a typical element of $A[x_1,\dots,x_n]$.

Define $\Psi : A[x_1,\dots,x_n]_s \longrightarrow A_s[x_1,\dots,x_n]$ by $\Psi(\frac{f}{s}) = \sum\left[\frac{r_{v_1 \dots v_n}}{s}\right] x_1^{v_1} \dots x_n^{v_n}$

clearly Ψ is an isomorphism.

Hence, $\mathbf{A[x_1,\dots,x_n]_s \cong A_s[x_1,\dots,x_s]}$

Proposition 10: Let p be a prime ideal of A.

Then, $PA[x_1,\dots,x_n]$ is a prime ideal of the polynomial ring $A[x_1,\dots,x_n]$.

Proposition 11: Let A = a noetherian ring:

Let p = a prime ideal of A.

Then, $PA[x_1,...,x_n]$ is a prime ideal of $A[x_1,...,x_n]$ and it has the same height as p.

Proof: (North cott, 1968, p.265)

Proposition 12: Let F = a field.

Then, each ideal of the polynomial ring F[x] can be generated by a single element.

Proof: (Northcott, 1968, p.269)

Proposition 13: Let F = a field

Then, F[x] is not a field, but every non-zero prime ideal is a maximal ideal.

Proof: (Northcoth, 1968, p.269)

Recall: Let A = a ring,

Let M = an A-module, U ⊆ M and N a submodule of M generated by U

Then, if $x: M \to M_s$ is the cannonical mapping and N_s is regarded as an A_s-submodule of M_s then N_s is generated by x(U).

Theorem 11: If A is regular, so is A[x]

Proof: Let Π be a maximal ideal of A[x].

Let d = dim A.

WTS: $A[x]_{\Pi}$ is a regular local ring.

ie, To show dim $A[x]_{\Pi}$ = d+1 and the maximal ideal of $A[x]_{\Pi}$ is generated by d+1 elements.

- clearly $A[x]_{\Pi}$ is a noetherian local ring.

Let p = Π ∩ A

Now, if $s = A-p$, then by prop. 4, $A[x]_s \cong A_s[x]$. On this understanding Π_s is a maximal ideal of $A_s[x]$. Since A is regular, A_s is a regular local ring, so Π_s contracts to the maximal ideal of A_s. So for our purpose we may add the assumption that A is a regular local ring, and that Π of $A[x]$ contracts to the maximal ideal of A.

Hence, (A,P) is a local ring.

(i) To show $\dim A[x]_{\Pi} = d+1$

- Since P is a prime ideal of A, PA[x] is a prime ideal of A[x]. But, since $A[x]/PA[x] \cong (A/P)[x] = k[x]$ is not a field by prop 13 PA[x] is not a maximal ideal of A[x]. So $\Pi/PA[x] \neq 0$ ideal of k[x].

Then, by prop 12, $\Pi/PA[x]$ can be generated by a single element, say f.

$\therefore \ \Pi = pA[x] + fA[x]$

Let $p = (\alpha_1, \alpha_2, \ldots, \alpha_d)$

$\therefore$ htp = d . . . . since dim A = ht p

- Since A is noetherian and P a prime ideal of A, by prop. 11, ht(PA[x]) = d

$\therefore \ ht(\Pi) = d + 1.$

But, $\dim A[x]_{\Pi} = ht(\Pi) = d+1$ . . . . since dim $(A_p) = ht(p)$.

Hence, $\dim A[x]_{\Pi} = d+1$

(ii) To show the maximal ideal of $A[x]_{\Pi}$ is generated by d+1 elements.

Let $\Psi: A[x] \longrightarrow A[x]_{\Pi}$ be the cannonical mapping

Let $\alpha_1', \alpha_2', \ldots, \alpha_d', f'$ be the images of $\alpha_1, \alpha_2, \ldots \alpha_d, f$ under Ψ, which are distinct.

Then, by the above result, the extension of $\Pi = (\alpha_1, \alpha_2, \ldots, \alpha_d, f)A[x]$ in $A[x]_{\Pi}$ is generated by $\alpha_1', \alpha_2', \ldots, \alpha_d', f'$.

