POLYNOMIAL RINGS
AND
POWER SERIES RINGS.

Sima Jajodia
DEPARTMENT OF MATHEMATICS
NORTH - EASTERN HILL UNIVERSITY

Submitted in partial fulfilment of the requirement
of the Degree of Master of Philosophy

To

NORTH - EASTERN HILL UNIVERSITY
SHILLONG
APRIL 1992.

CERTIFICATE.

I certify that the dissertation entitled "Polynomial rings and power series rings " submitted by Ms Sima Jajodia in partial fulfilment of the requirements for the degree of Master of Philosophy is the outcome of a study undertaken by the candidate.

I certify that the sources from which ideas have been borrowed have been duly referred to.

The material in this dissertation has not been presented for the award of a degree in any university before.

This dissertation may be placed before examiners for evaluation and necessary formalities. I certify that this dissertation is worthy of consideration by the examiners.

Mangesh B. Rege

Mangesh B. Rege
Supervisor
Mathematics Department
North-Eastern Hill University
SHILLONG.

Shillong,
April 30 , 1992.

ACKNOWLEDGEMENT.

This work was carried out under the supervision of Dr. Mangesh. B. Rege. I would like to take this oppurtunity to express my deep sense of gratitude to him for his unfailing help and kind cooperation during the course work period and in the preparation of this thesis.

Thanks are also due to Dr. P. Saikia and Dr. S. S. Khare for the effort made by them to give us courses as per the M.Phil programme

The typing of this manuscript was a joint effort by my research colleagues and me. Special thanks are due to Mr. Basil S. Koikara for showing me how to operate the word processor and initiating the process and Ms. Debadatta Bhattacharjee for helping me follow it up. Our research scholar and computer expert Mr. Bipul S. Purkayastha was very generous with computer time, even sometimes to the detriment of his own work. Thanks are due to him and the head of the department of Mathematics for providing all the necessary facilities.

I am grateful to my senior colleagues Ms. M. Ibemhal Devi, Mrs. S. Dutta and Mrs. I Dutta for helping me in every possible way. My co-M.phil students Ms. Amita Mitra and Ms. D. Bhattacharjee were also very cooperative during the entire period.

I would also like to thank all the staff and teachers of the department of Mathematics for their kind cooperation.

Lastly I wish to express my heartfelt thanks to all my family members for always being a source of inspiration to me.

Sima Jajodia

Ms. Sima Jajodia

PREFACE.

Polynomial and power series rings were classical objects of study. These concepts have been generalised to polynomial and power series modules. It is impossible to study even a substantial portion of the work carried out in this field. In this dissertation a very small portion has been studied and a few specimen results have been recorded in each chapter.

Chapters 1, 2, 3 are almost independent of each other. Chapter 0 is basically aimed at introducing terms and notations which are used in later chapters. Those terms which are of standard usage have been used without prior introduction. Chapter 1 studies the conditions under which Hilbert Basis Theorem has a generalisation to polynomial and power series modules over rings not necessarily containing identity element. Knowledge of Noetherian modules is assumed.

Many a time it has been observed that on imposing certain conditions on a ring, various properties of the ring so obtained carry over to the respective polynomial, and to some extent, power series rings. These properties like Baer rings, P.P. rings, P.S. rings and regular rings have been the subject of study in chapter 2. (These concepts have been defined in chapters 0 and 2.). In this chapter, our rings are associative but usually non-commutative.

Zero-divisors and nilpotent elements of polynomial and power series rings turn out to be of considerable interest. Although the final chapter has been entitled "Polynomial and Power Series

Rings Over Commutative Rings ", only the above- mentioned aspects of these rings have been studied in some detail.

No originality is claimed for any of the material (except for a few remarks which we did not find recorded in the literature). This work is a survey of some research done by the following algebraists: K. Varadarajan, W. Xue, E. Armendariz, M.W. Evans, S. Endo, P. Pillay, W.K. Nicholson, J.F. Watters, W.R. Scott, D.E. Fields, R. Gilmer, E. Snapper and others. Detailed mention of the debt is made at the end of each chapter.

The Bibliography has been divided into two parts: (I) Books and Monographs and (II) Research papers. A book may be cited as [X II] os as [XYZ]; here [X] or [XYZ] will denote the initial letter(s) of the names of the author(s). A memoir may be cited eg.,as [XYZ:53]; Here 53 gives the year in which the paper was published. This will give an approximate idea of when the research was carried out.

CONTENTS.

CHAPTER 0

SOME PRELIMINARY DEFINITIONS AND NOTATIONS.

Introduction.

This chapter is more or less an introduction to the dissertation. It consists of notations, definitions and conventions which will be followed consistently (unless mentioned otherwise) in the rest of the dissertation. Some definitions which are of a general nature are also given here. This chapter also helps to set a link between the other chapters of the dissertation. For unexplained concepts, we refer to standard books, e.g., [AF], [L], [S], [JI] and others.

§ 0.1 Some conventions and notations.

In this section we fix some conventions and notations. We shall try to adhere to these throughout the dissertation. Note that all our left-sided concepts and results have right-sided counterparts.

0.1.1 *Convention.* Unless mentioned otherwise, by a ring we shall mean an associative ring with an identity element. The letter R will always denote a ring. In Chapter 1 rings will be associative but they need not have identity element.

0.1.2 *Notation.* By a module ${}_RM$, we mean a left R-module and by a module M_R we mean a right R-module.

0.1.3 *Convention.* An ideal will mean a two-sided ideal. A left or right ideal will be specifically mentioned.

§ 0.2 Basic Definitions.

The definitions to be used in this dissertation are given below.

0.2.1 *Definition.* By a domain we mean a (possibly non-commutative) ring in which the product of non-zero elements is non-zero.

0.2.2 *Definition.* A ring R is called a prime ring if for ideals A, B the equality AB = O implies A = O or B = O. (Clearly, domains are prime rings.)

0.2.3 *Definition.* An ideal P of R is a prime ideal if R/P is a prime ring. (Note that in the commutative case, generally R is not regarded as a prime ideal.) An ideal P is prime if and only if whenever $x, y \in R$, $xRy \subseteq P \Rightarrow x \in P$ or $y \in P$. The prime radical or the lower nil radical (denoted by Nil(R)) of a ring R is the intersection of all prime ideals of R. A ring R is semi-prime in case Nil(R) is zero; equivalently if it has no non-zero nilpotent ideals. The Jacobson radical of R denoted by J(R) is the intersection of all maximal left ideals of R. (See Exer. 15.14 of [AF]for more information concerning these concepts.)

0.2.4 *Definition.* Let L be a submodule of a module M. Then L is called a large (essential) submodule of M if for every non-zero submodule N of M, we have $L \cap N$ is non-zero. By a large left ideal of R we mean a large submodule of ${}_R R$.

0.2.5 *Notation.* Let ${}_R M$ be a module. We shall use the notation

$$Z(M) = \left\{ m \in M \mid Lm = 0 \text{ for some large left ideal of } R \right\}$$

It can be verified that Z(M) is a submodule of M.

0.2.6 *Definition.* We call Z(M) the singular submodule of M. If Z(M) = 0, M is called a non-singular module. If Z(M) = M, M is called a singular module. We call a ring R a left nonsingular ring if $Z({}_R R)$ equals zero.

0.2.7 *Definition.* A ring R is said to be reduced if it has no non-zero nilpotent elements. Note that reduced $\Rightarrow$ semiprime. If R is commutative then reduced $\Leftrightarrow$ semiprime.

0.2.8 Annihilators. We shall denote the left annihilator of a subset X of a module ${}_R M$ by l(X), and the right annihilator of a subset X of a module M_R by r(X). If X = {m} where $m \in M$ we shall write $l(m)$ instead of $l(\{m\})$ and $r(m)$ instead of $r(\{m\})$. The special case when $M = R$ will also occur very often.

Let R be a reduced ring, and $a, b \in R$ are such that $ab = 0$. Then $ba = 0$, for $ab = 0 \Rightarrow bab = 0 \Rightarrow baba = 0 \Rightarrow ba = 0$. Thus in these rings left and right annihilators will be the same, either for an element or for a subset and so we can talk of the annihilator without ambiguity. We shall try to use the notations Ann(S) (for the annihilator of a subset S of R) and Ann(a) whenever we have the equality ofleft and right annihilators. (In addition to subsets of reduced rings this will happen for each central subset of a ring; in particular, for each subset of a commutative ring R.)

0.2.9 *Definition.* A ring R is said to be normal (abelian) if every idempotent is central. (It is easy to see that reduced rings are normal.)

0.2.10 *Definition.* A ring R is called semi-simple if every left ideal of R is a direct summand of ${}_RR$. A ring R is called indecomposable, if it cannot be expressed as $R_1 \times R_2$ where R_1, R_2 are non-zero rings.

0.2.11 *Definition.* A ring R is called left duo (invariant) if every left ideal is an ideal. (Commutative rings are left and right duo and left (or right) duo rings are normal.)

0.2.12 *Definition.* A ring is said to be (von Neumann) regular if for every element $a \in R$, there exists an element $b \in R$ such that the relation $a = aba$ holds.

0.2.13 Basic results on regular rings.

(I) Let R be a ring. The following conditions are equivalent.

(i) R is (von Neumann) regular.

(ii) Every left ideal of R is generated by an idempotent (equivalently, is a direct summand).

(iii) Every finitely generated left ideal is generated by an idempotent (equivalently, is a direct summand).

(II) Division rings are clearly regular.

(III) Let $\{ R_i \}_{i \in I}$ be a family of rings. Then $\prod_{i \in I} R_i$ is regular if and only if each R_i is regular. Hence it follows from (II) that if D_i are division rings then $\prod_{i \in I} D_i$ is a regular ring.

(IV) Let M_R be a semi-simple module. Then its endomorphism ring $\mathrm{End}_R(M)$ is a regular ring.

(V) We have, more generally, $\mathrm{End}_R(M)$ is regular if and only if for each $f \in \mathrm{End}_R(M)$, the submodules $\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$ are direct summands of M.

(VI) If R is a semi-simple ring then it is regular.

(VII) Let V_D be a vector space over a division ring D. Then $End_D(V)$ is a regular ring. (This follows from (IV) above.)

(VIII) As a special case of (V) or (VI) we have: If D is a division ring then $M_n(D)$ is regular for all n.

(IX) If R is a commutative regular ring, then R is necessarily reduced. (This is not true if R is not commutative. Consider the ring $R = M_n(K)$, K a field, $n \geq 2$. This is not reduced (see (VIII) above).)

(X) For a detailed survey of (almost) everything known about regular rings till 1980 see [GII].

§0.3 A basic result.

0.3.1 PROPOSITION. Let R be a commutative ring. Then R is non-singular if and only if R is reduced.

Proof: This proposition can be restated in two parts.

PART I R reduced implies R left and right non-singular.

PART II R commutative implies R reduced.

Proof of part I. Let $x \in Z({}_R R)$. Then $Lx = 0$ for some large left ideal L of R $\rightarrow$ $x \in Ann(L)$.

Let $y \in L \cap Rx$. Then $y = rx$ for some $r \in R$.

Also $Lx = 0$ $\rightarrow$ $yx = 0$ $\rightarrow$ $rx.x = 0$ $\rightarrow$ $x.rx = 0$ (since R is reduced) $\rightarrow$ $xr.x = 0$ $\rightarrow$ $xr.xr = 0$ $\rightarrow$ $xr = 0$ $\rightarrow$ $y = 0$

$\rightarrow$ $L \cap Rx = 0$ $\rightarrow$ $Rx = 0$ $\rightarrow$ $x = 0$.

Proof of part II. Let R be commutative non-singular. Let $x \in R$ be such that $x^2 = 0$. This implies that $x \in \mathrm{Ann}(x)$.

Claim. $\mathrm{Ann}(x)$ is a large left ideal of R.

Let $0 \neq y \in R$. Consider $Ry \cap \mathrm{Ann}(x)$. Now $x^2 = 0 \Rightarrow x^2y = 0 \Rightarrow x.xy = 0 \Rightarrow xy \in \mathrm{Ann}(x)$. Also $xy \in Ry$.

Case I Suppose $xy \neq 0$. Then $xy \in Ry \cap \mathrm{Ann}(x)$ (as seen above) showing that $Ry \cap \mathrm{Ann}(x) \neq 0$.

Case II If $xy = 0$, then $y \in Ry \cap \mathrm{Ann}(x)$, again showing that $Ry \cap \mathrm{Ann}(x) \neq 0$.

Also since y was an arbitraily chosen element of R, the claim is established.

Now $\mathrm{Ann}(x).x = 0 \Rightarrow x \in Z({}_RR) = 0$ showing that R is reduced. ∎

0.3.2 <u>EXAMPLE</u>. Let $n \geq 2$ and K a field. Then $R = M_n(K)$ is left and right non-singular but not reduced. This shows that Part II of 0.3.1 is not valid for non-commutative rings.

———————— * ————————

CHAPTER I
POLYNOMIAL MODULES AND POWER SERIES MODULES.

Introduction

In this chapter we shall make a brief study on Polynomial and power series modules, over rings which need not contain identity element. A generalisation of Hilbert Basis Theorem due to K.Varadarajan is the main aim of this chapter.

§ 1.1 Basic concepts.

Let R be a ring not necessarily possessing an identity element. An R-module M is, unless otherwise mentioned, considered to be a left R-module. Also, concepts will be left sided concepts unless mentioned otherwise.

Let x be an indeterminate over R. Then R[x] is the usual polynomial ring over R, R[[x]], the power series ring and $R[x,x^{-1}]$ is the ring of Laurent polynomials consisting of elements of the type $\sum_{i=-n}^{m} \alpha_i x^i$, $n,m \in \mathbb{N} \cup \{0\}$ and $\alpha_i \in R$, $\forall$ i. We now have the following definitions.

1.1.1 *Definition* : The Module of Polynomials $_{R[x]}M[x]$.

The elements of M[x] are formal sums of the form $\sum_{i=0}^{k} a_i x^i$, $k \geq 0$, $k \in \mathbb{N} \cup \{0\}$ and $a_i \in M$. Addition is defined by adding the corresponding coefficients. Next let $\sum_{i=0}^{k} \alpha_i x^i \in R[x]$ and $\sum_{j=0}^{l} a_j x^j \in M[x]$.

Then, $\left(\sum_{i=0}^{k}\alpha_i x^i\right)\left(\sum_{j=0}^{l} a_j x^j\right) = \sum_{\mu=0}^{k+l} c_\mu x^\mu$ 1.1.2

where $c_\mu = \sum_{i+j=\mu} \alpha_i a_j$ for each μ.

The right hand side of 1.1.2 is clearly an element of $M[x]$ as M is a left R-module. This gives a left $R[x]$-module structure on $M[x]$. Any non-zero element $\alpha \in M[x]$ can be written uniquely as $\sum_{i=0}^{l} a_i x^i$ with $l \geq k \geq 0$, $a_i \in M$ and $a_k \neq 0$, $a_l \neq 0$. The integer k is now referred to as the order of α, l its degree, a_k the initial coefficient and a_l as the leading coefficient. Is it clear?

1.1.3 *Definition:* The Power Series Module $M[[x]]$

The elements of $M[[x]]$ are formal power series $\sum_{i\geq 0} a_i x^i$ with $a_i \in M \ \forall\ i$. Addition is defined as usual by adding the coefficients of corresponding powers of x. For the $R[[x]]$-module structure to be defined on $M[[x]]$, consider

$\sum_{i\geq 0} \lambda_i x^i \in R[[x]]$ and $\sum_{j\geq 0} a_j x^j \in M[[x]]$, and define

$$\left(\sum_{i\geq 0} \lambda_i x^i\right)\left(\sum_{j\geq 0} a_j x^j\right) = \sum_{\mu\geq 0} c_\mu x^\mu \quad \text{............ 1.1.4}$$

where $c_\mu = \sum_{i+j=\mu} \lambda_i a_j$ for any $\lambda_i \in R$, $a_j \in M$. As in definition 1.1.1 RHS of 1.1.4 is an element of $M[[x]]$ since M is an R-module, which makes $M[[x]]$ into an $R[[x]]$ module.

Any non-zero element α of $M[[x]]$ can be written uniquely as $\sum_{i\geq k} a_i x^i$ with $a_i \in M$, $k \geq 0$ and $k \neq 0$. In this case k is called the order of α and a_k, the initial coefficient of α.

1.1.5 *Definition* : The module of Laurent polynomials $M[x, x^{-1}]$.

The elements of $M[x, x^{-1}]$ are formal sums of the form $\sum_{i=-\gamma}^{k} a_i x^i$ with $k,\gamma \in \mathbb{Z}$, $k,\gamma \geq 0$ and $a_i \in M$.

Addition is as usual defined by adding the coefficients of corresponding powers of x. The action of the ring $R[x, x^{-1}]$ is as in the above two definitions an obvious one making $M[x, x^{-1}]$ an $R[x, x^{-1}]$-module.

Any non-zero element α of $M[x, x^{-1}]$ can be written uniquely in the form $\sum_{i=-k}^{l} a_i x^i$, with $l \geq k$, $l,k \in \mathbb{Z}$ and $a_k \neq 0$, $a_l \neq 0$. In this case we refer to k as the order of α, l as its degree; a_k is the initial coefficient and a_l is the leading coefficient.

1.1.6. Let n be any integer ≥ 1 and

$I_n = \{0\} \cup \{\alpha / 0 \neq \alpha \in R[x]$, order of $\alpha \geq n\}$. We claim that I_n is a two sided ideal of $R[x]$.

For $\alpha,\beta \in I_n$, $\alpha \neq 0$, $\beta \neq 0$, order $\boxed{\alpha \geq n,\ \beta \geq n,}$ order $\beta \geq n$? no need of this ?

? $\Rightarrow \alpha-\beta \neq 0$ and order $(\alpha-\beta) \geq n$. So $\alpha-\beta \in I_n$. why $\alpha-\beta \neq 0$?