$\therefore \ \Pi_s$ is generated by $\alpha_1', \alpha_2', \ldots, \alpha_d', f'$, where $s = A[x]-\Pi$

But, we know that if s = A-P, then the prime ideals of A which do not meet S are those contained in P, and that the prime ideals of A are in a 1-1 correspondence with the prime ideals of A that are in p. Indeed if $p' \subset p$ is a prime ideal of A the corresponding prime ideal of A_p is it's extension. That will be contained in the extension of P. Therefore, it follows that the extension of P is the only maximal ideal of A_p.

Hence, Π_s is the only maximal ideal of $A[x]_\Pi$.

$\therefore$ The maximal ideal of $A[x]_\Pi$ is generated by d+1 elements.

$\therefore$ $\text{rank}_k(\Pi_s/\Pi_s^2) = d+1$

$\therefore$ $A[x]_\Pi$ is a regular local ring.

- since Π is an arbitrary maximal ideal of A[x], we get

A[x] is regular

Corollary 5: If A is regular, so is $A[x_1, \ldots, x_n]$.

Proof: Follows from theorem 11, by induction on n.

Recall: Let k = a field

Let Π = any maximal ideal of the polynomial ring $k[x_1, \ldots, x_n]$

Then, $ht(\Pi) = n$ and Π can be generated by n elements.

Corollary 6: (Hilbert syzygy theorem)

Let $A = k[x_1, x_2, \ldots, x_n]$ be a polynomial ring over a field k.

Then, gl.dim A = n

Proof: Let Π be a maximal ideal of A.

- Since k is a field and hence noetherian, we have A is noetherian.

$\therefore$ A_Π is a noetherian local ring (as A = commutative)

- Since a k-module is a vector space over k, and hence possesses a basis every k-module is free and hence projective.

$\therefore$ For every k-module M, proj.dim M = 0

$\therefore$ gl.dim k = 0 < ∞.

But, since k is a noetherian local ring (trivially), k must be regular by theorem 10.

$\therefore$ $k[x_1,\dots,x_n]$ is regular by corollary 6.

$\therefore$ $A_{\Pi} = k[x_1,\dots,x_n]_{\Pi}$ is a regular local ring.

Thus, by theorem 8, we have:

$$\begin{aligned} \text{gl.dim } A_{\Pi} &= \dim A_{\Pi} \\ &= ht(\Pi) \quad \dots \text{ since } \dim A_p = ht(p) \text{ for all } p \in \text{spec } (A) \\ &= n \end{aligned}$$

Hence, gl.dim $A_{\Pi} = n$

- Since Π is an arbitrary maximal ideal of A, if we take the suppremum over all maximal ideal we get

  gl.dim A = n by lemma 26 //

5. Regular Local Rings as UFD

In this section we are going to prove that every regular local ring is a unique factorization domain (UFD). To prove this theorem, we shall introduce some auxillary concepts.

Definition 22: Let A be a ring , $0 \neq a \in A$. we say a is irreducible if:

(1) a is not a unit of A

(2) whenever $a = xy$, $x, y \in A$, either x or y is a unit of A.

Definition 23: An integral domain A is called a unique factorization domain (UFD) if the following two conditions are satisfied:

(1) If a is non-zero non-unit of A, then a can be written as a finite product of irreducible elements of A.

(2) If a is non-zero non-unit of A , and if

$$a = \pi_1\pi_2\dots\pi_s = \lambda_1\lambda_2\dots\lambda_t$$

are two expressions of a as a product of irreducible elements, then $s = t$ and it is possible to renumber $\pi_1, \pi_2, \dots, \pi_s$ so that π_i and λ_i are associates $(1 \leq i \leq s)$.

Examples: (1) The ring of integers Z. In Z, we have, for instance $24 = (2)(2)(3)(2) = (-2)(-3)(2)(2)$. Here 2 and -2 are associates as are 3 and -3.

Thus, except for order and associates, the irreducible factors in these two factorizations of 24 are the same.

(2) The ring of polynomials, F[x], with coefficients in a Field.

Proposition 14: Let A be an integral domain. Then A is a UFD iff every irreducible element is prime and the principal ideals of A satisfy the ascending chain condition (acc).

Proof: Similar to the proof of a principal ideal domain is a UFD.