Let $f(x) \in R[x]$ and $\alpha \in I_n$. Clearly $f(x)\alpha \in I_n$ and $\alpha f(x) \in I_n$. The quotient ring $R[x]/I_n$ will be called the truncated polynomial ring, truncated at degree $n \geq 1$.

If R has identity then $I_n = (x^n)$. Even if R does not have identity element, we will symbolically denote $R[x]/I_n$ by $R[x]/(x^n)$

An element of $R[x]/(x^n)$ can be uniquely written as $\sum_{i=0}^{n-1} \lambda_i x^i$, $\lambda_i \in R$.

Let $D_n = \{0\} \cup \{\alpha \mid 0 \neq \alpha \in M[x]$, order of $\alpha \geq n\}$.

Then D_n is an $R[x]$-submodule of $M[x]$. Since $I_n M[x] \subseteq D_n$, $R[x]/(x^n)$

acts on $M[x]/D_n$. We denote the module $M[x]/D_n$ by $M[x]/(x^n)$. The action of $R[x]/(x^n)$ on $M[x]/(x^n)$ is given by

$$\left(\sum_{i=0}^{n-1} \lambda_i x^i\right)\left(\sum_{j=0}^{n-1} a_j x^j\right) = \sum_{i=0}^{n-1} c_\mu x^\mu \text{ , where } c_\mu = \sum_{i+j=\mu} \lambda_i a_j \text{ ; } \lambda_i \in R,$$

$a_j \in M$. Any non-zero element α can be written uniquely in the form $\sum_{i=k}^{n-1} a_i x^i$ with $a_i \in M$, $a_k \neq 0$, $0 \leq k \leq n-1$. In this case k is called the order of α and a_k the initial coefficient of α.

§ 1.2 The R-module $L_i(A)$.

1.2.1 Let M be any R-module. Let A be an R[x]-submodule of M[x]. Let $i \geq 0$ be an integer. Define

$L_i(A)$ = {0} ∪ {leading coefficients of elements of degree i in A}

$L_i(A)$ is an R-submodule of A (clearly).

If R has an identity element and M is unitary, we have $L_i(A) \subseteq L_{i+1}(A)$, since $(1.x)A \subseteq A$. The inclusion does not hold on general. Consider the following example.

1.2.2 EXAMPLE. Let R be any ring and M any non-zero abelian group. Define R-action on M by $r.m = 0$ for any $r \in R$ and $m \in M$.

Let N be a subgroup of M with $N \subsetneqq M$ (e.g. N = 0). The induced action of R[x] on M[x] is $f(x).\alpha = 0$ for any $f(x) \in R[x]$ and $\alpha \in M[x]$. So the R[x]-submodules are the same ae the additive subgroups of M[x].

Let q be any integer ≥ 0 and let

$A = \left\{\alpha \in M[x] \mid \text{the coefficient of } x^{q+1} \text{ in } \alpha \text{ is an element of } N\right\}$

Then A is an $R[x]$-submodule of $M[x]$. Now

$L_q(A) = \{0\} \cup \{$leading coefficients of elements of degree q in $A\}$
$\subseteq M$.

Let $m \in M$. If $m = 0$ then $m \in L_q(A)$. Suppose $m \neq 0$. Consider $mx^q = g(x)$ say. Then $g(x) \in A$ (since the coefficient of x^{q+1} equals 0 and $0 \in N$). This imples that $m \in L_q(A)$. Thus we have $M \subseteq L_q(A)$. Therefore $L_q(A) = M$. Also

$L_{q+1}(A) = \{0\} \cup \{$leading coefficient of elements of degree $q+1$ in $A\}$
$= N$ (clearly).

Since $N \subsetneq M$, we have that $L_q(A) \nsubseteq L_{q+1}(A)$.

1.2.3 LEMMA. Let $A \subseteq B$ be $R[x]$-submodules of $M[x]$ satisfying $L_i(A) = L_i(B)$ $\forall\ i \geq 0$. Then $A = B$.

Proof: Let $\beta \in B$. If $\beta = 0$ then $\beta \in A$.
Suppose $\beta \neq 0$. Let $\deg \beta = k$, $\beta = b_0 + b_1x + \ldots + b_kx^k$, with $b_k \neq 0$ and all $b_i \in M$. Since $\beta \in B$, $b_k \in L_k(B) = L_k(A)$. This implies that $\exists\ \alpha_k \in A$ such that $\deg \alpha_k = k$ and the leading coefficient of $\alpha_k = b_k$. Therefore $\beta-\alpha_k \in B$ (since $\beta \in B$, $\alpha_k \in B$) and $\deg(\beta-\alpha_k) \leq k-1$. If $\deg(\beta-\alpha_k) < k-1$ define $\alpha_{k-1} = 0 \in A$. If $\deg(\beta-\alpha_k) = k-1$ using the equality $L_{k-1}(A) = L_{k-1}(B)$ and arguing as above we obtain $\alpha_{k-1} \in A$ with $\deg(\beta-\alpha_k-\alpha_{k-1}) \leq k-2$. Proceeding in this way we get elements $\alpha_j \in A$ for $k \geq j \geq 0$ such that $\deg\left[\beta - \sum_{i=0}^{r} \alpha_{k-i}\right] \leq k-r-1$ $\forall\ r = 1,2,\ldots,k-1$.

So $\deg\left[\beta - \sum_{i=0}^{k} \alpha_{k-i}\right] \leq k-k-1 \Rightarrow \beta - \sum_{i=0}^{k} \alpha_{k-i} = 0$
$\Rightarrow \beta = \alpha_k + \alpha_{k-1} + \ldots + \alpha_0 \in A$
$\Rightarrow B \subseteq A$. Therefore $A = B$.

M Following the induction on n is possibly the beautiful way.

1.2.4 For any $R[x]/(x^n)$-submodule A of $M[x]/(x^n)$ and $i \in \{0,1,2,\ldots,n-1\}$ <u>define</u> $\Gamma_i(A)$ as follows.

$\Gamma_i(A) = \{0\} \cup \{$initial coefficients of elements of order i in $A\}$

As before, if R has identity and M is unitary we have $\Gamma_i(A) \subseteq \Gamma_{i+1}(A)$, for $0 \le i \le n-2$; this is not true if R does not have an identity element.

1.2.5 <u>Lemma</u>: Let $C \subseteq D$ be $R[x]/(x^n)$-submodules of $M[x]/(x^n)$ satisfying $\Gamma_i(C) = \Gamma_i(D)$ for $0 \le i \le n-1$. Then $C = D$.

Proof: Let $d \in D$. If $d = 0$ then $d \in C$ (clearly).

Suppose $d \neq 0$ and order $d = k$; $0 \le k \le n-1$.

So d is of the type $\sum_{i=k}^{n-1} d_i x^i$, $d_i \in M$, $d_k \neq 0$.

Since $d \in D$, $d_k \in \Gamma_k(D) = \Gamma_k(C)$.

So there exists $c_k \in C$ such that order $c_k = k$ and the initial coefficient of $c_k = d_k$. Thus $d - c_k \in D$, and order $(d-c_k) \ge k+1$.

If order $(d-c_k) > k+1$, write $c_{k+1} = 0 \in C$.

If order $(d-c_k) = k+1$, then using the equality $\Gamma_{k+1}(D) = \Gamma_{k+1}(C)$ and arguing as above, we get $c_{k+1} \in C$ with order $(d - c_k - c_{k+1}) \ge k+2$.

Proceeding in this way we get an element c_j of C for $k \ge j \ge 0$ such that the order $\left(d - \sum_{i=0}^{r} c_{k+i}\right) \ge k+r+1$.

Now the only element of $M[x]/(x^n)$ of order $> n-1$ is the zero element. It follows that $\left(d - \sum_{i=0}^{n-k-1} c_{k+i}\right) = 0$.

Thus $d = c_k + c_{k+1} + \ldots + c_n \in C$.

This proves that $D \subseteq C$.

§ 1.3 Modules with property(F).

Let M be an R-module and N a submodule of M. Then $\{x \mid x \in M, Rx \subseteq N\}$ is clearly a submodule of M containing M. This is dependent on M as well as on N. When M becomes clear from the context we write

$$R^{-1}N = \{x \mid x \in M, Rx \subseteq N\}.$$

This is comparable to the situation when R is a ring and A,B ideals of R; then the usual definition of (A:B) is given by

$$(A:B) = \{x \in R \mid xB \subseteq A\}.$$

The above definition however should certainly not be confused with $S^{-1}R = \{a/b \mid a \in R, b \in S\}$, S an m.c set of a commutative ring R.

1.3.1 *Definition.* We say that the R-module M has property (F) if $R^{-1}N = N$ for all submodules N of M.

1.3.2 LEMMA: An R-module M has property (F) $\Longleftrightarrow$ for every factor module M" of M and every $x" \neq 0$ in M" we have $Rx" \neq 0$.

Proof: Let M" be a factor module of M and $0 \neq x" \in M"$. Write M" as M/N and $x" = x + N$, $x \in M$; $x \notin N$. Since M has property (F), $R^{-1}N = N$. Since $x \notin N$, $Rx \subseteq N \Rightarrow Rx" \neq 0$ in M/N. ? For $R^{-1}N = N$, $x \notin N \Rightarrow x \notin R^{-1}N \Rightarrow Rx \nsubseteq N \Rightarrow Rx" \neq 0$ in M/N

Conversely, assume that for any $0 \neq x" \in M"$, (where M" is a factor module of M). We have $Rx" \neq 0$. Let N be any submodule of M. If N = M, then clearly $R^{-1}N = N$. If $N \neq M$ for any $x \in M$ which is not in N, we have $x + N \neq 0$ in M/N. Hence $R(x + N) \neq 0$ in M/N. This implies that $Rx \subseteq N \Rightarrow x \notin R^{-1}N$. Thus $R^{-1}N \subseteq N$. We already have $N \subseteq R^{-1}N$. Therefore $N = R^{-1}N$. ∎

$R(x+N) \neq 0$
$\Rightarrow Rx \nsubseteq N$

1.3.3 <u>COROLLARY</u>. Let M possess property(F). Then

(i) every factor module of M has property(F).

and (ii) every submodule of M has property(F).

Proof: (i) Let $\bar{M}$ be a factor module of M, and M" a factor module of $\bar{M}$. Then M" is a factor module of M.

Then by Lemma 1.3.2, $\forall\ x'' \neq 0,\ x'' \in M''$, we have $Rx'' \neq 0$.

Hence $\bar{M}$ has property(F).

(ii) Follows from definition.

Given any ring homomorphism $f: R \longrightarrow S$ and an S-module M, we can regard M as an R-module using f, namely, $\lambda.x = f(\lambda).x$, for any $\lambda \in R$.

1.3.4 <u>LEMMA</u>. Let $f : R \longrightarrow S$ be an onto homomorphism of rings. Then an S-module M has property(F) iff it has property(F) as an R-module.

Proof: By hypothesis, the S-submodules of M are the same as the R-submodules of M. Also for any $x \in M$, and any $r \in R$, $r.x = f(r).x$. i.e., $Rx = Sx \quad \forall\ x \in M$.

In particular, for any submodule N of M, we have $S^{-1}N = R^{-1}N$.

1.3.5 <u>PROPOSITION</u>.

The following conditions on an R-module M are equivalent.

(1) M has property(F) as an R-module.

(2) M[x] has property(F) as an R[x]-module.

(3) $M[x]/(x^n)$ has property(F) as an $R[x]/(x^n)$-module for any $n \geq 1$.

(4) $M[x,x^{-1}]$ has property(F) as an $R[x,x^{-1}]$-module.

Proof: ((1)$\Rightarrow$(2)) Let A be an $R[x]$-submodule of $M[x]$. Let $\alpha \in M[x]$ satisfy $R[x]\alpha \subseteq A$. We have to show $\alpha \in A$. If $\alpha = 0$ then there is nothing to prove. Suppose $\alpha \neq 0$. Proof is by induction on deg α.
If deg $\alpha = 0$, then $\alpha = a_0 \neq 0$, $a_0 \in M$.
Since M has property(F), $a_0 \in L_0(A)$. Hence $a_0 \in A$.
Now let deg $\alpha = k > 0$. Then $\alpha = a_0 + a_1 + \ldots + a_k x^k$, with $a_i \in M$ and $a_k \neq 0$. Since $R[x]\alpha \subseteq A$, we get $R\alpha \subseteq A \Rightarrow R.a_k \subseteq L(A)$.
Since M has property(F), $a_k \in L_k(A)$. Hence there exists an $\alpha_k \in A$ with deg $\alpha_k = k$ and leading coefficient of $\alpha_k = a_k$.
Then deg $\alpha \leq k-1$ and $R[x](\alpha-\alpha_k) \subseteq A$. Hence by induction assumption $\alpha-\alpha_k \in A$. Since $\alpha_k \in A$, it follows that $\alpha \in A$.

((2)$\Rightarrow$(3)) The canonical map $\eta : R[x] \longrightarrow R[x]/(x^n)$ is a homomorphism and so the $R[x]/(x^n)$-module $M[x]/(x^n)$ could be regarded as an $R[x]$-module. Clearly this module is a factor module of $M[x]$. By Corollary 1.3.3 and Lemma 1.3.4 we get the implication ((2)$\Rightarrow$(3)).

((2)$\Rightarrow$(4)) We already have the implication ((1)$\Rightarrow$(2)). Using that from (2) we get that $M[x,y]$ as an $R[x,y]$-module has property(F), where x,y are two independent indeterminates. Using the quotient map $\eta : R[x,y] \longrightarrow R[x,x^{-1}]$, the module $M[x,x^{-1}]$ can be regarded as an $R[x,y]$-module. Clearly $M[x,x^{-1}]$ as an $R[x,y]$-module is a quotient module of $M[x,y]$. Now the implication is immediate from Corollary 1.3.3(1) and Lemma 1.3.4.

((3)$\Rightarrow$(1)). Let M'' be a factor module of M and $0 \neq x'' \in M''$.

Clearly $M''[x]/(x^n)$ is a factor module of the $R[x]/(x^n)$-module $M[x]/(x^n)$. Hence $R[x]/(x^n).x'' \neq 0$ in $M''[x]/(x^n)$. So there exists a $\beta \in R[x]/(x^n)$ with $\beta x'' \neq 0$. If $\beta = \sum_{\iota=k}^{n-1} \lambda_\iota x^\iota$ $(k \geq 0)$ with $\lambda_\iota \in R$ then $\lambda_\iota . x'' \neq 0$ for some ι. Hence $Rx'' \neq 0$.

((4)$\Rightarrow$(1)). Let M'' be a factor module of M and $0 \neq x'' \in M''$. Clearly $M''[x,x^{-1}]$ is a factor module of the $R[x,x^{-1}]$-module $M[x,x^{-1}]$. Hence $R[x,x^{-1}].x'' \neq 0$ in $M''[x,x^{-1}]$. So $\exists$ a $\beta \in R[x.x^{-1}]$ with $\beta x'' \neq 0$. If $\beta = \sum_{\iota=k}^{l} \lambda_\iota x^\iota$, $\lambda_\iota \in R$ we have $\lambda_\iota x'' \neq 0$ for some ι. Hence $Rx'' \neq 0$.

Thus we have proved the equivalence of the above four statements.∎

§ 1.4 A theorem of Varadarajan.

Varadarajan's generalisation of Hilbert basis theorem is the following result.

1.4.1 THEOREM. The following are equivalent for an R-module M.

(a) M is Noetherian as an R-module and has property(F).

(b) $M[x]$ is Noetherian as an $R[x]$-module.

(c) $M[x,x^{-1}]$ is Noetherian as an $R[x,x^{-1}]$-module.

(d) $M[[x]]$ is Noetherian as an $R[[x]]$-module.

Proof: ((b)$\Rightarrow$(a), (c)$\Rightarrow$(a), (d)$\Rightarrow$(a)).

Suppose M is a non-Noetherian R-module. Let $N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq \cdots$ be an infinite ascending chain of R-submodules of M. Then clearly $N_1[x] \subsetneqq N_2[x] \subsetneqq N_3[x] \subsetneqq \cdots$ is an infinite ascending chain of $R[x]$-

submodules of $M[x]$. Thus $M[x]$ is non-Noetherian as an $R[x]$-module. Similiarly $M[x,x^{-1}]$ is non-Noetherian as an $R[x,x^{-1}]$-module and $M[[x]]$ is non-Noetherian as an $R[[x]]$ module.

Suppose M does not have property(F). Then there is a factor module M'' of M and an element $0 \neq x'' \in M''$, with $Rx'' = 0$. If N'' is the R-submodule of M'' generated by x'' then $N'' \neq 0$ and $RN'' = 0$. $N''[x]$ is a non-zero $R[x]$-submodule of $M''[x]$. From $RN'' = 0$ we see that $f(x).\alpha = 0$ for any $f(x) \in R[x]$ and $\alpha \in N''[x]$. Hence the $R[x]$-submodules of $N''[x]$ are the same as additive subgroups of $N''[x]$. Clearly $N''[x]$ is an infinite direct sum of nonzero abelian groups. Hence, $N''[x]$ is non-Noetherian as an $R[x]$-module. Since $N''[x]$ is an $R[x]$-submodule of $M''[x]$ and $M''[x]$ is a factor module of $M[x]$, it follows that $M[x]$ is non-Noetherian as an $R[x]$-module. Similarly it can be shown that if M does not have property(F) then $M[x,x^{-1}]$ cannot be Noetherian as an $R[x,x^{-1}]$-module and $M[[x]]$ cannot be Noetherian as an $R[[x]]$-module. This proves the implications (b) $\Rightarrow$ (a), (c) $\Rightarrow$ (a) and (d) $\Rightarrow$ (a)

((a)$\Rightarrow$(b)). Let A be any $R[x]$-submodule of $M[x]$. For each integer $i \geq 0$, let $L_i(A)$ be defined as in § 2. Let $a \in L_i(A)$. Then $\exists$ an element $\alpha = a_0 + a_1x + \ldots + a_ix^i \in A$ with $a_i = a$. For any $r \in R$ we have $rx.\alpha = ra_0x + ra_1x^2 + \ldots + ra_ix^{i+1} \in A$. This implies that $ra \in L_{i+1}(A)$. Thus, $RL_i(A) \subseteq L_{i+1}(A)$, or equivalently $L_i(A) \subseteq R^{-1}L_{i+1}(A)$ (as submodules of M). Since M has property(F), $R^{-1}L_{i+1}(A) = L_{i+1}(A)$. Therefore $L_i(A) \subseteq L_{i+1}(A)$.

Suppose $A_0 \subseteq A_1 \subseteq \ldots$ is an ascending sequence of $R[x]$-submodules of $M[x]$. Consider the family $\{L_i(A_j)\}$ $i \geq 0$, $j \geq 0$

of submodules of M. We already have,

$L_i(A_j) \subseteq L_{i+1}(A_j) \quad \forall\, i \geq 0.$

Also, $A_j \subseteq A_{j+1} \Rightarrow L_i(A_j) \subseteq L_i(A_{j+1})$. Since M is Noetherian the family $\{L_i(A_j)\}$, $j \geq 0$, $i \geq 0$, has a maximal element say $L_{i_0}(A_{j_0})$. Hence, $L_i(A_j) = L_{i_0}(A_{j_0})$ whenever $i \geq i_0$, $j \geq j_0$. For any fixed $i < i_0$, because M is Noetherian, we can find an integer $n(i)$ with $L_i(A_j) = L_i(A_{n(i)})$ for $j \geq n(i)$.

Let $q = \mathrm{Max}\{\, n(0), n(1), \ldots, n(i_0-1), j_0 \}$

Then $L_i(A_j) = L_i(A_q)$ for $j \geq q$ and $i \geq 0$. From Lemma 1.2.4, it follows that $A_j = A_q$ for $j \geq q$ which shows that $M[x]$ is Noetherian as an $R[x]$-module.

((a) $\Rightarrow$ (c)). From Proposition 1.3.5, we know that if M has property(F), then $M[x]$ also has property(F) as an $R[x]$-module. Now from ((a)$\Rightarrow$(b)) which has been proved, we see that $M[x]$ is Noetherian as an $R[x]$-module.

$M[x,x^{-1}]$ can be regarded as an $R[x,y]$-module via the quotient map $R[x,y] \longrightarrow R[x,x^{-1}]$. Also as an $R[x,y]$-module, $M[x,x^{-1}]$ is a factor module of $M[x,y]$. Since $M[x]$ is Noetherian with property(F) by ((a)$\Rightarrow$(b)) of the theorem, we have that $M[x,y]$ is Noetherian as an $R[x,y]$-module. Hence $M[x,x^{-1}]$ is Noetherian as an $R[x,y]$-module. Since the map $R[x,y] \longrightarrow R[x,x^{-1}]$ is onto, the $R[x,x^{-1}]$-submodules of $M[x,x^{-1}]$ are the same as the $R[x,y]$-submodules of $M[x,x^{-1}]$. Thus $M[x,x^{-1}]$ is Noetherian as an $R[x,x^{-1}]$-module.

((a)→(d)) This implication can be proved by modifying the technique of the proof of ((a) ⇒ (b)). For details we refer to [V:82].

1.4.2 COROLLARY. Let M be a Noetherian R-module with property(F). Then if $x_1, x_2, \ldots, x_k$ are finitely many indeterminates over R, the module $M[x_1, x_2, \ldots, x_k]$ is a Noetherian $R[x_1, x_2, \ldots, x_k]$-module with property(F).

Also $M[x_1, x_2, \ldots, x_k, x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}]$ is a Noetherian $R[x_1, x_2, \ldots, x_k, x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}]$-module with property(F).

1.4.3 REMARK. If R has identity, then every unitary R-module M has property(F). In particular taking M = R, the implication ((a) ⇒ (b)) of Theorem 1.4.1 yields the usual Hilbert Basis Theorem. Similarly the implication ((a) ⇒ (b)) generalises the power series analogue of the Hilbert Basis Theorem.

? (c)

1.4.4. REMARK. Let $n \geq 1$. Then $M[x]/(x^n)$, an $R[x]/(x^n)$-module, is a direct sum of finitely many copies of M. Any $R[x]/(x^n)$-submodule of $M[x]/(x^n)$ is also an R-submodule of $M[x]/(x^n)$. Hence $M[x]/(x^n)$ is Noetherian as an $R[x]/(x^n)$-module iff M is noetherian as an R-module. M need not have property(F).

1.4.5. REMARK. Let M be any non-zero module. For any integer $k \geq 0$, let $A_k = \{0\} \cup \{\text{elements of order} \geq k \text{ in } M[x]\}$. Then $A_0 \supsetneq A_1 \supsetneq \cdots$ is a strict descending chain of R[x]-submodules. Hence M[x] is not

Artinian as an $R[x]$-module. Similarly $M[[x]]$ is not Artinian as an $R[[x]]$-module.

§ 1.5 Some related questions.

Recall that an R-module M has Property(F) if for any R-submodule N of M, we have $R^{-1}N = \{m \in M \mid Rm \subseteq N\} = N$. We now prove the following equivalence.

1.5.1. PROPOSITION. An R-module M has Property(F) $\Leftrightarrow$ $m \in Rm$ $\forall$ $m \in M$.

Proof: Let M have property(F) and $m \in M$. Then Rm is an R-submodule of M. Consider $R^{-1}(Rm) = \{ x \in M \mid Rx \subseteq Rm \}$. Since M has property(F), $R^{-1}(Rm) = \{ x \in M \mid Rx \subseteq Rm \} = Rm$. Clearly $m \in R^{-1}(Rm)$ always. So $m \in Rm$ $\forall$ $m \in M$.

Conversely let $m \in Rm$ for each $m \in M$; and let N be an R-submodule of M. Then $R^{-1}N = \{ m \in M \mid Rm \subseteq N \}$. We always have $R^{-1}N \supseteq N$. $m \in Rm$

Now let $m \in R^{-1}N$. Then $Rm \subseteq N$ (by definition of $R^{-1}N$). Also $m \in M$?? by hypothesis. Hence $m \in N$. So $R^{-1}N \subseteq N$. Therefore $R^{-1}N = N$. ∎

The questions posed by Varadarajan may be stated as follows.

1.5.2 QUESTION. If the $R[[x]]$-module $M[[x]]$ has property(F), so does the R-module M. Is the converse true?

This question has been answered by Weimin Xue [X:91] in the negative and will be considered along with another of Varadarajan's questions stated below.

1.5.3 QUESTION. If an R-module M is Noetherian with property(F) is $M[x,y]$ Noetherian as an $R[x,y]$-module?

This question has also been answered by Weimin Xue but in the affirmative.

Xue's example which settles Question 1.5.2 is as follws:

Consider a field F and let $R = \bigoplus_{i=1}^{\infty} F$ be a direct sum of countable infinite copies of F. Let $M = {}_R R$. Clearly M has the property(F) as an R-module since $r \in Rr \ \forall\ r \in R$. We now show that the $R[[x]]$-module $M[[x]]$ does not have property(F).

Let $m_0 = (1,0,\dots), m_1 = (1,1,0,\dots),\ m_2 = (1,1,1,0,\dots),\dots$
Let $f(x) = \sum_{j\geq 0} m_j x^j \in M[[x]]$. For any $g(x) \in R[[x]]$, $g(x) = \sum_{i\geq 0} r_i x^i$, with $r = (a_0, a_1, \dots, a_t, 0, 0, \dots, 0)$ for some t. Then the coefficient of x^t in $g(x)f(x)$ is of the type $(b_1, b_2, \dots, b_t, 0, 0, \dots) \neq m$. So $g(x)f(x) \neq f(x)$. Since $f(x)$ was arbitrary, it follows that $f(x) \notin R[[x]]f(x)$. Hence $M[[x]]$ does not have property(F) as an $R[[x]]$-module.

NOTE. The module ${}_R R$ considered above is not a Noetherian module. The following theorem settles the second question(1.5.3).

1.5.4 THEOREM. If M is a Noetherian module with property(F), then the $R[[x]]$-module is also Noetherian with property(F).

Proof: It has already been proved by Varadarajan that $M[[x]]$ is Noetherian. It remains to show that $M[[x]]$ has property(F).
Let $f(x) = \sum_{j\geq 0} m_j x^j \in M[[x]]$; $m_j \in M$. Since M is Noetherian and has property(F), there exists $n \geq 0$ with $m_j \in \sum_{i=0}^{n} Rm_i$ for any $j \geq 0$.
Then $f(x) \in \sum_{i=0}^{n} R[[x]]m_i$. We use induction on n to show that

$f(x) \in R[[x]]f(x)$.

If $n = 0$ then, $m_i = a_i m_o$ for some $a_i \in R$ and all $i \geq 0$.

(i.e., $m_1 = a_1 m_o$, $m_2 = a_2 m_o$, ..., etc.).

Let $g(x) = \sum_{i\geq o} r_i x^i$ where $r_i = a_o$,

$r_1 = a_1 - r_o a_1$, ..., $r_k = a_k - r_{k-1}a_1 - r_{k-2}a_2 - \ldots\ldots - r_o a_k$.

Now $g(x)f(x) = \sum_{i\geq o} r_i x^i \sum_{j\geq o} m_j x^j$. The kth degree term of

$$g(x)f(x) = \Big(\sum_{i+j=k} r_i m_j\Big)x^k = \Big(\sum_{i+j=k} r_i a_j m_o\Big)x^k$$

Now $r_k = a_k - a_1 r_{k-1} - a_2 r_{k-2} - \ldots - a_k r_o$.

Therefore $a_k = r_k + r_{k-1}a_1 + r_{k-2}a_2 + \ldots + r_o a_k$.

$$= \sum_{i+j=k} r_i a_j m_o + (r_k - r_k a_o)$$

Therefore $m_k = a_k m_o = \sum_{i+j=k} r_i a_j m_o + (r_k - r_k a_o)m_o$

$$= \sum_{i+j=k} r_i a_j m_o + r_k m_o - r_k a_o m_o$$

$$= \sum_{i+j=k} r_i a_j m_o + r_k m_o - r_k m_o \quad \text{(Since } a_o m_o = m_o)$$

$$= \sum_{i+j=k} r_i a_j m_o .$$

Therefore the coefficient of x^k in (1) equals the coefficient of x^k in $f(x)g(x)$. Thus we have $f(x) = g(x)f(x) \in R[[x]]f(x)$.

Now let $n \geq 1$ and write $f = f_1 + f_2$ where $f_1 \in R[[x]]m_o$ and $f_2 \in \sum_{i=1}^{n} R[[x]]m_i$. By the above proof $\exists\ g_1 \in R[[x]]$ such that $g_1 f_1 = f_1$. Also since $f_2 - g_1 f_2 \in \sum_{i=1}^{n} R[[x]]m_i$, by induction there exists $g_2 \in R[[x]]$ such that $g_2(f_2 - g_1 f_2)$. Now take

$g = g_1 + g_2 - g_2 g_1$. Then

$gf = (g_1 + g_2 - g_2 g_1)(f_1 + f_2)$

$= g_1f_1 + g_2f_1 - g_2g_1f_1 + g_1f_2 + g_2f_2 - g_2g_1f_2$

$= g_2(f_2 - g_1f_2) + g_1f_2 + g_2f_1 + g_1f_1 - g_2g_1f_1$

$= f_2 - g_1f_2 + g_1f_1 + g_2f_1 + g_1f_2 - g_2g_1f_1$

$= f_2 + g_1f_1 + g_2f_1 - g_2g_1f_1$

$= f_2 + g_1f_1(1 - g_2) + g_2f_1$

$= f_2 + f_1(1 - g_2) + g_2f_1$

$= f_2 + f_1 - f_1g_2 + f_1g_2$

$= f_2 + f_1.$

Thus the theorem has been proved.

§ 1.6 Bibliographical notes.

1 The first four sections of this chapter i.e., § 1.1 to § 1.4 have been almost completely reproduced from [V:82]. The last section is aimed at answering a few questions posed by Varadarajan. This material is reproduced from [X:91].

2 A left module M (over a ring R, possibly without identity) is said to be s-unital if $u \in Ru$ for each $u \in M$. This concept has been attributed to Tominaga in [HT:79] and [H:81]. It follows from Proposition 1.5.1 that the concept of an s-unital module coincides with the concept of a module with property(F).

—————— * ——————

CHAPTER 2

POLYNOMIAL AND POWER SERIES RINGS OVER NON-COMMUTATIVE RINGS

Introduction.

In this chapter an attempt has been made to study polynomials and power series rings over rings (containing identity) which are not necessarily commutative. Among the rings considered will be Baer rings, P.P. rings, P.S. rings and regular rings. It is intended to see if the defining properties of the above- mentioned rings carry over to the respective polynomial and power series rings. Some results which are of independent interest concerning these rings have also been proved. These have been recorded at the beginning of each section.

§ 2.1 Basic Properties Of Polynomial And Power Series Rings.

Some standard properties of polynomial and power series rings which are well-known are stated (without proof) below.

(1) A ring R is a domain $\Leftrightarrow$ $R[x]$ is a domain $\Leftrightarrow$ $R[[x]]$ is a domain.

(2) A ring R is reduced $\Leftrightarrow$ $R[x]$ is reduced $\Leftrightarrow$ $R[[x]]$ is reduced.

(3) A ring R is a field $\Leftrightarrow$ $R[x]$ is a p.i.d.

If R is a field then $R[[x]]$ is a local p.i.d having a unique maximal ideal which is generated by x. Any non-zero ideal of $R[[x]]$ is of the type (x^m) where m is a natural number or zero.

(4) If $R = R_1 \times R_2 \times R_3 \times \ldots \times R_n$, where $R_1, R_2, \ldots, R_n$ are rings then $R[x] \cong R_1[x] \times R_2[x] \times \ldots \times R_n[x]$

NOTE. This isomorphism does not have an analogue in the case of direct product of rings. In general the natural map from $(\prod R_i)[x]$ to $\prod (R_i[x])$ is only one-one and not necessarily onto.

(5) If $R = \prod_{i=1}^{n} K_i$, K_i are fields, then $R[x]$ is hereditary, that is every ideal is projective.

§.2.2 C.P MODULES.

2.2.1 *Definition.* Let R be a ring. A right R-module M is said to be a C.P. module if every cyclic submodule of M is projective.

2.2.2. REMARKS AND EXAMPLES.

(I) Let R be a commutative domain and M a torsion free R-module. Then for each non-zero element $m \in M$ $Rm \cong R$. Thus every cyclic submodule of M is free over R (and hence projective) over R. Therefore M is a C.P. module.

(II) Let M be regular in the sense of Zelmanowitz [Z :72] i.e M is a module in which every cyclic submodule is a projective direct summand. Then every cyclic submodule is projective. Therefore M is a C.P. module.

(III) Letting M = R in the definition of a right C.P. module we get the concept of a right P.P. ring i.e a ring in which every principal right ideal is projective. These rings have been studied in more detail in the next section.

2.2.3 PROPOSITION. Let R be a ring and A_R a right R-module. The following conditions are equivalent.

(1) A_R is a C.P. module.

(2) For each $x \in A_R$, $r(x) = eR$ for some idempotent $e \in R$.

Proof. ((1)⇒(2)). Consider the exact sequence

$$0 \longrightarrow r(x) \xrightarrow{\iota} R \xrightarrow{j} xR \longrightarrow 0$$

where ι is the inclusion map and $j(a) = xa$ for any $a \in R$. Then, since xR is projective (being a cyclic submodule) the exact sequence splits and hence $R = r(x) \oplus x'R$ where $x'R \cong xR$. Therefore $r(x) = eR$ for some idempotent e of R.

((2)⇒(1)) Suppose xR is a cyclic submodule. Consider the exact sequence $0 \longrightarrow r(x) \longrightarrow R \longrightarrow xR \longrightarrow 0$ (with obvious maps).

We get $xR \cong R/r(x) = R/eR \cong (1-e)R$ and so projective.

Therefore xR is projective and A_R is a C.P. module.

2.2.4 THEOREM For a ring R, the following are equivalent.

(i) R is right P.P.

(ii) Every right R-module F_R is a C.P. module

(iii) Every projective right R-module P_R is a C.P. module.

Proof. ((i)⇒(ii)) It suffices to prove (ii) in the case $F_R = R^{(n)} = \{ (x_1, x_2, \ldots, x_n) \mid x_i \in R \}$ for some positive integer n.

Let $n \geq 1$ and let $xR \subseteq R^{(n)}$ where $x = (x_1, x_2, \ldots, x_n) \in R^{(n)}$.
Let $\Pi : R^{(n)} \longrightarrow R$ be the map given by $\Pi(r_1, r_2, \ldots, r_n) = r_1$ which is the projection to the first component of $R^{(n)}$.
Let $\bar{\Pi} = \Pi|_{xR}$ Then $\operatorname{Im} \bar{\Pi} = \{r' \in R \mid r' = \Pi(xr) \text{ for some } r \in R\}$.

$$= \{r' \in R \mid r' = x_1 r \text{ for some } r \in R\}$$

$= x_1R$, which is a principal (and therefore projective) right ideal of R. Therefore the exact sequence

$$0 \longrightarrow \operatorname{Ker} \bar{\Pi} \longrightarrow xR \longrightarrow \operatorname{Im} \bar{\Pi} \longrightarrow 0$$ splits and

$xR \cong \operatorname{Ker} \bar{\Pi} \oplus \operatorname{Im} \bar{\Pi}$. Hence $\operatorname{Ker} \bar{\Pi}$ is a cyclic sub-module of $R^{(n-1)}$ (since it is a direct summand of xR) and so is projective by the induction assumption.

Since $xR \cong \operatorname{Ker} \bar{\Pi} \oplus \operatorname{Im} \bar{\Pi}$ is the direct sum of two projective modules, xR is also projective. This proves the implication (1)⇒(2).

((2)⇒(3)) Trivial.