Lemma 31: A noetherian domain A in which every irreducible element generates a prime ideal is a UFD.

Proof: Since A is noetherian, the principal ideals of A satisfy the acc. Let π = an irreducible element of A.

Then, (π) is a prime ideal by hypothesis.

But, in an integral domain we know that (π) is a prime ideal iff π is a prime element

$\therefore$ π is a prime element of A

Hence, by prop.14, A is a UFD.

Theorem 12: A noetherian integral domain A is a UFD iff every prime ideal of height 1 is principal

Proof: I. **Suppose A is a UFD**

Let p = a prime ideal of height 1 of A.

WTS: p is principal

Let $a \in P$, $a \neq 0$. Let $a = \prod p_i$, as a product of prime (irreducible) elements. (This is possible since A is a UFD).

- Since p is a prime ideal, atleast one of the p_i belongs to p.

If $p_i \in p$, then $(p_i) \subseteq p$, but (p_i) is a non-zero prime ideal and ht(p) = 1 (by assumption).

$\therefore$ $p = (p_i)$

$\therefore$ p is principal

Hence, every prime ideal of height 1 is principal

II. **Suppose every prime ideal of height 1 is principal**

WTS: A is a UFD

Let π = an irreducible element of A.

Let p = minimal prime over ideal of πA.

Then, $ht(p) \leq 1$ .... by Lemma 2.

$\therefore$ ht(p) = 1.

Thus, by hypothesis, we have p is principal.

Let p = (a).

- Since $\pi A \subseteq p$ and π is irreducible then $\pi = au$, where u is a unit.

$\therefore$ π and a are associates.

$\therefore$ $(\pi) = (a) = p$

$\therefore$ π generates a prime ideal

- Since π is arbitrary, we get every irreducible element of A generates a prime ideal.

Hence, by Lemma 31, A is a UFD

Theorem 13: Let A = a noetherian integral domain,

Let Γ = a set of prime elements of A.

Let S = the multiplicative subset generated by Γ.

Then, A_S is UFD implies A is a UFD.

Proof: Assume $\Gamma \neq \phi$, otherwise $s = \{0\}$ and $A_s = A$, and hence the result holds trivially.

Now suppose A_s is a UFD

WTS: A is a UFD

It suffices to show that every prime ideal of height 1 is principal.
Let p be a prime ideal of height 1.

(i) If $p \cap S \neq \phi$, then p contains an element $s \in S$. But since $s = \pi_1 \pi_2 \ldots \pi_r$ with $\pi_i \in \Gamma$ and p is prime, $\pi_i \in p$ for some i.

$\therefore$ P contains an element π of Γ.

- Since πA is a non-zero prime ideal of A (as π is a prime element of A and A is an ID), $\pi A \subseteq P$ and p is of height 1 we have $p = \pi A$.

Hence, P is principal

(ii) If $p \cap s = \phi$, then pAs is a height 1 prime ideal of A_s.

- Since A_s is a UFD, by theorem 12, we have pA_s is principal.

$\therefore pA_s = aA_s$ for some $a \in P$.

Now, among such a choose the one such that aA is maximal. [maximal in the sense that there is no $a' \in p$ such that $aA \subset a'A$]

Claim: $p = aA$

Clearly, a is not divisible by any $\pi \in \Gamma$. [For if, a is divisible by $\pi \in \Gamma$, then $a = \pi x$ for some $x \in A$, which implies $\pi x \in p$ and hence $x \in p$. But from $a = \pi x$ we get $aA \subset xA$ (not equal since π is not a unit) which is a contradiction to the maximality of aA.]

Let $x \in P$. Then, $\frac{x}{1} \in pA_s$ . . . since $1 \in A$, $1 \in s$, $\frac{1}{1} = 1 \in A_s$

$\therefore \frac{x}{1} \in aA_s \Rightarrow \frac{x}{1} = ak$ for some $k \in A_s$

$\Rightarrow \frac{x}{1} = a\frac{y}{s}$ for some $s \in S$ and $y \in A$

$\Rightarrow sx = ay$

$\therefore sx = ay$ for some $s \in S$ and $y \in A$.