((3)⇒(1)) By hypothesis every projective right R-module is a C.P module. Now R_R is itself projective, since it is free over R. Therefore R_R is a C.P. module, i.e R is a right P.P. ring. ■

§ 2.3 Extensions of Baer and P.P. rings. The first half of this section contains : (i) definition and basic properties of Baer rings and P.P. rings; (ii) some results connecting Baer rings with P.P. rings ; (iii) results on quasi-regular rings; (iv) proof of the equivalence of left P.P. and right P.P. Conditions for normal rings. The second half is essentially devoted to the study of polynomial rings over reduced P.P. and reduced Baer rings.

2.3.1 REMARK. Let R be a ring and A any subset of R. Then in the notation of 0.2.8

$$l(A) = l(r(l(A))) \quad \ldots .(1)$$

and $$r(A) = r(l(r(A))) \quad \ldots .(2).$$

Proof. (See AF pp 37-38).

2.3.2 PROPOSITION. The following conditions are equivalent for any ring R.

(i) For each subset A of R, there exists an idempotent e of R such that $l(A) = Re$.

(ii) For each subset A of R, thers exists an idempotent e of R such that $r(A) = eR$.

Proof: It is enough to prove (i) $\Rightarrow$ (ii). The proof of the other implication will be exactly similar. By (i), we have

$$l(r(A)) = Re \text{ for some } e^2 = e .$$

Therefore $$r(A) = r(l(r(A))) \qquad \text{(by 2.3.1)}$$

$$= r(Re) = (1-e)R.$$

2.3.3 *Definition.* A ring R is said to be a Baer ring if the equivalent conditions of Proposition 2.3.2 hold.

2.3.4 REMARKS AND EXAMPLES.

(I) If R is a domain then R is clearly a Baer ring.

(II) If R is a semi-simple ring, then any left ideal is a direct summand, hence R is Baer.

(III) Let R be a Baer ring. Then R is left and right non-singular.
Proof: Let $x \in \mathcal{Z}({}_R R)$. Then $Lx = 0$ for some large left ideal L of R. So $x \in r(L) = fR$, where $f = f^2$ (since R is Baer.) This implies that $Lf = 0$.

Let $z \in L$. Then $zf = 0$ gives $z = z - zf = z(1 - f)$. Therefore $z \in R(1 - f)$ so we have $L \subseteq R(1 - f) \Rightarrow Rf = 0 \Rightarrow f = 0 \Rightarrow x = 0$ showing that $Z({}_R R) = 0$.

(IV) It follows from (III) that commutative Baer rings are necessarily reduced.(Apply 0.3.1 of Chapter 0.)

(V) A Baer ring contains no non-zero central nilpotent elements. This generalises (IV).

(VI) For example if ${}_D V$ is an arbitrary vector space,then $\mathrm{End}({}_D V)$ is a Baer ring.

(For proofs of (V), (VI) and related results on Baer rings, we shall refer to Chapter III §.8 of [S]. See also Example 4 (XII) § 5 of [S].)

(VII) If R is a Prüfer domain (i.e., a semi-hereditary domain, i.e., a (commutative) domain in which every finitely generated ideal is projective.) then $M_n(R)$ is a Baer ring $\forall$ n. (See page 17 of [K]).

2.3.5 *Definition.* A ring R is said to be a left P.P. ring (principal projective) if every principal left ideal of R is projective. An equivalent condition is that the left annihilator of every element of R is generated by an idempotent. The proof of this equivalence is a special case of Proposition 2.3.2.

2.3.6 PROPOSITION. Let R be a ring. Then the following conditions are equivalent. (i) $\forall\, a \in R$, Ra is projective.

(ii) $\forall\, a \in R$, $l(a) = Re$ for some $e = e^2$.

Proof: ((i) $\Rightarrow$ (ii)) Let $a \in R$. Consider the exact sequence

$$0 \longrightarrow l(a) \longrightarrow R \xrightarrow{g} Ra \longrightarrow 0$$

where g is defined by $g(x) = xa$. Since Ra is projective, this exact sequence splits. So $R = l(a) \oplus Ra'$ for some $a' \in R$. Hence $l(a) = Re$ for some $e = e^2$.

((ii) $\Rightarrow$ (i)) Let $a \in R$ and $l(a) = Re$ for some $e = e^2$. We have two exact sequences (with obvious maps):

$$0 \longrightarrow l(a) \longrightarrow R \longrightarrow Ra \longrightarrow 0 \text{ and}$$

$$0 \longrightarrow Re \longrightarrow R \longrightarrow R/Re \longrightarrow 0.$$

Since $l(a) = Re$, it follows that $Ra \cong R/Re \cong R(1-e)$ where $(1-e)^2 = (1-e)$, showing that Ra is projective. ∎

2.3.7 REMARKS AND EXAMPLES.

(I) Let R be a left semi-hereditary ring i.e., every finitely generated left ideal of R is projective. Then every principal left ideal of R is projective. Therefore R is a left P.P. ring.

(II) Let R be a domain. Then R is a left and right P.P. ring.

(III) Baer rings are always left and right P.P. The converse is however not true. Consider the following example.

2.3.8 EXAMPLE.

Let $\mathbb{N}$ be the set of natural numbers and $\mathcal{P}(\mathbb{N})$ its power set. Define $\oplus$ and $\circ$ in $\mathcal{P}(\mathbb{N})$ as follows: For $A, B \in \mathcal{P}(\mathbb{N})$

$A \oplus B = (A \setminus B) \cup (B \setminus A)$; and $A \circ B = A \cap B$.

This gives a ring structure, which has ϕ as the zero element, $\mathbb{N}$ is the multiplicative identity, and $A \oplus A = (A\setminus A) \cup (A \setminus A)$, showing that each element is its own additive inverse.

Also, $A^2 = A \circ A = A \cap A = A$. Hence $\mathcal{P}(\mathbb{N})$ becomes a Boolean ring

Consider the subring $L_o = \{ A \in \mathcal{P}(\mathbb{N}) \mid A \text{ is finite or co-finite.} \}$

Let $S = \{ \{2n\} \mid n \in N \} \subseteq L_o \subseteq \mathcal{P}(\mathbb{N})$. Then $l(S) \supseteq \{ 2n+1 \mid n \in \mathbb{N} \} = O_d$

$l(S) \in \mathcal{P}(\mathbb{N})$ but $l(S) \notin L_o$.

Now, $l_{\mathcal{P}(\mathbb{N})}(S) = \{ T \mid T \subseteq \text{odd natural numbers} \}$

$= O_d\mathcal{P}(\mathbb{N}) = \{ B \mid B \subseteq O_d \}$

We know $l_{L_o}(S) = l_{\mathcal{P}(\mathbb{N})}(S) \cap L_o$.

$= O_d\mathcal{P}(\mathbb{N}) \cap L_o$.

If $O_d\mathcal{P}(\mathbb{N}) \cap L_o = D\, L_o$ then

$O_d\mathcal{P}(\mathbb{N}) \cap L_o = \{ T \text{ finite} \mid T \subseteq O_d \}$. So D has to be such that T is finite, $T \subseteq O_d$ and $T \in D\, L_o \Rightarrow T \subseteq D$ which is absurd.

Thus L_o is P.P. but not Baer.

2.3.9. *Definition.* Let R be a commutative ring and S_o = N.Z.D's of R. Then R is said to be quasi-regular if $K = S_o^{-1}R$ is regular. (This notation will be followed in this section.)

2.3.10 REMARKS AND EXAMPLES.

(I) If R is a commutative regular ring, then every N.Z.D of R is a unit, so R is quasi-regular.

(II) Let $R = \prod_{\iota\in I} D_\iota$, D_ι commutative domain for each ι.

Let $K_\iota =$ the field of fractions of D_ι.

Then $S_o = \left\{(a_\iota)_{\iota\in I},\ \text{each } a_\iota \neq 0.\right\}$

An element z of $S_o^{-1}R$ is of the type $\left[\dfrac{(d_\iota)_{\iota\in I}}{(a_\iota)_{\iota\in I}}\right]$, $d_\iota \in D_\iota$; $a_\iota \neq 0\ \forall\ \iota$.

$$z = \left[\frac{d_\iota}{a_\iota}\right]_{\iota\in I},\quad d_\iota \in D_\iota,\ a_\iota \in A_\iota,\ a_\iota \neq 0.$$

So $z \in \prod_{\iota\in I} K_\iota$. Also any $(\alpha_\iota)_{\iota\in I} \in \prod_{\iota\in I} K_\iota$ is of the type

$$(\alpha)_{\iota\in I} = \left[\frac{d_\iota}{a_\iota}\right]_{\iota\in I};\ d_\iota \in D_\iota,\ a_\iota \in D_\iota,\ a_\iota \neq 0.$$

$$= \frac{(d_\iota)_{\iota\in I}}{(a_\iota)_{\iota\in I}};\quad d_\iota \in D_\iota,\ a_\iota \in D_\iota,\ a_\iota \neq 0.$$

$$\in S_o^{-1}R.$$

Thus we have $S_o^{-1}R \cong \prod_{\iota\in I} K_\iota$, and $\prod_{\iota\in I} K_\iota$, (being a product of fields) is regular. Hence $S_o^{-1}R$ is regular, so R is quasi-regular.

(III) Let $R = \prod_{\iota\in I} R_\iota$, each R_ι is quasi-regular.

Let $S_\iota =$ N.Z.D's of R_ι for each ι. Then

$S_o = \prod_{\iota\in I} S_\iota$. So $S_o^{-1}R = (\prod S_\iota)^{-1}\prod R_\iota \cong \prod_{\iota\in I}(S_\iota^{-1}R_\iota)$ which is regular by our hypothesis, showing that R is quasi-regular.

(IV) If R is quasi-regular then R is reduced. (Converse is not true). This holds since R is a subring of K, which being commutative regular, is reduced.

2.3.11 REMARK. If R is a reduced ring (not necessarily commutative), then $\mathrm{Ann}\,\mathrm{Ann}(x) \cap \mathrm{Ann}(x) = 0$, $\forall\, x \in R$. (See 0.2.8 for notation.)

Proof: Let $r \in \mathrm{Ann}\,\mathrm{Ann}(x) \cap \mathrm{Ann}(x)$, $x \in R$. Then $r\mathrm{Ann}(x) = 0$ and $r \in \mathrm{Ann}(x)$. Therefore $r^2 = 0 \Rightarrow r = 0$ (since R is reduced) which proves the remark. ■

2.3.12 REMARK. Let B be an ideal of a commutative ring R.

Then $\mathrm{Ann}_K(S_o^{-1}B) = S_o^{-1}\mathrm{Ann}_K(B)$.

Proof: Let $z/d \in S_o^{-1}\mathrm{Ann}_K(B)$, with $d \in S_o$, $z \in \mathrm{Ann}_K(B)$.

Then $zB = 0 \Rightarrow (z/d)(S_o^{-1}B) = 0$.

$\Rightarrow (z/d) \in \mathrm{Ann}_K(S_o^{-1}B)$.

Next let $x/d' \in \mathrm{Ann}_K(S_o^{-1}B) \Rightarrow (x/d')(S_o^{-1}B) = 0 \Rightarrow \forall\, y \in B$, $(x/d')(y/1) = 0 \Rightarrow (xy/d') = 0 \Rightarrow xy = 0$ (since S_o = N.Z.D's of R) $\forall\, y \in B$, $\Rightarrow x \in \mathrm{Ann}_R(B) \Rightarrow (x/d) \in S_o^{-1}\mathrm{Ann}_R(B)$, which proves the remark. ■

2.3.13 REMARK. $S_o^{-1}\mathrm{Ann}_R(A) \cap R = \mathrm{Ann}_R(A)$, if R is commutative.

Proof: We already have the inclusions $S_o^{-1}\mathrm{Ann}_R(A) \supseteq \mathrm{Ann}_R(A)$ and $R \supseteq \mathrm{Ann}_R(A)$. Therefore $S_o^{-1}\mathrm{Ann}_R(A) \cap R \supseteq \mathrm{Ann}_R(A)$ .... (1)

Now let $(a/t) \in S_o^{-1}\mathrm{Ann}_R(A) \cap R \Rightarrow (a/t) = r/1$ for some $r \in R$,

So we have $rt = a$, $aA = 0 \Rightarrow rtA = 0 \Rightarrow rA = 0$ (since $t \in S_o$)

$\Rightarrow r \in \mathrm{Ann}_R(A)$. Therefore $S_o^{-1}\mathrm{Ann}_R(A) \cap R \leq \mathrm{Ann}_R(A)$. ....(2)

From (1) and (2) we obtain $S_o^{-1}\mathrm{Ann}_R(A) \cap R = \mathrm{Ann}_R(A)$. ∎

We now have the following characterisation of quasi regular rings.

2.3.14 <u>THEOREM</u> For a commutative ring R, the following are equivalent.

(1) For all $x \in R$, $\exists\ x' \in R$ such that $\mathrm{Ann}\,\mathrm{Ann}(x) = \mathrm{Ann}(x')$ and R is a reduced ring.

(2) For all $x \in R$, $\exists$ a non-zero-divisor $d \in R$ such that $xd = x^2$.

(3) R is a quasi regular ring.

Proof: ((1)$\Rightarrow$(2)) We first show that $x + x'$ is a non-zero-divisor of R. Suppose $(x + x')s = 0$ for some $s \in R$. Then $xs = -x's$. Now $x \in \mathrm{Ann}\,\mathrm{Ann}(x)$. Since $\mathrm{Ann}\,\mathrm{Ann}(x) = \mathrm{Ann}(x')$ (by hypothesis), it follows that $x \in \mathrm{Ann}(x') \Rightarrow xx' = 0 \Rightarrow xx's = 0 \Rightarrow x's \in \mathrm{Ann}(x) \Rightarrow -x's \in \mathrm{Ann}(x) \Rightarrow xs \in \mathrm{Ann}(x) \Rightarrow xs \in \mathrm{Ann}\,\mathrm{Ann}(x) \cap \mathrm{Ann}(x)$. Since R is reduced, by Remark 2.3.11., $\mathrm{Ann}\,\mathrm{Ann}(x) \cap \mathrm{Ann}(x) = 0$. Hence $xs = 0$. Therefore, $s \in \mathrm{Ann}(x)$. Also, $xs = -x's = 0 \Rightarrow x \in \mathrm{Ann}(x') = \mathrm{Ann}\,\mathrm{Ann}(x)$. Therefore, $s \in \mathrm{Ann}\,\mathrm{Ann}(x) \cap \mathrm{Ann}(x) = 0$, showing that $x + x'$ is a non-zero-divisor, and

$$x(x + x') = x^2 + xx' = x^2 \text{ (since } xx' = 0).$$

((2) $\Rightarrow$ (3)). Let $xd^{-1} \in K$ where $x \in R$ and d is a non-zero-divisor of R. By (2), $\exists$ a non-zero-divisor $u \in R$ such that $xu = x^2$ or $x = x^2u^{-1}$ (in K). Hence, $x/d = (x/d)^2.d.u^{-1} = (x/d)(d/u)(x/d)$, showing that K is regular, hence R is quasi-regular.

((3) $\Rightarrow$ (1)). Let $x \in R \leq K$. Then since K is a P.P. ring (since K is commutative regular), $\mathrm{Ann}_K(x) = \mathrm{Ann}_K(x/1) = \mathrm{Ann}_K(K.\ x/1)$

$$= \mathrm{Ann}_K(S_o^{-1}(Rx)) = S_o^{-1}\mathrm{Ann}_R(x).$$

(by Remark 2.3.12)

Therefore, $\mathrm{Ann}_K(x) \cap R = (S_o^{-1}\mathrm{Ann}_R(x)) \cap R = \mathrm{Ann}_R(x)$ (by 2.3.13). Therefore, $(\mathrm{Ann}_K(\mathrm{Ann}_K(x))) \cap R = (\mathrm{Ann}_K(S_o^{-1}\mathrm{Ann}_R(x)))\cap R$

$$= (S_o^{1}\mathrm{Ann}_R(\mathrm{Ann}_R(x))) \cap R$$

$$= \mathrm{Ann}_R\mathrm{Ann}_R(x).$$ ∎

2.3.15 COROLLARY. If R is a commutative P.P.ring, then R is quasi-regular.

Proof: First note that if R is a commutative P.P. ring, then R is necessarily reduced. (For let $a \in R$ satisfy $a^2 = 0$. Since Ra is projective, the exact sequence

$$0 \longrightarrow \mathrm{Ann}(a) \longrightarrow R \longrightarrow Ra \longrightarrow 0$$

splits and therefore $R = \mathrm{Ann}(a) \oplus Ra'$ with $Ra' \cong Ra$. This isomorphism yields $aRa' = 0$ and therefore $aR = 0$.)

Let $x \in R$. Then $\mathrm{Ann}(x) = Re$ for some $e = e^2$ (by 2.3.6). Hence $\mathrm{Ann}(\mathrm{Ann}(x)) = R(e-1) = \mathrm{Ann}(e)$; so condition (1) of Theorem 2.3.14 is satisfied, which proves that R is quasi-regular. ∎

2.3.16 LEMMA. Let R be a normal right P.P. ring. Then for every element c of R, ∃ an idempotent e and a left non-zero-divisor a of R such that $c = ae$.

Proof: Since R is a right P.P. ring, we have $r(c) = e'R$ for some idempotent e' of R. If we write $e = 1 - e'$, then e is also an idempotent.

Note that $ce = c - ce' = c$. ....(i)

Next we write $a = e' + c$.

If $ad = 0$, $d \in R$, then $e'd + cd = ad = 0$ and so

$$ead = ee'd + ecd = ecd = ced = cd = 0.$$

(Here we use $c \in$ centre R and $ce = c$ which has been proved above). This implies that $d \in r(c) = e'R$ and

$e'ad = e'd + ecd = e'd + ce'd = e'd + cd = e'd = 0$ (since $cd = 0$.)

$\Rightarrow d \in r(e') = (1 - e')R$.

Therefore $d \in e'R \cap (1 - e')R = 0$,

showing that a is a left non-zero-divisor.

Since $ae = (e' + c)e$; $e'e + ce = c$, a and e are the elements as required. ∎

2.3.17 <u>LEMMA</u>. Let R be a normal right P.P. ring. Then every left or right non-zero-divisor of R, is a non-zero-divisor of R.

Proof: Let b be a left non-zero-divisor of R. Suppose that $cb = 0$, $c \in R$. By Lemma 2.3.16, we have that $c = ae$ for some idempotent e of R and a left non-zero-divisor a of R. Then we have $aeb = 0$. Since a is a left non-zero-divisor, we have $eb = be = 0 \Rightarrow e = 0$ (since b is a left non-zero-divisor). Therefore, $c = ae = 0$, hence b is a non-zero-divisor.

Now, let b be a right non-zero divisor of R. Again, by Lemma 2.3.16, $b = ae$ for some left non-zero-divisor and idempotent e. Then $eb = ea = ae = b$. Hence $(1-e)b = 0$; since b is a right non-zero-divisor, we have $1 = e$, so $b = a$, which is a left non-zero-divisor. ∎

2.3.18 <u>PROPOSITION</u>. A normal ring R is a left P.P. ring if and only if it is a right P.P. ring.

Proof : Let R be a right P.P., normal ring. Let $c \in R$. By Lemma 2.3.16, $c = ae = ea'$, for some left non-zero-divisor a and an idempotent $e \in R$. By Lemma 2.3.17, a is a non-zero-divisor. Now, $l(c) = \{x \in R \mid xc = 0\} = \{x \in R \mid xae = 0\}$ $= \{x \in R \mid xea = 0\} = \{x \in R \mid xe = 0\} = R(1-e)$, showing that R is left P.P. ∎

We now study some properties of zero-divisors in R[x], where R is a reduced ring. The case when R is commutative will be considered in more detail in Chapter 3. We start with the following lemma

2.3.19 LEMMA. Let R be a reduced ring and $f(x)$, $g(x) \in R[x]$, with $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. Then $f(x)g(x) = 0$ if and only if $a_i b_j = 0 \ \forall\ 0 \le i \le n\ ;\ 0 \le j \le m$.

Proof: "If" part is trivial. We shall prove the "only if" part below. Suppose that $f(x)g(x) = 0$. We can assume that $n = m$. Now $f(x)g(x) = 0 \rightarrow (a_0 + a_1 x + \ldots + a_n x^n)(b_0 + b_1 x + \ldots + b_n x^n) = 0$. Thus we have the following set of equations

$$(A)\quad \left\{\begin{array}{ll} a_0 b_0 = 0 & \text{.............}(AI) \\ a_0 b_1 + a_1 b_0 = 0 & \text{.............}(AII) \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 & \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ \sum_{i+j=t} a_i b_j = 0. & \end{array}\right.$$

Since R is reduced, $a_o b_o = 0 \Rightarrow b_o a_o b_o = 0 \Rightarrow b_o a_o b_o a_o = 0$

$\Rightarrow b_o a_o = 0$.

Now, $b_o.(AI) \Rightarrow b_o a_o b_1 + b_o a_1 b_o = 0 \Rightarrow b_o a_1 b_o = 0 \Rightarrow b_o a_1 b_o a_1 = 0$

$\Rightarrow b_o a_1 = 0$ (since R is reduced).

Also $b_o.(AII) \Rightarrow b_o a_o b_2 + b_o a_1 b_1 + b_o a_2 b_o = 0 \Rightarrow b_o a_2 b_o = 0 \Rightarrow b_o a_2 b_o a_2 = 0$

$\Rightarrow b_o a_2 = 0 \Rightarrow a_2 b_o = 0$. Continuing in this way we get that

$a_i b_0 = 0 \quad \forall \quad 1 \le i \le n$.

Thus the set of equations (A) reduce to

$$(B)\quad \begin{cases} a_o b_1 = 0 \\ a_1 b_1 + a_o b_2 = 0 \quad \text{.................................}(BI) \\ a_2 b_1 + a_1 b_2 + a_o b_3 = 0 \quad \text{.................................}(BII) \\ \text{.......................} \\ a_{n-1} b_1 + a_{n-2} b_2 + \ldots + a_o b_n = 0 \end{cases}$$

Again $a_o b_1 = 0 \Rightarrow b_1 a_o = 0$

$\Rightarrow b_1 a_1 = 0 \Rightarrow a_1 b_1 = 0$.

And $b_1 \times (BII) \Rightarrow b_1 a_2 b_1 + b_1 a_1 b_2 + b_1 a_o b_3 = 0 \Rightarrow b_1 a_2 b_1 = 0 \Rightarrow b_1 a_2 b_1 a_2 = 0$

$\Rightarrow b_1 a_2 = 0 \Rightarrow a_2 b_1 = 0$. Continuing in this way we have that

$a_i b_1 = 0 \quad \forall \quad 1 \le i \le n$. Repeating the process n times we have,

$a_i b_j = 0 \quad \forall \quad 1 \le i \le n, \quad 1 \le j \le n$.

2.3.20 REMARKS. (I) Suppose R is reduced and $f(x)g(x) = 0$ in the notation of 2.3.19. Then the lemma implies that $f(x)b_j = 0$ for each j. Hence $g(x) \neq 0$ implies that there exists $b \in R$, $b \neq 0$ such that $f(x)b = 0$. (See Remark (III) after Theorem 3.1.7 below.)

(II) The hypothesis R reduced cannot be dropped in 2.3.19.

Consider the following example:

2.3.21 EXAMPLE : Let $R = M_2(\mathbb{Z})$ (R is not reduced).

$R[x] = M_2(\mathbb{Z})[x]$. Let $f(x) = E_{12}x + E_{11}$; $g(x) = E_{11}x - E_{21}$.

Then $f(x)g(x) = (E_{12}x + E_{11})(E_{11}x - E_{21})$

$$= E_{12}E_{11}x^2 + (E_{11}E_{11} - E_{12}E_{21})x + E_{11}(-E_{21})$$

$$= 0 + (E_{11} - E_{11})x + 0 = 0.$$

But $E_{11}E_{11} = E_{11} \neq 0$ and $E_{12}(-E_{21}) = -E_{11} \neq 0$.

On imposing commutativity on R also, R reduced cannot be dropped, as can be seen in the example below.

2.3.22 EXAMPLE. We shall first recall NAGATA'S PRINCIPLE OF IDEALISATION which is as follows:

Let R be a commutative ring and M an R-module. Then the R-module $R \oplus M$ acquires a ring structure where addition is defined as usual and "$\circ$" is defined as: for $(a,m), (b,n) \in R \oplus M$, $(a,m)\circ(b,n) = (ab, an + bm)$. We shall use the notation $R(+)M$ for this ring. It is easy to see this operation is commutative as well as associative. Any ideal of $R(+)M$ contained in $0(+)M \equiv M$ is of the type $0(+)N$, where N is a sub-module of M. In particular M is also an ideal of $R(+)M$. Let $(0,m),(0,n) \in 0(+)M$. Then, $(0,m)\circ(0,n) = (0,0)$. Therefore $M^2 = 0$, so $R(+)M$ is not reduced whenever $M \neq 0$. With this identification M is a nilpotent ideal . Thus the above principle converts R-modules into ideals of $R(+)M$.

Now consider $\mathbb{Z}_8(+)\mathbb{Z}_8$, with + and $\circ$ defined as above and its ring of polynomials $\{\mathbb{Z}_8(+)\mathbb{Z}_8\}[x]$. Choose $f(x) = (4,0) + (4,1)x = a + bx$ (say Then $(f(x))^2 = a^2 + abx + abx + b^2x^2$. Now, $a^2 = (4,0)\circ(4,0) = (16,0) = 0$. $ab = (4,0)\circ(4,1) = (0,4) \neq 0$, $ab + ab = (0,4) + (0,4) = (0,8) = 0$.

Therefore we have that $(f(x))^2 = 0$, but $ab \neq 0$.

(We have not seen this example recorded in the literature.) good one

2.3.23 COROLLARY. If R is a reduced ring and $f(x) \in R[x]$ such that $(f(x))^2 = f(x)$, then $f(x) \in R$.

Proof: Let $f(x) = \sum_{i=0}^{n} a_i x^i$, so that $1 - f(x) = (1 - a_0) - \sum_{i=1}^{n} a_i x^i$.
Now $(f(x))^2 = f(x) \Rightarrow f(x)(1 - f(x)) = 0 \Rightarrow (1 - a_0)a_0 = 0$ and $a_i a_j = 0 \ \forall\ 1 \le i,j \le n$. In particular, $a_i^2 = 0 \ \forall\ 1 \le i \le n$.
Therefore $a_i = 0 \ \forall\ 1 \le i \le n$ (since R is reduced), $\Rightarrow f(x) \in R$. ∎

2.3.24 REMARK. The above corollary has a generalisation to normal rings (see 0.2.9), for let $(f(x))^2 = f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ where R is a normal ring. Then we have

$$\begin{aligned}(f(x))^2 &= (a_0 + a_1 x + \dots + a_n x^n)(a_0 + a_1 x + \dots + a_n x^n) \\ &= a_0^2 + (a_0 a_1 + a_1 a_0)x + (a_0 a_2 + a_1^2 + a_2 a_0)x^2 + \dots + a_n^2 x^{2n} \\ &= a_0 + a_1 x + \dots + a_n x^n\end{aligned}$$

Thus we have the following set of equations;

$a_0^2 = a_0 \Rightarrow a_0 \in C(R)$, the centre of R (since R is normal).

Therefore $a_0 a_i = a_i a_0 \quad \forall\ 1 \le i \le n$.

So $a_0 a_1 + a_1 a_0 = a_1$ i.e., $2a_0 a_1 = a_1$ ....(I).

Also $2a_0 a_2 + a_1^2 = a_2$ ....(II)

$a_0 \times (I) \Rightarrow 2a_0^2 a_1 = a_0 a_1$, i.e., $2a_0 a_1 = a_0 a_1 \Rightarrow a_0 a_1 = 0 \Rightarrow a_1 = 0$.

Also $2a_0 a_2 + a_1^2 = a_2 \Rightarrow 2a_0 a_2 = a_2 \Rightarrow 2a_0^2 a_2 = a_0 a_2 \Rightarrow 2a_0 a_2 = a_0 a_2$
$\Rightarrow a_0 a_2 = a_2 = 0$. Continuing in this way, we get that $a_i = 0 \ \forall\ i \ge 1$.
Therefore $f(x) \in R$. ∎

(We have not seen this generalisation recorded in the literature.)

2.3.25 COROLLARY. Let R be a reduced ring and $U \subseteq R[x]$. If $T = \bigcup_{f \in U} S_f$ then $Ann_{R[x]}(U) = Ann_R(T)[x]$, where $f = \sum_{i=0}^{n} a_i x^i$ and $S_f = \{a_0, a_1, \ldots, a_n\}$

Proof: Let $g(x) \in Ann_R(T)[x] \Rightarrow g(x) = b_0 + b_1 x + \ldots + b_t x^t$, where $b_i \in Ann_R(T) \quad \forall\ 1 \le i \le t \Rightarrow b_i U = 0 \quad \forall\ 1 \le i \le t \Rightarrow b_i \in Ann_R(U)$ and $Ann_R(U) \subseteq Ann_{R[x]}(U)$..............(I)

Conversely suppose that $gU = 0 \Rightarrow gf = 0 \quad \forall\ f \in U$ where $g = b_0 + b_1 x + \ldots + b_m x^m$. By Lemma 2.3.15, $b_i \in Ann_R(T) \Rightarrow$ $g \in Ann_R(T)[x] \Rightarrow Ann_{R[x]}(U) \subseteq Ann_R(T)[x]$ ....(II).

(I) and (II) $\Rightarrow Ann_R(T)[x] = Ann_{R[x]}(U)$.

2.3.26 REMARK. In any ring R, $l_R(a) = R \cap l_{R[x]}(a)$. (This is true in the more general situation when R is a subring of R'.)

Proof: Let $\underline{x} \in l_R(a)$. Then $\underline{x}a = 0$ and $\underline{x} \in R \subseteq R[x]$.

So $\underline{x} \in R \cap l_{R[x]}(a)$. Therefore $l_R(a) \subseteq R \cap l_{R[x]}(a)$..............(I)

Next let $f(x) \in R \cap l_{R[x]}(a) \Rightarrow f(x) \in R$ and $f(x)a = 0$ $\Rightarrow f(x) = y$ and $ya = 0 \Rightarrow y \in l_R(a)$. Therefore $R \cap l_{R[x]}(a) \subseteq l_R(a)$.......(II)

From (I) and (II) we have that $l_R(a) = R \cap l_{R[x]}(a)$.

2.3.27 REMARK Suppose $Ann_R(a) = Re_1$ and $Ann_R(b) = Re_2$, for some commuting idempotents e_1 and e_2 of R. Then $Ann_R\{(a,b)\} = Re_1e_2$.

Proof: $(e_1e_2)^2 = e_1e_2e_1e_2 = e_1e_1e_2e_2 = e_1e_2$. If $z = xe_1 = ye_2$ then $z = ze_2 = xe_1e_2 \in Re_1e_2$, showing that $Ann_R\{(a,b)\} = Re_1e_2$.

2.3.28 REMARK. If R is reduced then by 2.3.19 R is left P.P if and only if R is right P.P. Hence we can talk about reduced P.P. rings unambiguously.

2.3.29 THEOREM. Let R be a reduced ring. Then $R[x]$ is a P.P. ring if and only if R is a P.P. ring.

Proof: Let $a \in R$. Then $Ann_R(a) = R \cap Ann_{R[x]}(a)$ (by Remark 2.3.19) and $Ann_{R[x]}(a) = R[x]e$ for some idempotent e of $R[x]$ (since $R[x]$ is a P.P. ring).By Corollary 2.3.24 since $e^2 = e \in R[x]$ we have $e \in R$. Therefore $Re = R \cap R[x]e = Ann_R(a)$ showing that R is a P.P. ring.

Conversely let R be a P.P. ring; i.e., $\forall\ a \in R$, $Ann_R(a) = Re$ e is an idempotent element of R. Then by Remark 2.3.27, $Ann_R\{(a,b)\} = Re_1e_2$, e_1e_2 an idempotent of R. By induction we have that for any finite subset $U \subseteq R$, $Ann_R(U) = Re$ for some idempotent $e \in R$. If $f \in R[x]$, then by Corollary 2.3.20, putting $U = \{f\}$, $T = S_f$, we have $Ann_R(f) = Ann_R(S_f)[x] = Re[x] = R[x]e$. Hence $R[x]$ is a P.P. ring.

The above theorem has a generalisation to power series rings also, which can be stated as follows:-

2.3.30 THEOREM. Let R be a reduced ring. Then $R[[x]]$ is a P.P. ring if and only if R is a P.P. ring.
(see [B:76])

2.3.31 THEOREM. Let $R[x]$ be a reduced ring. Then $R[x]$ is a Baer ring if and only if R is a Baer ring.

Proof: Let $R[x]$ be a Baer ring and $U \subseteq R[x]$. Let $T = \bigcup_{f \in U} S_f$ where $S_f = \{ a_0, a_1, \ldots, a_n\}$ if $f = \sum_{i=0}^{n} a_i x^i$. Then $Ann_R(T)[x] = Ann_{R[x]}(U)$ and $Ann_{R[x]}(U) = R[x]e$ (by Corollary 2.3.25).

$Ann_{R[x]}(U) \cap R = Ann_R(T)[x] \cap R = Ann_R(T)$ i.e., $R[x]e \cap R = Ann_R(T)$.

Since $e \in R$, $R[x]e \cap R = Re = \mathrm{Ann}_R(T)$, so that R is a Baer ring.

Conversely, let R be a Baer ring and $T \subseteq R$.

Let $U = \left\{ f = \sum_{i=1}^{n} a_i x^i \mid a_i \in T \right\}$. Then $U \subseteq R[x]$ and

$\mathrm{Ann}_R(T)[x] = \mathrm{Ann}_{R[x]}(U)$ (by Corollary 2.3.25). Since R is Baer,

$\mathrm{Ann}_R(T) = Re$ for some idempotent element e of R. So

$\mathrm{Ann}_R(T)[x] = Re[x] = R[x]e$. Therefore $\mathrm{Ann}_{R[x]}(U) = R[x]e$,

showing that R[x] is a Baer ring. ∎

This theorem does not have a generalisation to power series rings. (See [B:76].)

2.3.32 LEMMA. Let R be a commutative ring and M a finitely generated R-module. Then the following statements are equivalent.

(I) M is R-projective.

(II) M_p is R_p-free for all $p \in \mathrm{Spec}(R)$ and the function $p \longrightarrow \mathrm{rank}_{R_p}(M_p)$ is a continuous function from Spec(R) to the integers $\mathbb{Z}$.

2.3.33 THEOREM. Let R be a commutative ring. R is a P.P. ring if and only if R[x] is a P.P. ring.

For proof of 2.3.32 and 2.3.32 see [J:71].

§.2.4 Polynomial Rings over Regular Rings.

To start this section we recall the definition of a regular ring.

(For basic properties and examples of these rings see 0.2.13.)

2.4.1 *Definition.* A ring R is said to be (von Neumann) regular, if for every element $a \in R$, $\exists$ an element $b \in R$ such that the relation

$aba = a$ holds.

Let R be a ring with identity, $S = R[x]$. We have the natural map $c : R[x] \longrightarrow R$ defined by $c(f) = f(0)$.

Let $a \in R$. Then $c^{-1}(aR) = \{ f \mid \text{constant term of } f \in aR \}$

The main result of this section is to prove that if R is (von Neumann) regular then $c^{-1}(aR) = f_o R[x]$ where f_o is a non-zero-divisor in $R[x]$. The proof is a part of the following theorem.

2.4.2 THEOREM. Let R be a ring with identity. Then the following are equivalent.

(i) R is regular.

(ii) For each $a \in R$, $aS + xS$ is a principal right ideal of S which has a non-zero-divisor as a generator.

(iii) For each $a \in R$, $aS + xS$ is a projective right ideal of S.

(iv) For any $a \in R$, $\exists$ a non-zero-divisor $f_o \in S$ such that $c^{-1}(aR) = f_o S$.