Let $s = \pi_1 \ldots \pi_r$, with $\pi_i \in \Gamma$. Since a is not divisible by any $\pi \in \Gamma, a \notin \pi_i A$, and hence $y \in \pi_i A$. (because $sx \in \pi_i A$, ie, $\pi_i(\pi_1 \ldots \pi_{i-1}\pi_{i+1} \ldots \pi_r)x \in \pi_i A$)

Thus, an induction on r shows that $y \in sA$.

$y = sk$ for some $k \in A$.

$\therefore \; sx = ay = ask = sak$

$\therefore \; x = ak \in aA$, since $s \neq 0$

$\therefore \; P \subseteq aA$

But, since $a \in p$, we get $aA \subseteq p$, and hence $p = aA$.

Hence, p is principal.

In any case, we get p is principal, then by theorem 12.

A is a UFD

Definition 24: A finite free resolution (or FFR for short) of an A-module M is an exact sequence $0 \to F_n \to F_{n-1} \to \ldots \to F_1 \to F_o \to M \to o$ (of finite length) such that each F_i is a f.g free module, $(0 \leq i \leq n)$.

Remark: For any prime ideal p of A, $o \to (F_n)_p \to \ldots \to (F_o)_p \to M_p \to o$ is an FFR of the A_p-module M_p. (as A_p is flat over A).

Definition 25: Let k = a field of fractions of the integral domain A. For a f.g A-module M, the dimension of $M \otimes_A k$ as a vector space over k is called the rank of M.

Remark: 1. The rank of a module M over an integral domain A is the maximal number of elements of M linearly indpendent over A, and

2. The number of elements in any basis of a f.g free A-module F is called the rank of F(over A).

Definition 26: Let A = a ring , M an A-module.

we say that M is stably free if there exists f.g free modules F and F′ such that $M \otimes F \cong F'$.

Remark: Obviously, a stably free A-module M is a f.g projective A-module and has an FFR, $0 \to F \to F' \to M \to 0$.

Proposition 15: If every f.g module over a noetherian ring A has an FFR, then A is regular.

Proof: Let $p \in$ spec (A).

WTS: A_p is a regular local ring

Let M = a f.g A_p-module. Then, M is a f.g A-module.

By hypothesis, M has an FFR, say $0 \to F_n \to F_{n-1} \to \ldots \to F_1 \to F_o \to M \to 0$

- Since F_n is free and hence projective A-module, then $(F_n)_p$ is projective A_p-module.

$\therefore$ proj.dim M $\le$ n. (as A_p-module)

- Since M is arbitrary f.g A_p-module and gl.dim (A_p) can be calculated from projective dimensions of f.g modules, we get

gl.dim $(A_p) < \infty$

$\therefore$ A_p is regular . . . . by theorem 10.

Hence, A is regualr.

Proposition 16: A f.g projective module having an FFR is stably free. (Hint: use induction on the length of the FFR).

Recall: 1. The determinant of a square matrix $A = (a_{ij})_{nxn}$ denoted by det (A) is :

$$\begin{vmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \vdots & \vdots \quad\ \ \vdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{vmatrix} = \sum_{K} (-1)^{\mu(\Pi)} a_{1j1} a_{2j2} \cdots a_{njn}$$

where $j_1, j_2, \ldots, j_n$ is a permutation Π of $1,2,\ldots,n$ and the summation extends over all n! permutations Π.

2. The cofactor in det (A) of an element of A.

Example: Let $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, then

$$\det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}(a_{22}a_{33} - a_{23}a_{32}) + a_{12}(a_{23}a_{31} - a_{21}a_{33}) + a_{13}(a_{21}a_{32} - a_{22}a_{31})$$

$$= a_{11}A_{11} + a_{12}A_{12} + a_{13}A_{13}$$

The expressions in parenthesis are cofactors of a_{11}, a_{12} and a_{13} respectively.

3. The cofactor A_{ij} of a_{ij} in the expansion of det A is $(-1)^{i+j}$ times the determinant of the submatrix obtained by deleting the i^{th} row and the j^{th} column of A.