Proof: ((i) $\Rightarrow$ (ii)) Let R be regular. Then $x \in S$, $a \in S \Rightarrow aS + xS \subseteq S$ for each $a \in R$. Now let $a \in R$. Since R is regular, $\exists\ b \in R$ such that the relation $aba = a$ holds. Let $e = ab = abab = e^2$. $ea = aba = a$. So $f = e + (1 - e)x \in S$.

Now $fa = (e + (1 - e)x)a = ea = a$; and

$$
\begin{aligned}
f((1 - e) + ex) &= (e + (1 - e)x)((1 - e) + ex) \\
&= e(1 - e) + e^2x + (1 - e)^2x + (1 - e)ex \\
&= ex + (1 - e)x = x.
\end{aligned}
$$

$$
\begin{aligned}
\text{Also } (1 - e + ex)f &= (1 - e + ex)(e + (1 - e)x) \\
&= (1 - e)e + (1 - e)^2x + e^2x + e(1 - e)x^2 \\
&= (1 - e)x + ex = x.
\end{aligned}
$$

Now $f = e + (1 - e)x = ab + (1 - ab)x \in aS + xS$. Therefore $fS \subseteq aS+xS$

Also $a = fa \in fS \Rightarrow aS \subseteq fS$, and $x = f(1 - e + ex) \in fS \Rightarrow xS \subseteq fS$

Therefore $aS + xS \subseteq fS$. We already have, $fS \subseteq aS + xS$. Therefore $aS + xS = fS$. Now to prove that f is a non-zero-divisor in S.

Let $g \in S$ be such that $fg = 0$. Then $xg = (1 - e + ex)\, fg = 0$.

This implies that $g = 0$ (since x is a non-zero-divisor).

Thus we have obtained f as a non-zero-divisor of S.

((ii) $\Rightarrow$ (iii)) Since $aS + xS = fS$, f non-zero-divisor, so $aS + xS$ is free over S and hence projective as a right ideal of S.

((iii) $\Rightarrow$ (iv)) Let $a \in R$. $c^{-1}(aR) = \{ f \mid \text{constant term of } f \in aR\}$

$= \{ab + a_1x + a_2x^2 + \ldots + a_nx^n \mid b \in R,\ a_i \in R\} = aR + xS \subseteq aS + xS$.

Now let $ag(x) + xh(x) \in aS + xS$. Then $g(x) = g_0 + g_1x + \ldots + g_mx^m$

So $ag(x) = ag_0 + ag_1x + \ldots + ag_mx^m = ag_0 + xg'(x)$. Therefore

$ag(x) + xh(x) = ag_0 + x(g'(x) + h(x)) \in aR + xS$ which shows that

$aS + xS \subseteq aR + xS$. Therefore $aR + xS = aS + xS$ and

$c^{-1}(aR) = aS + xS = f_0S$ where f_0 is a non-zero-divisor in S.

((iv) $\Rightarrow$ (iii)) Suppose $c^{-1}(aR) = f_0S$ for some f_0, a non-zero-divisor in S. We already have $c^{-1}(aR) = aS + xS$. So $aS + xS = f_0S$

$\Rightarrow aS + xS$ is a projective right ideal of S.

((iii) $\Rightarrow$ (i)) Let $K = aS + xS$ be a projective right ideal of S.

By dual basis lemma, $\exists$ S-homomorphisms $U, V : K \longrightarrow S$, such that

$\forall\, k \in K$, $k = aU(k) + xV(k) \longrightarrow$ (A). So in particular

$$a = aU(a) + xV(a) \longrightarrow \text{(B)}.$$ Since $x \in K$,

$xU(a) = U(a)x$ (since x is central), $U(a)x = U(x)a$ (since $x, a \in S$)

Then $(B).x \Rightarrow ax - aU(a)x = xV(a)x = x^2V(a) \Rightarrow ax - aU(x)a = x^2V(a) \longrightarrow (C)$

Let $U(x) = u_0 + u_1x + \ldots + u_tx^t$, $V(a) = d_0 + d_1x + \ldots + d_sx^s$.

Then R.H.S of (C) $= x^2V(a) = x^2(d_0+d_1x + \ldots + d_sx^s) = d_0x^2 + \ldots + d_sx^{s+2}$

The coefficient of x on the R.H.S of (C) equals 0, and

the coefficient of x on the L.H.S of (C) equals $a - au_1a$. Therefore

$a - au_1a = 0 \Rightarrow a = au_1a$. Hence R is regular.

2.4.3 COROLLARY. If R[x] is left or right semi-hereditary, then R is von Neumann regular.

§ 2.5 Rings with Projective Socle.

To start this section, we recall the definition of the socle of a module.

2.5.1 *Definition.* Let R be a ring, M a left R-module. Let $\mathcal{S} = \{ S \text{ sub-module of } M \mid S \text{ is simple} \}$. Then the Socle of M, written as SocM equals $\sum_{S \in \mathcal{S}} S$ and is a submodule of M.

2.5.2 EXAMPLES.

(I) When $R = \mathbb{Z}$, $M = \mathbb{Q}$, $Soc_{\mathbb{Z}}(\mathbb{Q}) = 0$.

(II) When $R = \mathbb{Z}$, $M = \mathbb{Z}$, $Soc_{\mathbb{Z}}(\mathbb{Z}) = 0$.

(III) When $R = \mathbb{Q}$, $M = \mathbb{Q}$, $Soc_{\mathbb{Q}}(\mathbb{Q}) = \mathbb{Q}$. More generally, we have that for a K-vector space V, $Soc_K(V) = V$.

2.5.3 *Definition.* A left R-module M is called a P.S. module if $Soc_R(M)$ is projective.

2.5.4 REMARKS AND EXAMPLES.

(I) An example of an R-module M which is non-projective but has a projective socle is when $R = \mathbb{Z}$, $M = \mathbb{Q}$. Then ${}_{\mathbb{Z}}\mathbb{Q}$ is non-projective but $Soc_{\mathbb{Z}}(\mathbb{Q}) = 0$ is projective.

(II) Let R be a ring, M a left R-module. Then the following conditions are equivalent.

(i) M is a P.S. module.

(ii) If S is a submodule of M, S simple, then S is projective.

Proof: ((i) → (ii)) Since M is a P.S module, $Soc_R(M) = \sum_{s \in S} S$ is projective. Now we know that $Soc_R(M)$ is semi-simple. So for any simple submodule S of M, S is a direct summand of $Soc_R(M)$, hence projective. ___

((ii) → (i)) TRIVIAL.

(III) Let M be a projective semi-simple module. Then $Soc_R(M) = M$ is projective, which shows that M is a P.S. module.

(IV) Let M be a Z-regular module i.e., every cyclic submodule is a projective direct summand of M ([Z:72]). Let S be a simple submodule of M. Since S is simple, S is cyclic, hence projective. So M is a P.S. module.

(V) Let M be a non-singular module. Then M is a P.S. module. (See 2.2.4 of [NW:88] for a proof.)

(VI) In fact we have the following implications.

M semi-simple projective ⇒ M Z-regular ⇒ M C.P. module ⇒ M P.S. module.

2.5.5 *Definition.* We call a ring a left P.S. ring if $_RR$ is a P.S. module.

2.5.6 REMARKS AND EXAMPLES.

(I) By letting M = R in 2.5.4(VI), we have the implications

R semi-simple ring $\Rightarrow$ R regular ring $\Rightarrow$ R left P.P. $\Rightarrow$ R left P.S.

(II) Let R be a left non-singular ring. Then R is a left P.S. ring. This is a special case of 2.5.4(V).

(III) For a commutative ring R, we have the implications;

R regular $\Rightarrow$ R P.P. $\Rightarrow$ R quasi-regular $\Rightarrow$ R reduced $\Rightarrow$ R P.S.

(IV) If R is a semi-prime ring then R is a left and right P.S. ring. (Apply [L], § 3.4, Corollary to Proposition 1.)

(V) Let R = $\mathbb{Z}$ or any domain. Then every principal left/right ideal is free. So R is left/right P.S.

2.5.7 THEOREM. Let R be a ring. The following conditions are equivalent

(i) R is a left P.S. ring.

(ii) R has a faithful left P.S. module.

(iii) If L is a maximal left ideal of R, then either r(L) = 0 or L = Re for some idempotent element e of R.

(iv) If L is an essential maximal left ideal of R then r(L) = 0.

(v) If L is maximal left ideal of R, then r(L) = fR where

f is an idempotent element of R.

(vi) If L is a maximal left ideal of R and $t \in r(L)$, then $t \in r(L)t$.

(vii) Every simple module ${}_RK$ is either projective or $K^d = 0$ where the dual module is given by $K^d = \mathrm{Hom}(K,R)$.

(viii) Soc $({}_RR)$ is projective.

Proof: ((i) $\Rightarrow$ (ii)) If R is a P.S.ring then ${}_RR$ is a faithful P.S. module.

((ii) $\Rightarrow$ (iii)) Let ${}_RM$ be a faithful P.S. module. Let $L \leq R$ be a maximal left ideal of R. If $r(L) \neq 0$, write $T = r(L)$ so that $LT = 0$. Also $RT \neq 0$ by hypothesis, since M is a faithful P.S. module, $RTM \neq 0$. So $\exists\ m \in TM$ such that $Rm \neq 0$. Now $TM = r(L)M$. So $Lm = 0 \Rightarrow L \leq l(m)$ and $l(m) \neq R$. Since L is a maximal left ideal of R, it follows that $L = l(m)$. Now $R/L = R/l(m) \cong Rm$, which is projective by hypothesis; and so $L = Re$ for some $e = e^2 \in R$.

((iii) $\Rightarrow$ (iv)) Since L is an essential maximal left ideal of R, then $L = Re$ (with $e^2 = e \neq 1$) is impossible.

((iv) $\Rightarrow$ (iii)) Let L be a maximal laft ideal of R satisfying $r(L) \neq 0$. Then, by hypothesis, L is non-essential and therefore a direct summand of ${}_RR$. Hence $L = Re$ is a direct summand of R.

((iv) $\Rightarrow$ (v)) Any maximal left ideal of R is either essential or a direct summand. If L is not essential, $L = Re$ for some $e = e^2$. Therefore $r(L) = (1-e)R = fR$ for some $f = f^2 \in R$.

$((v) \Rightarrow (vi))$ Let L be a maximal left ideal of R and $t \in r(L)$. Now $r(L) = fR$, $f = f^2 \in R$. So $t = ft \in r(L)t$.

$((vi) \Rightarrow (v))$ If $r(L) = 0$ we take $f = 0$. Therefore $r(L) = 0.R$ Otherwise let $0 \neq a \in r(L)$ with $f \in r(L)$. We shall show that $(1-f) \in L$. If $(1-f) \notin L$, since L is maximal, $R = L + R(1-f)$. So $1 = t + r(1-f)$, $t \in R$. Multiplying both sides by a, we have $a = ta + r(a-fa) = 0$ (since $t \in L$, $a \in r(L)$ $ta = 0$ and $a = fa$) which is a contradiction to our assumption that $0 \neq a$. Therefore $(1-f) \in L$. On the other hand, $(1-f)f = 0$ (since $f \in r(L)$) $\Rightarrow f^2 = f$. Also $Lf = 0 \Rightarrow L = L(1-f) \subseteq R(1-f) \neq R$. So $L = R(1-f)$ and $r(L) = fR$.

$((v) \Rightarrow (iv))$ Let L be an essential maximal left ideal of R. Since $r(L) = fR$, where $f^2 = f \in R$, $L \subseteq R(1-f)$. Also L is an essential left ideal. Therefore $L \cap Rf = 0 \Rightarrow Rf = 0 \Rightarrow f = 0$ $\Rightarrow r(L) = 0$.

$((iii) \Rightarrow (vii))$ Let $K = Rk$ be simple so that $L = l(k)$ is maximal and $R/L \cong K$. We now have the following cases.

Case 1. If $L = Re$, $e^2 = e$, then $K \cong R(1-e)$ is projective.

Case 2. Suppose $r(L) = 0$. Let $\lambda \in K^d = \mathrm{Hom}_R(K,R)$; $\lambda(k) = a \in R$, $La = L(\lambda(k)) = \lambda(Lk) = \lambda(0) = 0 \Rightarrow a \in r(L) = 0 \Rightarrow \lambda(k) = 0 \Rightarrow \lambda = 0$.

$((vii) \Rightarrow (viii))$ Let $\bar{K}$ be a simple left ideal of R. Notice that, for any non-zero left ideal $\bar{K}$ of R, $\mathrm{Hom}_R(\bar{K},R) \neq 0$ (the inclusion map from $\bar{K}$ to R belongs to $\mathrm{Hom}_R(\bar{K},R)$). Thus by hypothesis, ${}_R\bar{K}$ must be projective. Since $\bar{K}$ was arbitrarily chosen, it follows that $Soc_R(R)$ is projective.

((viii) ⇒ (i)) Follows by definition. ■

2.5.8 THEOREM. If R is a left P.S. ring, so also are $R[x]$ and $R[[x]]$.

Proof: Let L be a maximal left ideal of R. Let I denote the set *of all trailing coefficients of polynomials in L with 0 adjoined.* (Here trailing coefficient means the coefficient of the lowest non-zero degree term in the polynomial).

CLAIM. I is a left ideal of R.

Let $a,b \in I$. Now $a \in I \Rightarrow \exists\ f(x) \in L$ such that $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + ax^n$, $m > n$. Also $b \in I \Rightarrow \exists\ g(x) \in L$ such that $g(x) = b_t x^t + b_{t-1}x^{t-1} + \ldots + bx^u$, $t > u$.

Case 1. $n > u$. Let $l = n - u$. Then $x^l g(x) = b_t x^{l+t} + \ldots + bx^{u+l}$ Or $x^l g(x) = b_t x^{l+t} + \ldots + bx^n \in L$. Therefore $x^l g(x) - f(x) \in L$ $\Rightarrow b - a \in L \Rightarrow I$ is a subgroup of $(R, +)$. Similiarly if $u > n$, it can be shown that $a - b \in I$, and $n = u \Rightarrow f(x) - g(x) \in L \Rightarrow a - b \in L$.

Next let $a \in I$, $r \in R$. Now $a \in I \Rightarrow \exists\ f(x) \in L$, where $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + ax^n$. Then $rf(x) = ra_m x^m + ra_{m-1}x^{m-1} + \ldots + rax^n$ is clearly an element of L. Therefore $ra \in I$, showing that I is an ideal of R.

Suppose $I = R$. Then $\exists$ a polynomial $f(x) \in L$ such that $f(x)$ has 1 as its trailing coefficient i.e., $f(x)$ is of the type $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + 1.x^n$. Suppose $g(x) \in R[x]$ is such that $g(x)f(x) = 0$. Let $g(x) = g_t x^t + g_{t-1}x^{t-1} + \ldots + g_u x^u$. Then

$g(x)f(x) = (g_t x^t + \ldots + g_u x^u)(a_m x^m + \ldots + 1.x^n) = 0 \Rightarrow g_u = 0.$

So $g(x)$ reduces to $g_t x^t + \ldots + g_{u+1} x^{u+1}$. Therefore

$g(x)f(x) = g_t x^t + \ldots + g_{u+1} x^{u+1})(a_m x^m + \ldots + 1.x^n) = 0 \Rightarrow g_{u+1} = 0.$

Continuing in this way, it can be seen that $g_{u+2}, \ldots, g_m = 0$. Hence $g(x) = 0$. Since $g(x)$ was arbitrarily chosen, it follows that $r(L) = 0$. Next let $I \neq R$. We shall show that I is a maximal left ideal of R. Let $a \in R \setminus I$. Since $a \notin I$, $a \notin L$. So by maximality of L, $R[x] = L + R[x]a$. Since $1 \in R[x]$, $1 = f(x) + g(x)a$, where $f(x) \in L$, $g(x) \in R$. Considering constant terms,

$1 = l_o + r_o a$; $l_o \in L$, $f(x) = l_o + l_1 x + \ldots$; $r_o \in R$, $g(x) = r_o + r_1 x + \ldots$

If $l_o = 0$, $1 = r_o a \in Ra$. So $I + Ra = R$. If $l_o \neq 0$ also $I + Ra = R$, showing that I is a maximal left ideal of R. Since R is a P.S.ring, we have that $r(I) = eR$ with $e^2 = e \in R$. If $Le \subseteq L$, then $R[x] = L + Le$ Therefore $1 = f(x) + g(x)e$, $f(x), g(x) \in L$. Considering constant terms, $1 = f_o + g_o e$. By definition of I, $f_o, g_o \in I$. So $1 = f_o + g_o e$

$\Rightarrow e = (f_o + g_o e)e = f_o e + g_o e^2 = 0$ (since $Ie = 0$) $\Rightarrow e = 0$, $\Rightarrow g_o e = 0$

$\Rightarrow 1 = f_o \in I \Rightarrow I = R$, which is a contradiction. Therefore $Le \subseteq L$.

Now, let $f(x)e \in Le$; $f(x) \in L$. Then $f(x) = a_m x^m + \ldots + a_n x^n$; $a_n \in I$ So $f(x)e = a_m e x^m + \ldots + a_n e x^n$, but $a_n e = 0$. Therefore

$f(x)e = a_m e x^m + \ldots + a_{n+1} e x^{n+1} \in Le \subseteq L$

$\Rightarrow f_1(x) = a_m x^m + \ldots + a_{n+1} x^{n+1} \in L \Rightarrow a_{n+1} \in I \Rightarrow a_{n+1} e = 0$

$\Rightarrow f(x)e = a_m e x^m + \ldots + a_{n+2} e x^{n+2} \in Le \subseteq L \Rightarrow a_{n+2} \in I \Rightarrow a_{n+2} e = 0, \ldots$

$a_m \in I \Rightarrow a_m e = 0 \Rightarrow f(x)e = 0 \Rightarrow Le = 0$. Hence $r(L) \supseteq eR[x]$.