4. The determinant of the product of two square matrices is the product of their determinant.

5. In (2), we have $\det A = \sum_{i=1}^{3} a_{1i}A_{1i}$, but for $j \neq 1$, $\sum_{i=1}^{3} a_{ji}A_{1i} = 0$

Proof: For j = 2, we have:

$$\sum_{i=1}^{3} a_{2i}A_{1i} = a_{21}A_{11} + a_{22}A_{12} + a_{23}A_{13}$$

$$= a_{21}(a_{22}a_{33}-a_{23}a_{32})+a_{22}(a_{23}a_{31}-a_{21}a_{33})+a_{23}(a_{21}a_{32}-a_{22}a_{31})$$

$$= a_{21}a_{22}a_{33}-a_{21}a_{23}a_{32}+a_{22}a_{23}a_{31}-a_{22}a_{21}a_{33}+a_{23}a_{21}a_{32}-a_{23}a_{22}a_{31}$$

$$= 0$$

Lemma 32: Let A be an integral domain, and I an ideal of A such that $I \oplus A^n \cong A^{n+1}$, then I is principal

Proof: Fix the basis $e_0, e_1, \ldots, e_n$ of A^{n+1}, and viewing $I \oplus A^n \subseteq A \oplus A^n$, fix $f_0, f_1 \ldots, f_n$ such that f_o is a basis of A and $f_1, f_2, \ldots, f_n$ abasis of A^n. Then the map $\Psi: A^{n+1} \longrightarrow I \oplus A^n$ given by

$\Psi(e_i) = \sum_{j=o}^{n} a_{ij} f_j$ is an isomorphism.

Let d = the determinant of the matrix (a_{ij})

d_i = the $(i,0)^{th}$ cofactor of the matrix (a_{ij})

That is, $\Psi(e_o) = \sum_{j=o}^{n} a_{oj} f_i = a_{o1} f_1 + a_{o2} f_2 + \ldots + a_{on} f_n$

$$\Psi(e_1) = \sum_{j=o}^{n} a_{ij} f_i = a_{10} f_0 + a_{11} f_1 + a_{12} f_2 + \ldots + a_{1n} f_n$$

$\vdots$

$$\Psi(e_n) = \sum_{j=o}^{n} a_{nj} f_j = a_n f_o + a_{n1} f_1 + a_{n2} f_2 + \ldots + a_{nn} f_n, \quad \text{and}$$

$$(a_{ij}) = \begin{bmatrix} a_{00} & a_{01} & \ldots & a_{0n} \\ a_{10} & a_{11} & \ldots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{n0} & a_{n2} & \ldots & a_{nn} \end{bmatrix}$$

Then
$$d = \det(a_{ij}) = a_{00} \underbrace{\begin{vmatrix} a_{11} & a_{12} \ldots a_{1n} \\ a_{21} & a_{22} \ldots a_{2n} \\ \vdots & \vdots \quad \vdots \\ a_{n1} & a_{n2} \ldots a_{nn} \end{vmatrix}}_{= do} - a_{10} \underbrace{\begin{vmatrix} a_{01} & a_{02} \ldots a_{0n} \\ a_{21} & a_{22} \ldots a_{2n} \\ \vdots & \vdots \quad \vdots \\ a_{n1} & a_{n2} \ldots a_{nn} \end{vmatrix}}_{= -d1}$$

$$+ \ldots + a_{n0} \underbrace{\begin{vmatrix} a_{01} & a_{02} & a_{0n} \\ a_{11} & a_{12} & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n-11} & a_{n-12} & a_{n-1n} \end{vmatrix}}_{= dn}$$

$$= a_{00} d_0 + a_{10} d_1 + \ldots + a_{n0} d_n.$$

- Since Ψ is injective, $d \neq 0$ (otherwise if $d = 0$, then the matrix will not be invertible, so Ψ can not have an inverse and hence can not be injective.)

$$\therefore\ d = \sum_{i=o}^{n} d_i e_i \text{ and for } j \neq 0 \text{ we have } \sum_{i=o}^{n} a_{ij} d_i = 0 \text{ (by \# 5 above).}$$

Now set $e_o' = \sum_{i=o}^{n} d_i e_i$. Then $\Psi(eo') = \Psi\left[\sum_o^n d_i e_i\right] = \sum_o^n d_i\ \Psi(e_i)$

$$= \sum_o^n d_i \cdot \sum_{j=o}^{n} a_{ij} f_i$$

$$= \underbrace{\sum_o^n d_i a_{io} f_o}_{=d} + \underbrace{\sum_o^n d_i a_{i1} f_1}_{=0} + \dots + \underbrace{\sum_o^n d_i a_{in} f_n}_{=0}$$

$$= d\, f_o.$$

Moreover, since the image of Ψ includes $f_1, f_2, \dots, f_n$, there exist $e_1', \dots, e_n'$ in A^{n+1} such that $\Psi(e_j') = f_j$.

Now, define a matrix (c_{jk}) by $e_j' = \sum_{k=o}^{n} c_{jk} e_k$, for $j = 0, \dots, n$.

ie, $e_o' = c_{oo} e_o + c_{o1} e_1 + \dots + c_{on} e_n$

$e_1' = c_{1o} e_o + c_{11} e_1 + \dots + c_{1n} e_n$

$\vdots$

$e_n' = c_{no} e_o + c_{n1} e_1 + \dots + c_{nn} e_n$

$$\text{Thus, } (c_{jk}) = \begin{bmatrix} c_{oo} & c_{o1} & c_{o2} & \cdots & c_{on} \\ c_{1o} & c_{11} & c_{12} & \cdots & c_{1n} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{no} & c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix} = \begin{bmatrix} d_o & d_1 & d_2 & \cdots & d_n \\ c_{1o} & c_{11} & c_{12} & \cdots & c_{1n} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{no} & c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$$

$$(c_{jk})(a_{ij}) = \begin{bmatrix} d_o & d_1 & d_2 & \cdots & d_n \\ c_{1o} & c_{11} & c_{12} & \cdots & c_{1n} \\ \\ c_{no} & c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix} \begin{bmatrix} a_{oo} & a_{o1} & a_{o2} & \cdots & a_{on} \\ a_{1o} & a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & & \\ a_{no} & a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \sum a_{io}d_i & \sum a_{i1}d_i & \cdots & \sum a_{in}d_i \\ \sum c_{1i}a_{io} & \sum c_{1i}a_{i1} & \cdots & \sum c_{1i}a_{in} \\ \vdots & \vdots & & \\ \sum c_{ni}a_{io} & \sum c_{ni}a_{i1} & \cdots & \sum c_{ni}a_{in} \end{bmatrix}$$

Observe: 1. $\sum_{i=o}^{n} c_{ji}a_{ik} = \begin{cases} 1 \text{ for } j,k = 1,2,\ldots,n \text{ and } j = k \\ 0 \text{ otherwise} \end{cases}$

2. $d = \sum_{i=1}^{n} a_{io}d_i$ and $\sum_{i=1}^{n} a_{ij}d_i = 0$ for $j \neq 0$. (This is by # 5 above)

$$\therefore \ (c_{jk})(a_{ij}) = \begin{bmatrix} d & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Therefore, by comparing the determinants and applying number 4 above, we get $\det (c_{jk}) = 1$

- Since $\det (c_{jk}) = 1 \neq 0$, c is invertible and hence each e_i can be expressed as a linear combination e'_i.

$\therefore \ e'_o, e'_1, \ldots, e'_n$ is another basis of A^{n+1}.

Thus, If$_o$ = $\Psi(Ae'_o) = dAf_o$, which implies $I = dA$.

Hence, I is principal

Remark: Lemma 32 can be formulated as saying that for an integral domain A, a stably free rank 1 module is free.

Recall: Let A: a ring,

Let M = an A-module

1. we say that M is of <u>finite presentation</u> if there exists an exact sequence of the form.

$$A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0.$$

2. If (A, m) is a local ring, then a projective module over A is free.
3. Let $A \neq 0$. An A-module is said to be <u>free of rank n</u> if it is isomorphic to A^n

Theorem 14: Let A be a ring and M be an A-module of finite presentation. Then M is projective A-module iff M_m is a free A_m-module for all maximal ideal m of A.

Proof: (⇒) If M is projective, it is a direct summand of a free-module, and this property is preserved by localization. So that M_m is projective over A_m. By #2 above, since A_m is local we get M_m is free.

(⇐) Suppose M_m is free A_m-module

Let $N_1 \longrightarrow N_2 \longrightarrow 0$ be an exact sequence of modules

Let C = the cokernel of $\mathrm{Hom}_A(M,N_1) \longrightarrow \mathrm{Hom}_A(M,N_2)$.