Next let $g \in r(L) - eR[x]$; $g = b_n x^n + b_{n+1} x^{n+1} + \ldots$, $b_n \neq 0$. If $b_n \in eR$, then $g - b_n x^n \in r(L)$; So we may assume that $b_n \notin eR$. Now $\forall\, h \in L$, $hg = 0$. (since $g \in r(L) - eR[x]$). Let $z \in I$; so $\exists\, f \in L$, $f = zx^t + f_{t+1} x^{t+1} + \ldots$. Since $f \in L$, $fg = 0$.

$\Rightarrow (zx^t + f_{t+1}x^{t+1} + \ldots)(b_n x^n + b_{n+1}x^{n+1} + \ldots) = 0 \Rightarrow zb_n = 0.$

Since z was an arbitrarily chosen element of I it follows that $Ib_n = 0 \Rightarrow b_n \in r(I) = eR$ -- a contradiction. Therefore $b_n = 0$ $\Rightarrow g = 0 \Rightarrow r(L) = eR[x]$, which proves that R is a P.S. ring.

Similiarly it can be proved that $R[[x]]$ is a P.S. ring. ∎

The converse to this theorem is false. Consider the following remarks followed by a counter example.

2.5.9 REMARK. Let R be a commutative ring, $R[x]$ its ring of polynomials. Then $J(R[x]) = \mathrm{Nil}(R[x])$ (in the notation of 0.2.3).

Proof: See Chapter 3, Corollary 3.1.6.

2.5.10 REMARK. Let $(R, \mathfrak{m})$ be a commutative local ring. Then $R' = R[[x]]$ is also a local ring, having $\mathfrak{m}' = \mathfrak{m} + xR'$ as the unique maximal ideal.

Proof: We first show that $\mathfrak{m}'$ is a maximal ideal of R. Consider the homomorphism $\theta : R' \longrightarrow R/\mathfrak{m}$ defined by $\theta(a_0 + a_1 x + \ldots) = \bar{a}_0$. This is clearly a ring homomorphism and

$\mathrm{Ker}\ \theta = \{ f(x) = a_0 + a_1 x + \ldots \mid a_0 \in \mathfrak{m} \} = \{ f(x) \mid f(x) \in \mathfrak{m}R' + xR' \}$

$\subseteq \mathfrak{m}R' + xR'$. Next let $f(x) \in \mathfrak{m}R' + xR'$. Then

$f(x) = \mu(\alpha_0 + \alpha_1 x + \ldots) + (b_0 + b_1 x + \ldots); \ \mu \in \mathfrak{m}$

$\quad = \mu\alpha_0 + (\mu\alpha_1 + b_0)x + (\mu\alpha_2 + b_1)x^2 + \ldots$

$\theta(f(x)) = \overline{\mu\alpha_0} = 0$. (since $\mu\alpha_0 \in \mathfrak{m}$). Therefore $\mathrm{Ker}\theta = \mathfrak{m}R' + xR'$.

Hence $R'/(\mathfrak{m}R' + xR') \cong R/\mathfrak{m}$ showing that $\mathfrak{m}R'' + xR'$ is a maximal ideal of R'. Now let $h(x) \in R' - \mathfrak{m}' = R[[x]] - (\mathfrak{m}R' + xR')$

$h(x) = h_0 + h_1 x + \ldots = h_0 + x(h_1 + h_2 x + \ldots)$. Since $h(x) \notin \mathfrak{m}'$

$h_o \notin \mathfrak{m} \Rightarrow h_o \in U(R) \Rightarrow \exists\, g_o \in R$ such that $h_o g_o = 1$. Let $g(x) = g_o + (-h_1 g_o^2)x + (h_1^2 g_o^3 - h_2 g_o^2)x^2 + \ldots$. Then

$$f(x)g(x) = (h_o + h_1x + h_2x^2 + \ldots)(g_o - h_1g_o^2x + (h_1^2g_o^3 - h_2g_o^2)x^2 + \ldots)$$

$= h_o g_o = 1$. This shows that $h(x) \in U(R[x])$; and hence shows that $\mathfrak{m}'$ is the unique maximal ideal of R'. ▨

2.5.11 <u>EXAMPLE</u>. If $R = \mathbb{Z}_4$, then $R[x]$ and $R[[x]]$ are P.S. rings but R is not a P.S. ring.

Proof: We have by Remark 2.5.9, $J(R[x]) = \mathrm{Nil}(R[x]) = 2R[x]$, and $J(R[[x]]) = 2R[[x]] + xR[[x]]$ (by Remark 2.5.10).

If L is a maximal ideal of $R[x]$, then $L \supsetneq 2R[x]$. (since $R[x]/2R[x] \cong \mathbb{Z}_2[x]$ which is not a field). Let $f(x) \in L - 2R[x]$; $f(x) = f_o + f_1x + f_2x^2 + \ldots$ Suppose i is the least positive integer for which $f_i \notin 2\mathbb{Z}_4$. Then $g(x) = f(x) - (f_o + f_1x + f_2x^2 + \ldots + f_{i-1}x^{i-1})$ $\in L$ (since $f_o + f_1x + \ldots + f_{i-1}x^{i-1} \in 2R[x] \subseteq L$).
$g(x) = f_ix^i + f_{i+1}x^{i+1} + \ldots$, $f_i \notin 2R$. Therefore $f_i = 1$ or 3; and $f_i^{-1}(g(x) = 1.x^i + f_i^{-1}f_{i+1}x^{i+1} + \ldots \in L$. Therefore $1 \in I$;
$\Rightarrow r(L) = 0$, showing $R[x]$ is a P.S. ring. ▨

2.5.12 <u>REMARK</u>. This example shows that commutative P.S. rings need not be reduced. Therefore commutative P.S. rings need not be P.P.

§ 2.6 <u>Bibliographical notes</u>.

1. The study of C.P. modules in § 2.2 is due to Evans [E:72].
2. § 2.3 is mostly a survey of some research done by Armendariz [A:74], Evans [E:72], Endo [E:60], Jondrup [J:71] and

Wolfson [W:61].

3. § 2.4 has been recorded after studying the work of Camillo [C:73], McCarthy [M:73] and Pillai [P:85].

4. The results of § 2.5 are due to Nicholson and Watters [NW:88].

5. Example 2.3.22 and Remark 2.3.24 are believed to be new.

*

CHAPTER 3

POLYNOMIAL AND POWER SERIES RINGS OVER COMMUTATIVE RINGS.

Introduction.

In this chapter, we shall study polynomial and power series rings over commutative rings. The study has been confined largely to zero divisors and nilpotent elements. A few results on the unit elements of these rings have also been stated at the beginning of this chapter. A very brief study of primary rings has also been made and a few results have been recorded. Throughout this chapter (unless otherwise mentioned) rings will be commutative. We may however, add commutative for the sake of emphasis.

§3.1 Generalities. In this section, we will study results which are of a general nature. We will characterise the units of a polynomial ring $R[x]$, R being a commutative ring. We will also characterise the divisors of zero in polynomial rings over commutative rings. We start with some well known results .

Recall that $Nil(R) = \left\{ x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N} \right\}$.

3.1.1 REMARK. Let R be a commutative ring. Suppose $x, y \in Nil(R)$. Then $x + y \in Nil(R)$.

Proof: TRIVIAL.

In fact, if R is commutative then Nil(R) is an ideal of R. We also have the following theorem.

3.1.2 THEOREM. Let R be a ring, SpecR = {p | p is a prime ideal of R}. Then $\bigcap_{p \in \mathrm{SpecR}} p = \mathrm{Nil}(R)$.

(This theorem is due to Krull, for a proof see [JII], p 392; and for a generalisation to non-commutative rings see [L] § 3.2 Proposition 1.) ∎

3.1.3 REMARK. Let D be a domain and D[x] the ring of polynomials. Then U(D[x]) = U(D) (U(D) = Units of D.). ∎

Proof: TRIVIAL.

3.1.4 THEOREM. Let R be a commutative ring, and R[x] its ring of polynomials. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$. Then f(x) is a unit in R[x] if and only if a_0 is a unit in R and $a_1, a_2, \ldots a_n$ are nilpotents.

Proof: ("Only if" part) Let p ∈ Spec(R). Consider the map

$$\eta : R[x] \longrightarrow (R/p)[x],$$

where $\eta(\sum_{i=0}^{n} c_i x^i) = \sum_{i=0}^{n} \bar{c}_i x^i$. Since p is a prime ideal of R, R/p is a domain. Let $f(x) \in R[x]$. Then $\eta(f(x)) \in (R/p)[x]$. Since $f(x) \in U(R[x])$, $\exists\ g(x) = b_0 + b_1x + \ldots \in R[x]$, such that $f(x)g(x) = 1$. $\Rightarrow \eta(f(x)g(x)) = \bar{1}$. $\Rightarrow \eta(f(x))\eta(g(x)) = \bar{1}$. By Remark 3.1.3, we have $\deg(\eta(f(x))) = 0$ i.e.,

$\eta(f(x)) = \bar{a}_0 + \bar{a}_1x + \ldots + \bar{a}_nx^n = \bar{a}_0$

i.e., $\bar{a}_i = 0\ \forall\ i \geq 1$ in R/p. i.e., $a_i \in p$. This holds for all

$p \in \mathrm{Spec}R$; and for all $i \geq 1$.

Therefore $a_i \in \cap\, p$, $\forall\, i \geq 1$. i.e., $a_i \in \mathrm{Nil}(R)$ $\forall\, i \geq 1$. (by Theorem 3.1.2). Also $f(x)g(x) = 1$, implies that $a_o b_o = 1$ i.e., $a_o \in U(R)$.

Conversely suppose $f(x) = a_o + a_1 x + \ldots + a_n x^n \in R[x]$ is such that $a_o \in U(R)$ and $a_1, a_2, \ldots, a_n \in \mathrm{Nil}(R)$. Since $a_1, a_2, \ldots, a_n$ are nilpotents $a_1 x$, $a_2 x^2$, $a_3 x^3, \ldots$, $a_n x^n$ are also nilpotents and by Remark 3.1.1 $z = a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_n x^n$ is also nilpotent. So $z^t = 0$ for some $t \geq 1$.

Taking $g(x) = 1/a_o - z/a_o^2 + \ldots + z^{t-1}/a_o^t$

we see that $f(x)g(x) = 1$. Therefore $f(x) \in U(R[x])$.

This seems to be an appropriate place to record a couple of results. Remark 3.1.5 is a special case of a result valid for arbitrary rings. Corollary 3.1.6 ($\equiv$ Remark 2.5.9) has been used in 2.5.11.

3.1.5 <u>REMARK</u>. For any $f \in J(R[x])$, $1 + xf \in U(R[x])$.

Proof: Suppose $1 + xf$ is not a unit in $R[x]$. Then $(1 + xf)R[x] \subsetneq R[x]$. So there exists a maximal ideal $\mathfrak{m}_o$ of $R[x]$ such that $(1 + xf)R[x] \subseteq \mathfrak{m}_o$. Now $xf \in J(R[x]) \Rightarrow xf \in \mathfrak{m}$, for every maximal ideal $\mathfrak{m}$ of R. In particular $(1 + xf) \in \mathfrak{m}_o$. Therefore $(1 + xf) - xf \in \mathfrak{m}_o$ which is a contradiction. Thus $(1 + xf)$ must be a unit in $R[x]$. ∎

3.1.6 <u>COROLLARY</u>. The Jacobson radical $J(R[x])$ and the nil radical $\mathrm{Nil}(R[x])$ of the polynomial ring over a commutative ring R coincide.

Proof: We know that $\mathrm{Nil}(R[x]) \subseteq J(R[x])$. (This is in fact true for any commutative ring R; this follows as a corollary to Theorem 3.1.2.) Let $f(x) \in J(R[x])$,

$f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$. Then by Remark 3.1.5,

$1 + xf(x) = 1 + \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_n x^{n+1} \in U(R[x])$,

$\Rightarrow$ each α_i is nilpotent and $1 \in U(R) \Rightarrow f(x) \in Nil(R[x])$. Therefore we obtain $J(R[x]) = Nil(R[x])$. ∎

<u>REMARK</u>. For related results on the Jacobson radical of a polynomial ring due to S.Amitsur, we will refer to Ex 5 and 6, p 393 of [JII]. Note also that the analogous assertion for power series is false as can be seen by taking the power series ring over a field.

We now prove a theorem on zero-divisors which is due to Scott.

3.1.7 <u>THEOREM</u>. Let R be a commutative ring and let R[x] be the ring of polynomials over R. If $f(x) \in R[x]$ is a divisor of zero; then there is an element c in R, $c \neq 0$ such that $cf(x) = 0$.

Proof: Deny the theorem and let $g(x)$ be a polynomial of smallest degree such that $f(x)g(x) = 0$. Let

$f(x) = a_0 + a_1 x + \ldots + a_m x^m$; $g(x) = b_0 + b_1 x^1 + \ldots + b_n x^n$, where $b_n \neq 0$, and $n \geq 1$. Since $b_n f(x) \neq 0$, $a_i b_n \neq 0$ for some i and therefore $a_i g(x) \neq 0$. Let r be the largest integer such that $a_r g(x) \neq 0$. Then $f(x)g(x) = (a_0 + \ldots + a_r x^r)(b_0 + \ldots + b_n x^n) = 0$. Hence $a_r b_n = 0$ and $\deg(a_r g(x)) < n$. However $(a_r g(x))f(x) = 0$ which is a contradiction.

REMARKS. (I) A similiar result is valid for reduced rings. (See Remark 2.3.20(I) .)

(II) This theorem is not true for R non-commutative. Consider the following example.

3.1.8 EXAMPLE.

Let $R = M_2(\mathbb{Z})$, the ring of 2x2 matrices over the ring of integers. Let $f(x) = E_{12}x + E_{11}$; $g(x) = E_{11}x - E_{21}$. Then $f(x)g(x) = 0$ as seen earlier (2.3.21). Now suppose $r \in R$ is such that $rg(x) = 0$. Since $r \in R$, $r = r_1E_{11} + r_2E_{22} + r_3E_{12} + r_4E_{21}$, $r_i \in \mathbb{Z}$; $i = 1,2,3,4$.

Then, $r(g(x)) = 0 \Rightarrow (r_1E_{11} + r_2E_{22} + r_3E_{12} + r_4E_{21})(E_{11}x - E_{21}) = 0$.

$\Rightarrow r_1 = 0$, $r_4 = 0$; and $r_2 = 0 \Rightarrow r_3E_{12}(E_{11}x - E_{21}) = 0 \Rightarrow r_3 = 0$.

Therefore $r = 0$.

§.3.2 Primary rings.

The language of primary ideals will be used in the next section. The results of this section are also of some independent interest.

3.2.1 *Definition.* A commutative ring R is called a primary ring if its zero ideal is a primary ideal i.e., $\forall\ r \in R$, the homomorphism $\theta_r : R \longrightarrow R$ is either one-one or nilpotent. Equivalently, every element of R is either a non-zero divisor or a nilpotent element.

3.2.2 *Definition.* A commutative ring R is called a completely primary ring if its nil radical is a maximal ideal.

3.2.3 *Definition.* If a ring R is such that all its zero divisors belong to $J = J(R)$, it will be called a J-primary ring.

3.2.4 THEOREM. Let R be a ring. The following conditions are equivalent.

(i) R is a primary ring.

(ii) $R[x]$ is a primary ring.

(iii) $R[x]$ is a J-primary ring.

Proof: ((i) $\Rightarrow$ (ii)) Let R be a primary ring. Let $f(x)$ be a divisor of zero in $R[x]$. Then if $f(x) = \sum_{i=0}^{n} f_i x^i$, $\exists\ r \in R$ $r \neq 0$ such that $rf_i = 0 \quad \forall\ i = 0,1,\ldots,n$. This implies that $f_i \in \mathrm{Nil}(R) \quad \forall\ i = 0,1,\ldots,n \Rightarrow f(x) \in \mathrm{Nil}(R[x]) = J(R[x])$ (by 3.1.6) $\Rightarrow R[x]$ is a primary ring.

((ii) $\Rightarrow$ (i)) Let a be a zero divisor in R $\Rightarrow$ a is a zero divisor in $R[x] \Rightarrow a \in \mathrm{Nil}(R[x])$ (since $R[x]$ is a primary ring). This implies that $a \in \mathrm{Nil}(R) \Rightarrow$ R is a primary ring.

((ii) $\Rightarrow$ (iii)) OBVIOUS.

((iii) $\Rightarrow$ (ii)) Let $R[x]$ be J-primary, and $f(x) \in R[x]$. *Suppose that* $f(x)$ *is a divisor of zero. Then by hypothesis,* $f(x) \in J(R[x]) = \mathrm{Nil}(R[x])$ showing that $R[x]$ is a primary ring. ∎

§ 3.3 Zero-divisors and nilpotent elements.

In this section we will study some properties of the zero-divisor and nilpotents elements of the power series rings over a commutative ring.

Let $f(x) = \sum_{i=0}^{n} f_i x^i$. Then $f^{(n)}$ is zero or a polynomial of degree at most n.

3.3.1 <u>LEMMA</u>. Let R be a commutative ring having characteristic a positive prime p and let $f(x) = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$

The following conditions are equivalent.

(a) $f(x)$ is nilpotent.

(b) There is a natural number m such that $(f_i)^m = 0$ $\forall\ i \in \mathbb{N} \cup \{0\}$.

(c) There is a natural number m such that $(f^{(k)})^m = 0$ $\forall\ i \in \mathbb{N} \cup \{0\}$.

Proof: ((a) $\Rightarrow$ (b)) We know that in a ring of characteristic p $(a + b)^{p^n} = a^{p^n} + b^{p^n}$. Thus we have

$$(f(x))^{p^n} = (f_0 + f_1x + f_2x^2 + \ldots.)^{p^n} = f_0^{p^n} + (f_1x + f_2x^2 + \ldots.)^{p^n}$$

$$= f_0^{p^n} + (f_1x)^{p^n} + (f_2x^2 + \ldots.)^{p^n}$$

$$(f(x))^{p^n} = \sum_{i=0}^{\infty} f_i x^{ip^n}.$$

Conversely if $(f(x))^m = 0$, then choosing $n \in \mathbb{N}$ such that $p^n > m$,

$(f(x))^{p^n} = 0 \Rightarrow (f_i)^{p^n} = 0\ \forall\ i.$

3.3.2 <u>THEOREM</u>. Let R be a commutative ring with identity having characteristic $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_t^{e_t}$, and let $f(x) = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$

The following conditions are equivalent.

(a) $f(x)$ is nilpotent.

(b) There is a natural number m such that $(f_i)^m = 0$ for each $i \in \mathbb{N} \cup \{0\}$.

(c) There is a natural number m such that $(f^{(k)})^m = 0$ for each $k \in \mathbb{N} \cup \{0\}$.

Proof: We let $\phi_j : R[[x]] \longrightarrow R[[x]]/(p_j)$. Now $R[[x]]/(p_j) \cong (R/p_j)[[x]]$. We know that for $1 \le j \le t$, $R/(p_j)$ has characteristic p_j, and ϕ_j is the natural homomorphism for $1 \le j \le t$.

((a) $\Rightarrow$ (b)) Suppose $f(x)$ is nilpotent. i.e., $(f(x))^m = 0$ for some m. Then $\phi_j(f(x))^m = 0$ in $R[[x]]/(p_j)$. By Lemma 3.3.1, there is a natural number m_j $(1 \le j \le t)$ satisfying for each $i \in \mathbb{N} \cup \{0\}$ $(\phi_j(f_i))^{m_j} = 0$. i.e., $\phi_j((f_i)^{m_j}) = 0$. i.e., $(f_i)^{m_j} \in p_jR$ for each $i \in \mathbb{N} \cup \{0\}$. Let $m = m_1e_1 + m_2e_2 + \ldots + m_te_t$. Then

$$(f_i)^m = (f_i)^{m_1e_1+\ldots+m_te_t} \in (p_1R)^{e_1}(p_2R)^{e_2}\ldots(p_tR)^{e_t}$$
$$= (p_1^{e_1}p_2^{e_2}\ldots p_t^{e_t})R = nR = 0.$$

((b) $\Rightarrow$ (a)) Suppose there is a natural number satisfying $(f_i)^m = 0$ for each i. Then for each j; $1 \le j \le t$, $(\phi_j(f_i)^m) = (\phi_j(f_i))^m = 0 \ \forall\, i$. By Lemma 3.3.1, there is for each j; $(1 \le j \le t)$, a natural number m_j such that $(\phi_j f(x))^{m_j} = 0 \ \forall\, i$. Now $(\phi_j(f(x))^{m_j} = (\phi_j(f(x)^{m_j}) = 0 \Rightarrow (f(x))^{m_j} \in (p_j)$, $1 \le i \le t$. Let $m = m_1e_1 + m_2e_2 + \ldots + m_te_t$. Then

$$(f(x))^m = ((f(x)^{m_1})^{e_1}((f(x)^{m_2})^{e_2}\ldots((f(x)^{m_t})^{e_t}$$
$$\in (p_1R[[x]])^{e_1}(p_2R[[x]])^{e_2}\ldots(p_tR[[x]])^{e_t} = nR = 0.$$

So $f(x)$ is nilpotent.

((b) $\Rightarrow$ (c)) Follows from the above proof and Lemma 3.3.1.

3.3.3 THEOREM. Let R be a commutative ring with identity let $f(x) = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$. Let $A_f = \sum_{i=0}^{\infty} Rf_i$. Then the condition

(i) The ideal A_f is nilpotent implies the condition

(ii) f is nilpotent.

Proof: Suppose A_f is nilpotent of order k, i.e., $(A_f)^k = 0$. Now, $(A_f)^2 = \sum_{i,j \geq 0} r_{ij} f_i f_j$, $(A_f)^3 = \sum_{i \geq 0} r_{i_1 i_2 i_3} f_{i_1} f_{i_2} f_{i_3}$,

$$(A_f)^k = \sum_{i_t \geq 0} r_{i_1 i_2 \ldots i_k} f_{i_1} f_{i_2} \ldots f_{i_k} = 0.$$ This implies that

$$f_{i_1} f_{i_2} \ldots f_{i_k} = 0 \quad \forall\ i_t = 0 \text{ and } 1 \leq t \leq k.$$

We have $f(x) = \sum_{i=0}^{\infty} f_i x^i$. In the expansion of $(f(x))^k$, each coefficient will be of the type $f_{i_1} f_{i_2} \ldots f_{i_k}$, where the i_j's may be repeated. Since $f_{i_1} f_{i_3} \ldots f_{i_k} = 0 \ \forall\ i_t \geq 0$, it follows that

$(f(x))^k = 0 \rightarrow f(x)$ is nilpotent. ∎

3.3.4 COROLLARY. If A_f is finitely generated and each f_i is nilpotent, then f is nilpotent.

Proof: Let $A_f = Ra_1 + Ra_2 + \ldots + Ra_t$ and $f_i \in A_f$ where f_i is given as $f_i = \sum_{j=1}^{t} r_{ij} a_j$. Also $a_l = \sum_{p=0}^{n_l} r_{l_p} f_p$ and

$a_1, a_2, \ldots, a_n \in \sum_{p=0}^{n_0} Rf_p$, where $n_0 = \text{Max}(n_1, n_2, \ldots, n_t)$. Since each f_p is nilpotent, each a_l is nilpotent. Therefore $a_l^{m_l} = 0$ for some

$m_i \in \mathbb{N}$. If $k = \sum_{i=1}^{t} m_i$, $\quad (a_f)^k = 0 \rightarrow f^k = 0 \rightarrow f$ is nilpotent. ∎

We now give an example to show that f nilpotent does not in general imply that A_f is nilpotent. In other words finite generation of A_f is necessary for the validity of the condition (ii) implies condition (i) in 3.3.3.

3.3.5 <u>EXAMPLE</u>. Let $S = \mathbb{Z}/p\mathbb{Z}$, where p is a prime and $S_0 = S[X_0, X_1, \ldots, X_n, \ldots]$ be the ring of polynomials in countably many indeterminates.

Let $R = S_0/(X_0^p, X_1^p, \quad , X_i^p, \ldots)$. Let $f_i = \overline{X}_i$.

Consider $f(x) = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$. Then for each $k \in \mathbb{N} \cup \{0\}$, $(f^{(k)})^p = 0$. But for each $n \in \mathbb{N}$, $0 \neq f_0 f_1 f_2 \ldots f_{n-1} \in (A_f)^n$

(If $f_0 f_1 f_2 \ldots . f_{n-1} = 0$ then $f_0 f_1 f_2 \ldots . f_{n-1} \in (X_0^p, X_1^p, \ldots, X_n^p, \ldots)$ which is absurd. Thus A_f cannot be nilpotent.

3.3.6 <u>LEMMA</u>. Suppose there exists a $t \in \mathbb{N}$ such that f_t is a non-zero-divisor and f_j is nilpotent $\forall\ 1 \leq j \leq t-1$. Then $f(x) = \sum_{i=0}^{\infty} f_i x^i$ is a non-zero-divisor in $R[[x]]$.

Proof: Let $g(x) = \sum_{i=0}^{t-1} f_i x^i$, $h(x) = \sum_{i=t}^{\infty} f_i x^i$

so that g(x) is nilpotent and $f(x) = g(x) + h(x)$.

Let T = total quotient ring of R,

$= S_0^{-1}R$ (where S_0 is the set of all non-zero-divisors of R).

and $S = T[[x]]_M$, localisation at M, where $M = \left\{x, x^2, x^3, \ldots, x^m, \ldots\right\}$

is a multiplicatively closed set in $T[[x]]$.

Now $h(x) = x^{t}(f_{t} + f_{t+1}x + \ldots) = x^{t}h'(x)$,

where $h'(x) = \sum_{i=0}^{\infty} f_{t+i}x^{i}$.

So $h(x)$ and $h'(x)$ are associates in S. Also $f_{t} = (h'(x))_{o}$ is a non-zero-divisor in R. So $f_{t} \in S_{o}$, hence is a unit in T. Therefore $h'(x)$ is a unit in $T[[x]]$, hence a unit in S. This implies that $h(x)$ is a unit in S (since $h(x)$ and $h'(x)$ are associates).

Therefore $f(x) = g(x) + h(x)$ is a unit in S (since $h(x)$ is a unit and $g(x)$ is a nilpotent element of S) so that $f(x)$ is a non-zero-divisor in S. Suppose there exists an $\bar{f}(x) \in S$ such that $f(x)\bar{f}(x) = 0$ in $R[[x]]$. We already have the embeddings

$R[[x]] \longrightarrow T[[x]] \longrightarrow S$. Therefore $f(x)\bar{f}(x) = 0$ in S. This implies that $\bar{f}(x) = 0$, since $f(x)$ is a non-zero-divisor in S. Therefore $f(x)$ is a non-zero-divisor in $R[[x]]$. ■

3.3.7 THEOREM. Let R be a commutative ring in which every non-zero-divisor is nilpotent and let $f(x) = \sum_{i=0}^{\infty} f_{i}x^{i} \in R[[x]]$. If some f_{i} is a non-zero-divisor in R, then $f(x)$ is a non-zero-divisor in $R[[x]]$.

Proof: Let k be the least positive integer such that f_{k} is a non-zero-divisor. So $f_{o}, f_{1}, \ldots, f_{k-1}$ are zero-divisors and so by hypothesis they are all nilpotent. Now by applying 3.3.6 we immediately have that $f(x)$ is a non-zero-divisor in $R[[x]]$. ■

3.3.8 *Definition.* Let A be an ideal in a commutative ring R. We call A a primary ideal of R if for every $r \in R$, the R-homomorphism $\theta_{r} : R/A \longrightarrow R/A$ is either one-one or nilpotent.

(Equivalently: for all $r \in R$, if $\exists\ x \notin A$ such that $rx \in A$, then $r^m \in A$ for some $m \in \mathbb{N}$.)

Proof of this equivalence. Suppose $0 = \overline{rx} = r\bar{x} = \theta_r(\bar{x})$, $\bar{x} \neq 0$. So θ_r is nilpotent. Therefore $(\theta_r)^m = 0$ for some $m \Rightarrow r^m T = 0$ $\Rightarrow r^m \in A$ for some m.

Thus A is a primary ideal of R if and only if R/A is a primary ring in the sense of § 3.2.

3.3.9 <u>REMARK</u>. Let A be a primary ideal and let $\bar{A} = \left\{ r \in R \mid \theta_r \text{ is nilpotent} \right\}$. Now $0 \in \bar{A}$, so $\bar{A}$ is non-empty. Also $\bar{A}$ is an ideal of R satisfying $1 \notin A$ (We assume $1 \neq 0$). In fact, $\bar{A}$ is a prime ideal of R. For suppose $x, y \notin \bar{A}$, then θ_x, θ_y are one-one.

Therefore $\theta_{xy} = \theta_x\theta_y$ is also one-one $\Rightarrow xy \notin \bar{A}$. If $a \in A$, then $\theta_a = 0 \Rightarrow a \in \bar{A} \Rightarrow A \subseteq \bar{A}$. We say A is $\bar{A}$ primary. (Notice that the terminology differs from that used in 3.2.3.)

3.3.10 <u>COROLLARY</u>. Let R be a commutative ring with identity, in which each zero-divisor is nilpotent. If the ideal $\mathrm{Nil}(R)$ is nilpotent then in $R[[x]]$, each zero-divisor is nilpotent.

Proof: Let $f(x) = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$. Suppose $f(x)$ is not nilpotent. Then A_f is not nilpotent $\Rightarrow A_f \leq \mathrm{Nil}(R)$ i.e., not every coefficient of $f(x)$ is nilpotent. So by hypothesis, $f(x)$ has a non-zero-divisor as a coefficient and by Theorem 3.3.7, $f(x)$ is a non-zero-divisor. Thus each zero-divisor is nilpotent. ∎

In terms of Definition 3.3.8, Corollary 3.3.10 can be restated as follows. (See [F:71])

3.3.11 <u>COROLLARY</u>. Let R be a commutative ring with identity in which (O) is Nil(R)-primary. If Nil(R) is nilpotent, then (O) is a primary ideal of R[[x]].

Finally we state the following analogue of Theorem 3.1.7 without proof, and record a related example.

3.3.12 <u>THEOREM</u>. Let R be a Noetherian ring with identity. Then for $f(x) = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$, the following conditions are equivalent.

(I) f(x) is a zero-divisor in R[[x]].

(II) There is a non-zero-divisor element $r \in R$ which satisfies $rf(x) = 0$.

Proof: (II) $\Rightarrow$ (I) TRIVIAL.

(I) $\Rightarrow$ (II) See [F:71]. ∎

We conclude with an example to show that Theorem 3.3.12 fails when R is not Noetherian.

3.3.13 <u>EXAMPLE</u>. Let S be a commutative ring and let $\left\{ Y, X_0, X_1, \ldots, X_i, \ldots \right\}$ be a set of indeterminates over S and let $R = S\left[Y, \left\{X_i\right\}_{i=0}^{\infty} \right] / \left(X_0 Y, \left\{X_i - X_{i+1} Y \right\}_{i=0}^{\infty} \right)$

Let X be an indeterminate.

Let $y = \overline{Y}$ and let $f(X) = y - X$. Then f(X) has a unit coefficient so certainly $rf(X) \neq 0$ for each non-zero element r of R.

However, letting $x_i = \overline{X}_i$ and $g(X) = \sum_{i=0}^{\infty} x_i X^i$ we see that $f(X)g(X) = 0$ while $g(X) \neq 0$.

§ 3.4 Bibliographical notes.

1. Theorem 3.1.2 is due to Krull, see the references after its statement.

2. Gilmer [G:75] has carried out a detailed survey of the topics studied in this chapter and a number of other related topics. Brewer [B] has written a monograph on power series rings over commutative rings. Gilmer and Brewer have referred to several dozen other papers in this area.

3. Gilmer [G:75] attributes theorem to Snapper [S:50]

4. Theorem 3.1.7 is due to McCoy [M:42]. The elegent inductive proof given here is due to Scott [S:54].

5. The results of § 3.2 are due to Snapper [S:50].

6. The results of § 3.3 are due to Fields [F:71]. (Example 3.3.13 is due to Gilmer as mentioned by Fields in a footnote on p 433 of [F:71].)

BIBLIOGRAPHY

BOOKS AND MONOGRAPHS.

[AF] F.W. Anderson and K.R. Fuller, Rings and Categories of Modules, Springer-Verlag, New York, 1974.

[B] J.W. Brewer, Power series over commutative rings, Marecl Dekker, 1981.

[JI] N. Jacobson, Basic Algebra, Vol I, Hindustan Publishing Corporation, 1984.

[JII] N. Jacobson, Basic Algebra, Vol II, Hindustan Publishing Corporation, 1984.

[K] I. Kaplansky, Rings with operators, W.A. Benjamin, New York, 1968.

[KI] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhauser, Boston, 1985.

[L] J. Lambek, Lectures on Rings and Modules, Blaisdell, Waltham, 1966.

[N] M. Nagata, Local Rings, Interscience, 1962.

[R] J.J. Rotman, Notes on Homological Algebra, Van Nostrand Reinhold, New York, 1970.

[S] B.Stenstrom, Rings of Quotients: An introduction to the Methods of Ring Theory, Springer Verlag, New York, 1970.

[GII] K. R. Goodearl, Von Neumann Regular Rings, Pitman, London, 1979.

RESEARCH PAPERS.

[A:74] E. Armendariz, A note on extensions of Baer and P.P. rings, J. Austral. Math. Soc 18(1974), 470-473.

[B:76] Review of [A:74] by W.D. Burgess in Mathematical reviews, 51(1976) # 3224 (Reviews in Ring Theory 17.02.016)

[C:73] V.P.Camillo, A note on semi-hereditary rings, Arch. Math. 24(1973), 142-143.

[E:72] M.W. Evans, On commutative P.P. rings, Pacific Journal of Mathematics 41(1972), 687-697.

[E:60] S.Endo, Note on P.P. rings (A supplement to Hattori's paper) Nagoya Math. Journal 17(1960) 167-170.

[F:71] D.E. Fields, Zero divisors and nilpotent elements in power series rings, Proc. Amer. Math. Soc. 27(1971), 427-433.

[G:75] R. Gilmer, On polynomial and power series rings over a commutative ring, Rocky Mountain Journal of Mathematics 5(1975), 157-175.

[HT:79] Y. Hirano and H Tominaga, Regular rings, V-rings and their generalisations, Hiroshima Math. Journal 9(1979), 137-149.

[H:81] Y. Hirano, Regular modules and V-modules, Hiroshima Math. Journal 11(1981), 125-142.

[J:71] S.Jondrup, p.p. rings and finitely generated flat ideals, Proc. Amer. Math. Soc. 28(1971), 431-433.

[M:73] M. McCarthy, The ring of polynomials over a von Neumann regular ring, Proc. Amer. Math. Soc. 39(1973), 253-254.

[NW:88] W.K. Nicholson and J.F. Watters, Rings with projective socle, Proc. Amer. Math. Soc. 102(1988), 443-450.

[P:85] P.Pillay, A note on polynomial rings over von Neumann regular rings, Questiones Mathematicae 8(1985), 79-81.

[S:73] M.S. Shrikhande, On hereditary and co-hereditary modules, Canadian Journal of Mathematics 25(1973), 892-896.

[S:54] W.R. Scott, Divisors of zero in polynomial rings, Amer. Mat Monthly 61(1954), 336.

[S:50] E.Snapper, Completely primary rings II, Annals of Mathematics(2) 52(1950), 666-693.

[V:82] K. Varadarajan, A generalisation of Hilbert's basis theorem, Communications in Algebra 10(1982), 2191-2204.

[W:61] K.G. Wolfson, Baer rings of endomorphisms, Math. Ar 143(1961), 19-28.

[X:91] W. Xue, A note on two questions of K. Varadarajan, Communications in Algebra 19(5)(1991), 1445-1447.

[Z:72] J.M. Zelmanowitz, Regular modules, Trans. Amer. Math. Soc. 163(1972), 341-355.