Thus for any maximal ideal m of A we have

$C_m = \mathrm{coker}\ \{\mathrm{Hom}_{A_m}(M_m,(N_1)_m) \longrightarrow \mathrm{Hom}_{A_m}(M_m,(N_2)_m)\} = 0$, since M_m is free and hence projective A_m-module.

⇒ $C_m = 0$, for all maximal ideal m.

⇒ $C = 0$, because a module which is locally null at every maximal ideal is necessarly null.

∴ $\mathrm{Hom}_A(M,N_1) \longrightarrow \mathrm{Hom}_A(M,N_2)$ is exact.

Hence, M is a projective A-module.

Theorem 15: (Auslander and Buchsbuam [3]).

Every regular local ring is a unique factorization domain.

Proof: Let (A,m) be a regular local ring.

we use induction on dim A.

- If dim A = 0, then A is a field (by theorem 2) and hence a UFD.
- If dim A = 1, then A is a PID (by corollary 1) and hence a UFD.

Assume dim A > 1

- Since dim A > 1, then $\mathrm{rank}_k(m/m^2) > 1$ and $m \neq m^2$

Let $x \in m - m^2$. Then xA is a prime ideal and hence x is a prime element of A.

Now apply theorem 13 on $\Gamma = \{x\}$, and $s = \{1, x, x^2, \ldots\}$.
Here it suffices to show that A_s is a UFD.

Let P be a prime ideal of height 1 of A_s.

WTS: P is principal

put $\mathbb{P} = p \cap A$. Then $p = \mathbb{P}As$.
consider $\mathbb{P}$ as A-module, since A is noetherian, $\mathbb{P}$ is f.g. Thus, by lemma 29, $\mathbb{P}$ has a minimal resolution with each f.g and free. But since A is regular the length of the resolution must be finite, otherwise we get gl.dim A = ∞ , which is a contradiction to A is regular.

$\therefore$ $\mathbb{P}$ has an FFR

By the remark below definition 24, the A_s-module p has an FFR, say
$0 \to F_n \to F_{n-1} \to \ldots \to F_1 \to F_0 \to p \to 0.$

Now for any prime idial Q of A_s, the ring $(A_s)_Q = A_{Q\cap A}$ is a regular local ring of dimension less than that of A because

$$\dim\left(A_{Q\cap A}\right) = ht(Q\cap A) < \dim A.$$

Hence, by the induction assumption, AQ∩A is a UFD.
Now since p is a prime ideal of height 1, p_Q is also a prime ideal of height 1 of $A_{Q\cap A}$.

$\therefore$ p_Q is principal ...... by theorem 12.

$\therefore$ P_Q is a free $A_{Q\cap A}$ -module, and this is true for every maximal ideal of A_s.
Thus, by theorem 14, the A_s-module p is projective, since it is of finite presentation (ie $F_1 \to F_o \to p \to 0$ where $F_1 \cong A^n$ and $F_o \cong A^m$ for n and m ranks of F_1 and F_o respectively).

- Since A_s is noetherian, p is f.g. So we have p is a f.g projective module having an FFR.

$\therefore$ By , prop 16, p is stably free.

$\therefore$ P is stably free and has rank 1.

Thus, by Lemma 32, we have

P is a principal ideal of A_s.

$\therefore$ A_s is a UFD ..... by theorem 12.

Hence, by theorem 13, A is a UFD.

REFERENCES

1. Matsumura H. Commutative Algebra. Benjamin/Cunmings, 1980.
2. Matsumura H. Commutative ring theorey. Cambridge press, 1994.
3. Rotman, J.J. An Introduction To Homological Algebra, Academic press, 1979.
4. Northcott, D.G. Lesson On Rings, Modules and Multiplicities. Cambridge University press, 1968.
5. Northcott, D.G. Ideal Theory. Cambridge University press, 1960.
6. Nagata M. Local Rings, Interscience, 1962.
7. Zariski D. and Samuel P. Commutative Algebra, vol. II. Van Nostrand, 1958.
8. Hohn F.E. Introduction to Linear Algebra, Macmillan, 1972.